

*IBM Spectrum Protect Knowledge Center Version 8.1.3*



---

# Inhaltsverzeichnis

|   |    |
|---|----|
| <b>Willkommen</b>   | 1  |
| <b>Behindertengerechte Bedienung</b>  | 1  |
| <b>Produktsuites und zugehörige Produkte</b>                                      | 2  |
| <b>PDF-Dateien</b>  | 4  |
| <b>Aktualisierungen in diesem Release</b>   | 5  |
| <b>IBM Spectrum Protect-Konzepte</b>  | 5  |
| Übersicht über IBM Spectrum Protect   | 5  |
| Datenschutzkomponenten  | 5  |
| Datenschutzservices   | 6  |
| Prozesse zur Verwaltung des Datenschutzes   | 8  |
| Benutzerschnittstellen  | 11 |
| Konzepte der Datenspeicherung   | 12 |
| Datenspeichereinheiten  | 12 |
| Speicherpools   | 15 |
| Datenübertragung in Speicher  | 19 |
| Datenschutzstrategien   | 21 |
| Minimieren des Speicherbereichs für Sicherungen                                   | 22 |
| Strategien zum Schutz vor Katastrophen  | 23 |
| Konzepte der Wiederherstellung nach einem Katastrophenfall                        | 26 |
| <b>Datenschutzlösungen</b>  | 28 |
| Datenschutzlösung auswählen   | 28 |
| Plattenspeicherlösung für einen einzelnen Standort                                | 29 |
| Plattenspeicherlösung für mehrere Standorte                                       | 29 |
| Appliance-Lösung für mehrere Standorte  | 30 |
| Bandspeicherlösung  | 31 |
| Vergleich der Lösungen  | 32 |
| Lösungsroadmap  | 34 |
| Plattenspeicherlösung für einen einzelnen Standort                                | 35 |
| Planung   | 35 |
| Systemgröße auswählen   | 36 |
| Systemvoraussetzungen für eine Plattenspeicherlösung für einen einzelnen Standort | 37 |
| Hardwarevoraussetzungen   | 37 |
| Softwarevoraussetzungen   | 38 |
| Arbeitsblätter zur Planung  | 39 |
| Planung für Speicher  | 48 |
| Planung für Sicherheit  | 48 |
| Planung für Administratorrollen   | 49 |
| Planung für sichere Kommunikation   | 49 |
| Planung für die Speicherung verschlüsselter Daten                                 | 50 |
| Planung des Firewallzugriffs  | 50 |
| Implementierung   | 51 |
| System konfigurieren  | 52 |
| Speicherhardware konfigurieren  | 52 |
| Serverbetriebssystem installieren   | 52 |
| Installation auf AIX-Systemen   | 53 |
| Installation auf Linux-Systemen   | 54 |

|   |     |
|---|-----|
| Installation auf Windows-Systemen   | 58  |
| Multipath I/O konfigurieren   | 58  |
| AIX-Systeme   | 58  |
| Linux-Systeme   | 59  |
| Windows-Systeme   | 60  |
| Benutzer-ID für den Server erstellen  | 61  |
| Dateisysteme für den Server vorbereiten   | 62  |
| AIX-Systeme   | 62  |
| Linux-Systeme   | 63  |
| Windows-Systeme   | 64  |
| Server und das Operations Center installieren                                   | 64  |
| Installation auf AIX- und Linux-Systemen  | 64  |
| Installation auf Windows-Systemen   | 65  |
| Server und das Operations Center konfigurieren                                  | 66  |
| Serverinstanz konfigurieren   | 66  |
| Client für Sichern/Archivieren installieren                                     | 67  |
| Optionen für den Server festlegen   | 68  |
| Sichere Kommunikation mit Transport Layer Security konfigurieren                | 69  |
| Operations Center konfigurieren   | 69  |
| Produktlizenz registrieren  | 70  |
| Dateneduplizierung konfigurieren  | 70  |
| Datenaufbewahrungsregeln für Ihr Unternehmen definieren                         | 71  |
| Zeitpläne für Serververwaltungsaktivitäten definieren                           | 71  |
| Clientzeitpläne definieren  | 73  |
| Clients für Sichern/Archivieren installieren und konfigurieren                  | 73  |
| Clients registrieren und Zeitplänen zuordnen                                    | 74  |
| Clientverwaltungsservice installieren   | 74  |
| Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen             | 75  |
| Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren | 76  |
| Implementierung abschließen   | 77  |
| Überwachung   | 77  |
| Prüfliste für tägliche Tasks  | 77  |
| Prüfliste für regelmäßige Tasks   | 84  |
| Lizenz Einhaltung überprüfen  | 90  |
| Systemstatus mithilfe von E-Mail-Berichten verfolgen                            | 91  |
| Verwalten   | 92  |
| Operations Center verwalten   | 93  |
| Peripherieserver hinzufügen und entfernen                                       | 93  |
| Peripherieserver hinzufügen   | 93  |
| Peripherieserver entfernen  | 94  |
| Web-Server starten und stoppen  | 94  |
| Assistenten für die Erstkonfiguration erneut starten                            | 95  |
| Hub-Server ändern   | 96  |
| Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben                 | 96  |
| Anwendungen, virtuelle Maschinen und Systeme schützen                           | 97  |
| Clients hinzufügen  | 97  |
| Client-Software auswählen und Installation planen                               | 98  |
| Regeln zum Sichern und Archivieren von Clientdaten angeben                      | 100 |
| Maßnahmen anzeigen  | 101 |
| Maßnahmen editieren   | 101 |
| Sicherungs- und Archivierungsoperationen planen                                 | 102 |
| Clients registrieren  | 103 |
| Clients installieren und konfigurieren  | 104 |
| Client für die Ausführung geplanter Operationen konfigurieren                   | 105 |
| Kommunikation durch eine Firewall konfigurieren                                 | 107 |
| Clientoperationen verwalten   | 107 |
| Fehler in Clientfehlerprotokollen auswerten                                     | 108 |
| Clientakzeptor stoppen und erneut starten                                       | 108 |

|  |     |
|--|-----|
| Kennwörter zurücksetzen  | 109 |
| Bereich einer Clientsicherung ändern                                       | 110 |
| Client-Upgrades verwalten  | 111 |
| Clientknoten stilllegen  | 111 |
| Daten zum Freigeben von Speicherbereich inaktivieren                       | 113 |
| Datenspeicher verwalten  | 114 |
| Speicherpoolcontainer prüfen   | 114 |
| Bestandskapazität verwalten  | 114 |
| Speichernutzung und Prozessorauslastung verwalten                          | 116 |
| Geplante Aktivitäten optimieren  | 117 |
| Server schützen  | 117 |
| Sicherheitskonzepte  | 117 |
| Administratoren verwalten  | 119 |
| Kennwortanforderungen ändern   | 120 |
| Server auf dem System schützen   | 121 |
| Benutzerzugriff auf den Server einschränken                                | 121 |
| Zugriff über Porteinschränkungen einschränken                              | 122 |
| Server stoppen und starten   | 123 |
| Server stoppen   | 123 |
| Server für Verwaltungs- oder Rekonfigurationstasks starten                 | 124 |
| Durchführung eines Upgrades für den Server planen                          | 124 |
| Vorbereitungen für einen Ausfall   | 125 |
| Plan zur Wiederherstellung nach einem Katastrophenfall implementieren      | 125 |
| Wiederherstellung nach einem Systemausfall                                 | 126 |
| Plattenspeicherlösung für mehrere Standorte                                | 127 |
| Planung  | 127 |
| Systemgröße auswählen  | 128 |
| Planung der Standorte  | 129 |
| Systemvoraussetzungen für eine Plattenspeicherlösung für mehrere Standorte | 130 |
| Hardwarevoraussetzungen  | 130 |
| Softwarevoraussetzungen  | 131 |
| Arbeitsblätter zur Planung   | 133 |
| Planung für Speicher   | 142 |
| Planung für Sicherheit   | 142 |
| Planung für Administratorrollen  | 143 |
| Planung für sichere Kommunikation  | 143 |
| Planung für die Speicherung verschlüsselter Daten                          | 144 |
| Planung des Firewallzugriffs   | 144 |
| Implementierung  | 145 |
| System konfigurieren   | 146 |
| Speicherhardware konfigurieren   | 146 |
| Serverbetriebssystem installieren  | 147 |
| Installation auf AIX-Systemen  | 147 |
| Installation auf Linux-Systemen  | 148 |
| Installation auf Windows-Systemen  | 152 |
| Multipath I/O konfigurieren  | 152 |
| AIX-Systeme  | 152 |
| Linux-Systeme  | 153 |
| Windows-Systeme  | 154 |
| Benutzer-ID für den Server erstellen                                       | 155 |
| Dateisysteme für den Server vorbereiten                                    | 156 |
| AIX-Systeme  | 156 |
| Linux-Systeme  | 157 |
| Windows-Systeme  | 158 |
| Server und das Operations Center installieren                              | 158 |
| Installation auf AIX- und Linux-Systemen                                   | 159 |
| Installation auf Windows-Systemen  | 159 |
| Server und das Operations Center konfigurieren                             | 160 |

|  |     |
|--|-----|
| Serverinstanz konfigurieren  | 161 |
| Client für Sichern/Archivieren installieren  | 162 |
| Optionen für den Server festlegen  | 162 |
| Sichere Kommunikation mit Transport Layer Security konfigurieren                   | 163 |
| Operations Center konfigurieren  | 163 |
| Produktlizenz registrieren   | 164 |
| Dateneduplizierung konfigurieren   | 165 |
| Datenaufbewahrungsregeln für Ihr Unternehmen definieren                            | 165 |
| Zeitpläne für Serververwaltungsaktivitäten definieren                              | 165 |
| Clientzeitpläne definieren   | 167 |
| Clients für Sichern/Archivieren installieren und konfigurieren                     | 168 |
| Clients registrieren und Zeitplänen zuordnen                                       | 168 |
| Clientverwaltungsservice installieren  | 169 |
| Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen                | 169 |
| Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren    | 170 |
| Zweiten Server konfigurieren   | 171 |
| SSL-Kommunikation zwischen dem Hub-Server und einem Peripherieserver konfigurieren | 171 |
| Zweiten Server als Peripherieserver hinzufügen                                     | 173 |
| Replikation aktivieren   | 173 |
| Implementierung abschließen  | 173 |
| Überwachung  | 174 |
| Prüfliste für tägliche Tasks   | 174 |
| Prüfliste für regelmäßige Tasks  | 182 |
| Lizenz Einhaltung überprüfen   | 188 |
| Systemstatus mithilfe von E-Mail-Berichten verfolgen                               | 189 |
| Verwalten  | 190 |
| Operations Center verwalten  | 191 |
| Peripherieserver hinzufügen und entfernen  | 191 |
| Peripherieserver hinzufügen  | 191 |
| Peripherieserver entfernen   | 192 |
| Web-Server starten und stoppen   | 192 |
| Assistenten für die Erstkonfiguration erneut starten                               | 193 |
| Hub-Server ändern  | 194 |
| Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben                    | 194 |
| Anwendungen, virtuelle Maschinen und Systeme schützen                              | 195 |
| Clients hinzufügen   | 195 |
| Client-Software auswählen und Installation planen                                  | 196 |
| Regeln zum Sichern und Archivieren von Clientdaten angeben                         | 198 |
| Maßnahmen anzeigen   | 199 |
| Maßnahmen editieren  | 199 |
| Sicherungs- und Archivierungsoperationen planen                                    | 200 |
| Clients registrieren   | 201 |
| Clients installieren und konfigurieren   | 202 |
| Client für die Ausführung geplanter Operationen konfigurieren                      | 203 |
| Kommunikation durch eine Firewall konfigurieren                                    | 205 |
| Clientoperationen verwalten  | 205 |
| Fehler in Clientfehlerprotokollen auswerten  | 206 |
| Clientakzeptor stoppen und erneut starten  | 206 |
| Kennwörter zurücksetzen  | 207 |
| Bereich einer Clientsicherung ändern   | 208 |
| Client-Upgrades verwalten  | 209 |
| Clientknoten stilllegen  | 209 |
| Daten zum Freigeben von Speicherbereich inaktivieren                               | 211 |
| Datenspeicher verwalten  | 212 |
| Speicherpoolcontainer prüfen   | 212 |
| Bestandskapazität verwalten  | 213 |
| Speichernutzung und Prozessorauslastung verwalten                                  | 214 |
| Geplante Aktivitäten optimieren  | 215 |

|   |     |
|---|-----|
| Replikation verwalten   | 215 |
| Replikationskompatibilität  | 216 |
| Knotenreplikation aktivieren  | 216 |
| Daten in Verzeichniscontainerspeicherpools schützen                   | 217 |
| Replikationseinstellungen ändern                                      | 218 |
| Unterschiedliche Aufbewahrungsmaßnahmen festlegen                     | 219 |
| Server schützen   | 220 |
| Sicherheitskonzepte   | 220 |
| Administratoren verwalten   | 222 |
| Kennwortanforderungen ändern  | 222 |
| IBM Spectrum Protect auf dem System schützen                          | 223 |
| Benutzerzugriff auf den Server einschränken                           | 224 |
| Zugriff über Porteinschränkungen einschränken                         | 224 |
| Server stoppen und starten  | 225 |
| Server stoppen  | 225 |
| Server für Verwaltungs- oder Rekonfigurationstasks starten            | 226 |
| Durchführung eines Upgrades für den Server planen                     | 227 |
| Vorbereitungen für einen Ausfall                                      | 227 |
| Plan zur Wiederherstellung nach einem Katastrophenfall implementieren | 228 |
| Wiederherstellung nach einem Datenverlust oder Systemausfall          | 228 |
| Datenbank zurückschreiben   | 231 |
| Beschädigte Daten wiederherstellen                                    | 233 |
| Speicherpools reparieren  | 233 |
| Bandspeicherlösung  | 234 |
| Planung   | 234 |
| Planungsvoraussetzungen für Bänder                                    | 235 |
| Systemvoraussetzungen für eine bandbasierte Lösung                    | 236 |
| Hardwarevoraussetzungen   | 236 |
| Softwarevoraussetzungen   | 239 |
| Arbeitsblätter zur Planung  | 240 |
| Planung für Plattenspeicher   | 244 |
| Planung für Bandspeicher  | 244 |
| Unterstützte Bandeinheiten und Speicherarchive                        | 245 |
| Unterstützte Bandeinheitenkonfigurationen                             | 246 |
| Datenversetzung zwischen Speichereinheiten                            | 246 |
| Gemeinsame Speicherarchivnutzung                                      | 247 |
| LAN-unabhängige Datenversetzung                                       | 247 |
| Gemischte Einheitentypen in Speicherarchiven                          | 248 |
| Verschiedene Datenträgergenerationen in einem Speicherarchiv          | 248 |
| Gemischte Datenträger und Speicherpools                               | 249 |
| Erforderliche Definitionen für Bandspeichereinheiten                  | 250 |
| Planung der Speicherpoolhierarchie                                    | 250 |
| Auslagerung von Daten   | 252 |
| Planung für Sicherheit  | 253 |
| Planung für Administratorrollen                                       | 253 |
| Planung für sichere Kommunikation                                     | 254 |
| Planung für die Speicherung verschlüsselter Daten                     | 254 |
| Planung des Firewallzugriffs  | 255 |
| Implementierung   | 256 |
| System konfigurieren  | 257 |
| Speicherhardware konfigurieren  | 257 |
| Serverbetriebssystem installieren                                     | 258 |
| Installation auf AIX-Systemen   | 258 |
| Installation auf Linux-Systemen                                       | 259 |
| Installation auf Windows-Systemen                                     | 263 |
| Multipath I/O konfigurieren   | 263 |
| AIX-Systeme   | 264 |
| Linux-Systeme   | 264 |

|   |     |
|---|-----|
| Windows-Systeme   | 265 |
| Benutzer-ID für den Server erstellen  | 266 |
| Dateisysteme für den Server vorbereiten   | 267 |
| AIX-Systeme   | 267 |
| Linux-Systeme   | 268 |
| Windows-Systeme   | 269 |
| Server und das Operations Center installieren   | 270 |
| Installation auf AIX- und Linux-Systemen  | 270 |
| Installation auf Windows-Systemen   | 271 |
| Server und das Operations Center konfigurieren  | 271 |
| Serverinstanz konfigurieren   | 272 |
| Client für Sichern/Archivieren installieren   | 273 |
| Optionen für den Server festlegen   | 273 |
| Sicherheitskonzepte   | 274 |
| Operations Center konfigurieren   | 276 |
| Produktlizenz registrieren  | 276 |
| Datenaufbewahrungsregeln für Ihr Unternehmen definieren   | 277 |
| Zeitpläne für Serververwaltungsaktivitäten definieren   | 277 |
| Clientzeitpläne definieren  | 282 |
| Bandeinheiten für den Server anschließen  | 282 |
| Automatisierte Speicherarchivereinheit an das System anschließen  | 282 |
| Bandeinheitentreiber auswählen  | 283 |
| IBM Bandeinheitentreiber  | 283 |
| IBM Spectrum Protect-Bandeinheitentreiber   | 283 |
| Geräte dateinamen für Bandeinheiten   | 284 |
| Bandeinheitentreiber installieren und konfigurieren   | 285 |
| IBM Einheitentreiber für IBM Bandeinheiten installieren und konfigurieren   | 285 |
| AIX-Systeme   | 287 |
| SCSI- und Fibre Channel-Einheiten   | 287 |
| IBM Spectrum Protect-Einheitentreiber für Datenträgerwechsler konfigurieren   | 288 |
| IBM Spectrum Protect-Einheitentreiber für Bandlaufwerke konfigurieren   | 288 |
| An ein Fibre Channel-SAN angeschlossene Einheiten konfigurieren   | 289 |
| Linux-Systeme   | 289 |
| IBM Spectrum Protect-Durchgriffstreiber für Bandeinheiten und Speicherarchive konfigurieren                           | 290 |
| zSeries LinuxFibre Channel-Adapter-Einheitentreiber (zfcp) installieren   | 291 |
| Informationen zu SCSI-Einheiten Ihres Systems   | 291 |
| Überschreiben von Bandkennsätzen verhindern   | 291 |
| Windows-Systeme   | 292 |
| Verwendung des IBM Spectrum Protect-Durchgriffstreibers für Bandeinheiten und Speicherarchive vorbereiten             | 292 |
| IBM Spectrum Protect-SCSI-Treiber für Bandeinheiten und Speicherarchive konfigurieren                                 | 293 |
| Speicherarchive für die Verwendung durch einen Server konfigurieren   | 293 |
| Bandeinheiten definieren  | 295 |
| Speicherarchive und Laufwerke definieren  | 295 |
| Speicherarchive definieren  | 295 |
| Laufwerke definieren  | 296 |
| Bandeinheitenklassen definieren   | 297 |
| Einheitenklassen LTO definieren   | 298 |
| LTO-Laufwerke und -Datenträger in einem Speicherarchiv mischen  | 298 |
| Mountlimits in LTO-Umgebungen mit gemischten Datenträgern   | 299 |
| Laufwerkverschlüsselung für LTO-Bandlaufwerke der Generation 4 oder späterer Generationen aktivieren und inaktivieren | 300 |
| Einheitenklassen 3592 definieren  | 300 |
| Generationen von 3592-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv mischen                          | 301 |
| Datenzugriffsgeschwindigkeiten für 3592-Datenträger steuern   | 302 |
| Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen aktivieren und inaktivieren     | 303 |
| Gemeinsame Speicherarchivnutzung konfigurieren  | 303 |
| Beispiel: Gemeinsame Speicherarchivnutzung für AIX- und Linux-Server  | 305 |
| Beispiel: Gemeinsame Speicherarchivnutzung für Windows-Server   | 306 |

|  |     |
|--|-----|
| Speicherarchivmanager-Server konfigurieren                                 | 306 |
| Speicherarchivclient-Server konfigurieren                                  | 308 |
| Speicherpoolhierarchie konfigurieren                                       | 309 |
| Anwendungen und Systeme schützen   | 310 |
| LAN-unabhängige Datenversetzung konfigurieren                              | 310 |
| Verschlüsselungsverfahren  | 310 |
| Bandspeicheroperationen steuern  | 312 |
| Wie Datenträger von IBM Spectrum Protect gefüllt werden                    | 313 |
| Geschätzte Kapazität von Banddatenträgern angeben                          | 313 |
| Aufzeichnungsformate für Banddatenträger angeben                           | 313 |
| Speicherarchivobjekte Einheitenklassen zuordnen                            | 314 |
| Datenträgermountoperationen für Bandeinheiten steuern                      | 314 |
| Anzahl gleichzeitig bereitgestellter Datenträger steuern                   | 315 |
| Steuern, wie lange ein Datenträger bereitgestellt bleibt                   | 315 |
| Zeit steuern, die der Server auf ein Laufwerk wartet                       | 316 |
| Operationen zurückstellen  | 316 |
| Zurückstellung von Operationen für einen Mountpunkt                        | 317 |
| Zurückstellung des Datenträgerzugriffs                                     | 317 |
| Auswirkungen von Einheitenänderungen im SAN                                | 318 |
| Einheitendaten anzeigen  | 318 |
| WORM-Banddatenträger   | 319 |
| WORM-fähige Laufwerke  | 320 |
| WORM-Datenträger zurückstellen   | 320 |
| Einschränkungen für WORM-Datenträger                                       | 320 |
| Mountfehler bei WORM-Datenträgern  | 320 |
| WORM-Datenträgern neue Kennsätze zuordnen                                  | 321 |
| Private WORM-Datenträger aus einem Speicherarchiv entfernen                | 321 |
| Erstellung von DLT WORM-Datenträgern                                       | 321 |
| Unterstützung für kurze und normale 3592 WORM-Bänder                       | 321 |
| Einheitenklasse nach der Einstellung des Parameters WORM abfragen          | 321 |
| Einheitenfehler beheben  | 321 |
| Implementierung abschließen  | 322 |
| Überwachung  | 323 |
| Prüfliste für tägliche Tasks   | 323 |
| Prüfliste für regelmäßige Tasks  | 329 |
| Bandalernachrichten auf Hardwarefehler überwachen                          | 336 |
| Durch Datenträgerinkompatibilität verursachte Fehler verhindern            | 336 |
| Operationen mit Reinigungskassetten  | 336 |
| Lizenz Einhaltung überprüfen   | 337 |
| Systemstatus mithilfe von E-Mail-Berichten verfolgen                       | 338 |
| Verwalten  | 339 |
| Operations Center verwalten  | 340 |
| Clientoperationen verwalten  | 340 |
| Fehler in Clientfehlerprotokollen auswerten                                | 340 |
| Clientakzeptor stoppen und erneut starten                                  | 341 |
| Kennwörter zurücksetzen  | 342 |
| Client-Upgrades verwalten  | 343 |
| Clientknoten stilllegen  | 343 |
| Daten zum Freigeben von Speicherbereich inaktivieren                       | 345 |
| Datenspeicher verwalten  | 346 |
| Bestandskapazität verwalten  | 346 |
| Geplante Aktivitäten optimieren  | 347 |
| Operationen durch Aktivierung der Kollokation von Clientdateien optimieren | 348 |
| Auswirkungen der Kollokation auf Operationen                               | 349 |
| Datenträger bei aktivierter Kollokation auswählen                          | 351 |
| Datenträger bei inaktiverter Kollokation auswählen                         | 352 |
| Kollokationseinstellungen  | 353 |
| Kollokation von Kopierspeicherpools  | 353 |



|  |     |
|--|-----|
| Kollokation planen und aktivieren  | 353 |
| Bandeinheiten verwalten  | 355 |
| Austauschbare Datenträger vorbereiten  | 355 |
| Banddatenträgern Kennsätze zuordnen  | 356 |
| Speicherdatenträger in ein Speicherarchiv zurückstellen  | 357 |
| Einzelnen Datenträger in ein SCSI-Speicherarchiv zurückstellen   | 358 |
| Datenträger aus Speicherarchivspeicherschächten zurückstellen  | 358 |
| Speicherdatenträger aus Eingangs-/Ausgangsports eines Speicherarchivs zurückstellen                          | 359 |
| Datenträger mithilfe von Barcodelesern in Speicherarchiven zurückstellen                                     | 359 |
| Datenträger zurückstellen  | 359 |
| Datenträger mit der Auslagerungsfunktion in ein volles Speicherarchiv zurückstellen                          | 360 |
| Private Datenträger und Arbeitsdatenträger   | 360 |
| Elementadressen für Speicherarchivspeicherschächte   | 361 |
| Datenträgerbestand verwalten   | 361 |
| Zugriff auf Datenträger steuern  | 362 |
| Bänder wiederverwenden   | 362 |
| Vorrat an Arbeitsdatenträgern bereithalten   | 363 |
| Vorrat an Datenträgern in einem Speicherarchiv mit WORM-Datenträgern bereithalten                            | 364 |
| Datenträgerbestand in automatisierten Speicherarchiven verwalten   | 365 |
| Status eines Datenträgers in einem automatisierten Speicherarchiv ändern                                     | 365 |
| Datenträger aus einem automatisierten Speicherarchiv entfernen   | 366 |
| Vorrat an Arbeitsdatenträgern in einem automatisierten Speicherarchiv bereithalten                           | 366 |
| Überlaufposition verwalten   | 367 |
| Datenträgerbestand prüfen  | 367 |
| Teilweise beschriebene Datenträger   | 368 |
| Operationen für gemeinsam genutzte Speicherarchive   | 368 |
| Serveranforderungen für Datenträger  | 369 |
| Bandlaufwerke verwalten  | 371 |
| Laufwerke aktualisieren  | 371 |
| Datenprüfung während Schreib-/Leseoperationen auf Band   | 372 |
| Unterstützte Laufwerke   | 373 |
| Schutz logischer Blöcke aktivieren und inaktivieren  | 373 |
| Schreib-/Leseoperationen für Datenträger   | 375 |
| Speicherpoolverwaltung in einem Bandarchiv   | 375 |
| Bandlaufwerke reinigen   | 375 |
| Methoden zum Reinigen von Bandlaufwerken   | 376 |
| Server für die Laufwerkreinigung in einem automatisierten Speicherarchiv konfigurieren                       | 377 |
| Reinigungskassette in ein Speicherarchiv zurückstellen   | 378 |
| Operationen mit Reinigungskassetten  | 336 |
| Fehler bei der Laufwerkreinigung beheben   | 379 |
| Bandlaufwerke ersetzen   | 379 |
| Bandlaufwerke löschen  | 379 |
| Laufwerke durch andere Laufwerke desselben Typs ersetzen   | 380 |
| Daten in Laufwerke umlagern, für die ein Upgrade durchgeführt wurde  | 381 |
| Server schützen  | 381 |
| Administratoren verwalten  | 381 |
| Kennwortanforderungen ändern   | 382 |
| Server auf dem System schützen   | 383 |
| Server stoppen und starten   | 383 |
| Server stoppen   | 384 |
| Server für Verwaltungs- oder Rekonfigurationstasks starten   | 384 |
| Durchführung eines Upgrades für den Server planen  | 385 |
| Vorbereitungen für einen Ausfall   | 386 |
| Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM | 386 |
| Plandatei zur Wiederherstellung nach einem Katastrophenfall  | 387 |
| Server und Clientdaten wiederherstellen  | 389 |
| Wiederherstellungsdrilloperationen   | 390 |
| Datenbank zurückschreiben  | 391 |

|   |            |
|---|------------|
| <b>Server</b>   | <b>392</b> |
| Neuerungen  | 393        |
| Aktualisierungen für das Operations Center  | 394        |
| Aktualisierungen für den Server   | 394        |
| Cloud-Tiering für die langfristige Datenaufbewahrung verwenden                                | 395        |
| IBM Spectrum Protect unter Linux Ubuntu Server LTS installieren                               | 395        |
| Sicherheit Ihrer Speicherumgebung erweitern   | 395        |
| Maßnahmen zum Schutz Ihres Systems vor Ransomware ergreifen                                   | 396        |
| V8.1 Releaseinformationen   | 396        |
| Server  | 396        |
| Operations Center   | 398        |
| Einheiten   | 399        |
| V8.1 Readme-Dateien für Fixpacks  | 400        |
| Installieren und Upgrade durchführen  | 401        |
| IBM Spectrum Protect-Lösung implementieren  | 401        |
| Verfügbarkeit von Funktionen nach Betriebssystem  | 401        |
| Server installieren und Upgrade durchführen   | 403        |
| AIX: Server installieren  | 403        |
| AIX: Installation des IBM Spectrum Protect-Servers planen                                     | 404        |
| AIX: Vorausgesetzte Kenntnisse  | 404        |
| AIX: Planung für optimale Leistung  | 405        |
| AIX: Planung für die Server-Hardware und das Betriebssystem                                   | 405        |
| AIX: Planung für Platten für die Serverdatenbank  | 408        |
| AIX: Planung für Platten für das Serverwiederherstellungsprotokoll                            | 410        |
| AIX: Planung für Containerspeicherpools   | 411        |
| AIX: Planung für Speicherpools des Typs DISK oder FILE  | 417        |
| AIX: Planung der Speichertechnologie  | 419        |
| AIX: Bewährte Verfahren bei der Installation  | 421        |
| AIX: Systemmindestvoraussetzungen für AIX-Systeme   | 422        |
| AIX: Kompatibilität des IBM Spectrum Protect-Servers mit anderen DB2-Produkten auf dem System | 424        |
| AIX: IBM Installation Manager   | 425        |
| AIX: Arbeitsblätter für Planungsdetails für den Server  | 426        |
| AIX: Kapazitätsplanung  | 426        |
| AIX: Speicherbedarf für die Datenbank   | 427        |
| AIX: Maximale Anzahl Dateien  | 427        |
| AIX: Speicherpoolkapazität  | 429        |
| AIX: Datenbankmanager und temporärer Speicherbereich  | 429        |
| AIX: Speicherplatzbedarf für das Wiederherstellungsprotokoll                                  | 430        |
| AIX: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll                    | 430        |
| AIX: Beispiel: Grundlegende Clientspeicheroperation   | 431        |
| AIX: Beispiel: Mehrere Clientsitzungen  | 432        |
| AIX: Beispiel: Operationen für gleichzeitiges Schreiben                                       | 434        |
| AIX: Beispiel: Grundlegende Clientspeicher- und Serveroperationen                             | 435        |
| AIX: Beispiel: Bedingungen mit extremen Abweichungen schätzen                                 | 435        |
| AIX: Beispiel: Datenbankgesamtsicherungen   | 435        |
| AIX: Beispiel: Datendeduplizierung  | 437        |
| AIX: Speicherbereich des Spiegels für aktive Protokolldateien                                 | 441        |
| AIX: Speicherbereich des Übernahmeverzeichnisses für Archivprotokolle                         | 441        |
| AIX: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen     | 441        |
| AIX: Rollbackdateien der Installation löschen   | 442        |
| AIX: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen | 443        |
| AIX: Rollbackdateien für die Installation mit der Befehlszeile löschen                        | 443        |
| AIX: Empfehlungen für die Serverbenennung   | 443        |
| AIX: Installationsverzeichnisse für den IBM Spectrum Protect-Server                           | 445        |
| AIX: Serverkomponenten installieren   | 445        |
| AIX: Installationspaket abrufen   | 446        |

|   |     |
|---|-----|
| AIX: Installationsassistenten verwenden   | 446 |
| AIX: Konsoleninstallationsassistenten verwenden   | 447 |
| AIX: Unbeaufsichtigter Modus  | 448 |
| AIX: Serversprachenpakete installieren  | 449 |
| AIX: Spracheinstellungen für den Server   | 449 |
| AIX: Sprachenpaket konfigurieren  | 450 |
| AIX: Sprachenpaket aktualisieren  | 450 |
| AIX: Die ersten Schritte nach der Installation von Version 8.1.3                                | 451 |
| AIX: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen                              | 452 |
| AIX: IBM Spectrum Protect-Server konfigurieren  | 453 |
| AIX: Konfigurationsassistenten verwenden  | 453 |
| AIX: Manuelle Konfigurationsschritte  | 453 |
| AIX: Serverinstanz erstellen  | 454 |
| AIX: Server- und Clientübertragung auf UNIX-Systemen konfigurieren                              | 455 |
| AIX: TCP/IP-Optionen definieren   | 456 |
| AIX: Shared Memory-Optionen definieren  | 456 |
| AIX: Secure Sockets Layer-Optionen definieren   | 457 |
| AIX: Datenbank und Protokoll formatieren  | 457 |
| AIX: Datenbankmanager für die Datenbanksicherung vorbereiten                                    | 458 |
| AIX: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren                        | 459 |
| AIX: Serverinstanz starten  | 460 |
| AIX: Zugriffsberechtigungen und Benutzergrenzwerte überprüfen                                   | 461 |
| AIX: Server mit der Instanzbenutzer-ID starten  | 462 |
| AIX: Server automatisch starten   | 462 |
| AIX: Server im Verwaltungsmodus starten   | 463 |
| AIX: Server stoppen   | 464 |
| AIX: Lizenzregistrierung  | 464 |
| AIX: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben                          | 465 |
| AIX: Mehrere Serverinstanzen auf einem System ausführen   | 465 |
| AIX: Server überwachen  | 466 |
| AIX: IBM Spectrum Protect-Fixpack installieren  | 467 |
| AIX: Von Version 8.1.3 auf eine vorherige Serverversion zurücksetzen                            | 468 |
| AIX: Referenz: DB2-Befehle für Serverdatenbanken  | 470 |
| AIX: IBM Spectrum Protect deinstallieren  | 473 |
| AIX: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren            | 474 |
| AIX: IBM Spectrum Protect im Konsolenmodus deinstallieren                                       | 474 |
| AIX: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren                             | 475 |
| AIX: IBM Spectrum Protect deinstallieren und erneut installieren                                | 475 |
| AIX: IBM Installation Manager deinstallieren  | 476 |
| Linux: Server installieren  | 477 |
| Linux: Installation des IBM Spectrum Protect-Servers planen                                     | 477 |
| Linux: Vorausgesetzte Kenntnisse  | 478 |
| Linux: Planung für optimale Leistung  | 478 |
| Linux: Planung für die Server-Hardware und das Betriebssystem                                   | 478 |
| Linux: Planung für Platten für die Serverdatenbank  | 482 |
| Linux: Planung für Platten für das Serverwiederherstellungsprotokoll                            | 483 |
| Linux: Planung für Containerspeicherpools   | 484 |
| Linux: Planung für Speicherpools des Typs DISK oder FILE  | 490 |
| Linux: Planung der Speichertechnologie  | 492 |
| Linux: Bewährte Verfahren bei der Installation  | 494 |
| Linux: Systemmindestvoraussetzungen für Linux-Systeme   | 495 |
| Linux: Servermindestvoraussetzungen für Linux x86_64  | 496 |
| Linux: Servermindestvoraussetzungen für Linux on System z                                       | 498 |
| Linux: Servermindestvoraussetzungen für Linux on Power Systems (Little Endian)                  | 500 |
| Linux: Kompatibilität des IBM Spectrum Protect-Servers mit anderen DB2-Produkten auf dem System | 502 |
| Linux: IBM Installation Manager   | 502 |
| Linux: Arbeitsblätter für Planungsdetails für den Server  | 503 |
| Linux: Kapazitätsplanung  | 503 |

|   |     |
|---|-----|
| Linux: Speicherbedarf für die Datenbank   | 504 |
| Linux: Maximale Anzahl Dateien  | 504 |
| Linux: Speicherpoolkapazität  | 506 |
| Linux: Datenbankmanager und temporärer Speicherbereich  | 506 |
| Linux: Speicherplatzbedarf für das Wiederherstellungsprotokoll                                  | 507 |
| Linux: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll                    | 507 |
| Linux: Beispiel: Grundlegende Clientspeicheroperation   | 508 |
| Linux: Beispiel: Mehrere Clientsitzungen  | 509 |
| Linux: Beispiel: Operationen für gleichzeitiges Schreiben                                       | 511 |
| Linux: Beispiel: Grundlegende Clientspeicher- und Serveroperationen                             | 512 |
| Linux: Beispiel: Bedingungen mit extremen Abweichungen schätzen                                 | 512 |
| Linux: Beispiel: Datenbankgesamtsicherungen   | 512 |
| Linux: Beispiel: Datendeduplizierung  | 514 |
| Linux: Speicherbereich des Spiegels für aktive Protokolldateien                                 | 518 |
| Linux: Speicherbereich des Übernahmeverzeichnis für Archivprotokolle                            | 518 |
| Linux: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen     | 518 |
| Linux: Rollbackdateien der Installation löschen   | 519 |
| Linux: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen | 520 |
| Linux: Rollbackdateien für die Installation mit der Befehlszeile löschen                        | 520 |
| Linux: Empfehlungen für die Serverbenennung   | 520 |
| Linux: Installationsverzeichnisse für den IBM Spectrum Protect-Server                           | 522 |
| Linux: Serverkomponenten installieren   | 522 |
| Linux: Installationspaket abrufen   | 523 |
| Linux: Installationsassistenten verwenden   | 523 |
| Linux: Konsoleninstallationsassistenten verwenden   | 524 |
| Linux: Unbeaufsichtigter Modus  | 525 |
| Linux: Serversprachenpakete installieren  | 525 |
| Linux: Spracheinstellungen für den Server   | 526 |
| Linux: Sprachenpaket konfigurieren  | 527 |
| Linux: Sprachenpaket aktualisieren  | 527 |
| Linux: Die ersten Schritte nach der Installation von Version 8.1.3                              | 527 |
| Linux: Kernelparameter für Linux-Systeme optimieren   | 528 |
| Linux: Parameter aktualisieren  | 529 |
| Linux: Wertvorschläge   | 529 |
| Linux: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen                            | 529 |
| Linux: IBM Spectrum Protect-Server konfigurieren  | 531 |
| Linux: Konfigurationsassistenten verwenden  | 531 |
| Linux: Manuelle Konfigurationsschritte  | 531 |
| Linux: Serverinstanz erstellen  | 532 |
| Linux: Server- und Clientübertragung auf UNIX-Systemen konfigurieren                            | 533 |
| Linux: TCP/IP-Optionen definieren   | 534 |
| Linux: Shared Memory-Optionen definieren  | 534 |
| Linux: Secure Sockets Layer-Optionen definieren   | 535 |
| Linux: Datenbank und Protokoll formatieren  | 535 |
| Linux: Datenbankmanager für die Datenbanksicherung vorbereiten                                  | 536 |
| Linux: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren                      | 537 |
| Linux: Serverinstanz starten  | 538 |
| Linux: Zugriffsberechtigungen und Benutzergrenzwerte überprüfen                                 | 539 |
| Linux: Server mit der Instanzbenutzer-ID starten  | 540 |
| Linux: Server auf Linux-Systemen automatisch starten  | 541 |
| Linux: Server im Verwaltungsmodus starten   | 542 |
| Linux: Server stoppen   | 543 |
| Linux: Lizenzregistrierung  | 543 |
| Linux: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben                        | 543 |
| Linux: Mehrere Serverinstanzen auf einem System ausführen                                       | 544 |
| Linux: Server überwachen  | 544 |
| Linux: IBM Spectrum Protect-Fixpack installieren  | 545 |
| Linux: Von Version 8.1.3 auf eine vorherige Serverversion zurücksetzen                          | 547 |

|   |     |
|---|-----|
| Linux: Referenz: DB2-Befehle für Serverdatenbanken  | 549 |
| Linux: IBM Spectrum Protect deinstallieren  | 552 |
| Linux: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren            | 553 |
| Linux: IBM Spectrum Protect im Konsolenmodus deinstallieren                                       | 553 |
| Linux: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren                             | 553 |
| Linux: IBM Spectrum Protect deinstallieren und erneut installieren                                | 554 |
| Linux: IBM Installation Manager deinstallieren  | 555 |
| Windows: Server installieren  | 555 |
| Windows: Installation des IBM Spectrum Protect-Servers planen                                     | 556 |
| Windows: Vorausgesetzte Kenntnisse  | 556 |
| Windows: Planung für optimale Leistung  | 556 |
| Windows: Planung für die Server-Hardware und das Betriebssystem                                   | 557 |
| Windows: Planung für Platten für die Serverdatenbank  | 560 |
| Windows: Planung für Platten für das Serverwiederherstellungsprotokoll                            | 562 |
| Windows: Planung für Containerspeicherpools   | 563 |
| Windows: Planung für Speicherpools des Typs DISK oder FILE  | 569 |
| Windows: Planung der Speichertechnologie  | 571 |
| Windows: Bewährte Verfahren bei der Installation  | 573 |
| Windows: Systemmindestvoraussetzungen für Windows-Systeme   | 574 |
| Windows: IBM Installation Manager   | 576 |
| Windows: Arbeitsblätter für Planungsdetails für den Server  | 577 |
| Windows: Kapazitätsplanung  | 577 |
| Windows: Speicherbedarf für die Datenbank   | 578 |
| Windows: Maximale Anzahl Dateien  | 578 |
| Windows: Speicherpoolkapazität  | 580 |
| Windows: Datenbankmanager und temporärer Speicherbereich  | 580 |
| Windows: Speicherplatzbedarf für das Wiederherstellungsprotokoll                                  | 581 |
| Windows: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll                    | 581 |
| Windows: Beispiel: Grundlegende Clientspeicheroperation   | 582 |
| Windows: Beispiel: Mehrere Clientsitzungen  | 583 |
| Windows: Beispiel: Operationen für gleichzeitiges Schreiben                                       | 585 |
| Windows: Beispiel: Grundlegende Clientspeicher- und Serveroperationen                             | 586 |
| Windows: Beispiel: Bedingungen mit extremen Abweichungen schätzen                                 | 586 |
| Windows: Beispiel: Datenbankgesamtsicherungen   | 586 |
| Windows: Beispiel: Dateneduplizierung   | 588 |
| Windows: Speicherbereich des Spiegels für aktive Protokolldateien                                 | 592 |
| Windows: Speicherbereich des Übernahmeverzeichnis für Archivprotokolle                            | 592 |
| Windows: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen     | 592 |
| Windows: Rollbackdateien der Installation löschen   | 593 |
| Windows: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen | 594 |
| Windows: Rollbackdateien für die Installation mit der Befehlszeile löschen                        | 594 |
| Windows: Empfehlungen für die Serverbenennung   | 594 |
| Windows: Installationsverzeichnisse für den IBM Spectrum Protect-Server                           | 596 |
| Windows: Serverkomponenten installieren   | 596 |
| Windows: Installationspaket abrufen   | 596 |
| Windows: Installationsassistenten verwenden   | 597 |
| Windows: Konsoleninstallationsassistenten verwenden   | 598 |
| Windows: Unbeaufsichtigter Modus  | 598 |
| Windows: Serversprachenpakete installieren  | 599 |
| Windows: Spracheinstellungen für den Server   | 599 |
| Windows: Sprachenpaket konfigurieren  | 600 |
| Windows: Sprachenpaket aktualisieren  | 600 |
| Windows: Die ersten Schritte nach der Installation von Version 8.1.3                              | 601 |
| Windows: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen                            | 602 |
| Windows: IBM Spectrum Protect-Server konfigurieren  | 603 |
| Windows: Konfigurationsassistenten verwenden  | 603 |
| Windows: Manuelle Konfigurationsschritte  | 604 |
| Windows: Serverinstanz erstellen  | 604 |

|  |     |
|--|-----|
| Windows: Datenübertragung auf Windows-Systemen konfigurieren   | 605 |
| Windows: TCP/IP-Optionen definieren  | 606 |
| Windows: Optionen für benannte Pipes definieren  | 607 |
| Windows: Secure Sockets Layer-Optionen definieren  | 607 |
| Windows: Datenbank und Protokoll formatieren   | 607 |
| Windows: Datenbankmanager für die Datenbanksicherung vorbereiten   | 608 |
| Windows: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren   | 609 |
| Windows: Serverinstanz auf Windows-Systemen starten  | 610 |
| Windows: Server für den Start als Windows-Dienst konfigurieren   | 610 |
| Windows: Server als Windows-Dienst starten   | 611 |
| Windows: Windows-Dienst manuell erstellen und konfigurieren  | 612 |
| Windows: Server im Vordergrund starten   | 612 |
| Windows: Dem Server zugeordnete Services auf Windows-Systemen  | 613 |
| Windows: Server im Verwaltungsmodus starten  | 613 |
| Windows: Server stoppen  | 614 |
| Windows: Lizenzregistrierung   | 614 |
| Windows: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben   | 614 |
| Windows: Mehrere Serverinstanzen auf einem System ausführen  | 615 |
| Windows: Server überwachen   | 615 |
| Windows: IBM Spectrum Protect-Fixpack installieren   | 616 |
| Windows: Von Version 8.1.3 auf eine vorherige Serverversion zurücksetzen   | 618 |
| Windows: Referenz: DB2-Befehle für Serverdatenbanken   | 620 |
| Windows: IBM Spectrum Protect deinstallieren   | 624 |
| Windows: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren   | 624 |
| Windows: IBM Spectrum Protect im Konsolenmodus deinstallieren  | 625 |
| Windows: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren  | 625 |
| Windows: IBM Spectrum Protect deinstallieren und erneut installieren   | 626 |
| Windows: IBM Installation Manager deinstallieren   | 627 |
| Upgrade des Servers auf Version 8.1 durchführen  | 627 |
| Upgrade auf Version 8.1 durchführen  | 628 |
| Planung des Upgrades   | 628 |
| Vorbereitung des Systems   | 629 |
| Server installieren und Upgrade prüfen   | 631 |
| Server-Upgrade in einer Clusterumgebung durchführen  | 635 |
| Upgrade von Version 6.3 oder Version 7.1 auf Version 8.1.3 in einer Clusterumgebung unter AIX mit einer gemeinsam genutzten Datenbankinstanz durchführen | 636 |
| Upgrade von Version 6.3 auf Version 8.1.3 in einer Clusterumgebung unter AIX mit separaten Datenbankinstanzen durchführen.                               | 638 |
| Upgrade auf Version 8.1.3 in einer Clusterumgebung unter Linux durchführen   | 640 |
| Upgrade von Version 6.3 oder Version 7.1 auf Version 8.1.3 in einer Clusterumgebung unter Windows durchführen  | 640 |
| Operations Center installieren und Operations Center-Upgrade durchführen   | 642 |
| Installation des Operations Center planen  | 643 |
| Systemvoraussetzungen für das Operations Center  | 644 |
| Voraussetzungen für den Computer des Operations Center   | 644 |
| Voraussetzungen für Hub- und Peripherieserver  | 645 |
| Tipps für das Entwerfen der Hub- und Peripherieserverkonfiguration   | 645 |
| Tipps für die Auswahl eines Hub-Servers  | 646 |
| Betriebssystemvoraussetzungen  | 647 |
| Voraussetzungen für den Web-Browser  | 647 |
| Voraussetzungen für die Sprache  | 648 |
| Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices   | 650 |
| Administrator-IDs, die für das Operations Center erforderlich sind   | 651 |
| IBM Installation Manager   | 651 |
| Prüfliste für die Installation   | 652 |
| Operations Center installieren   | 654 |
| Operations Center-Installationspaket abrufen   | 654 |
| Operations Center mit einem grafisch orientierten Assistenten installieren   | 655 |
| Operations Center im Konsolenmodus installieren  | 656 |

|   |     |
|---|-----|
| Operations Center im unbeaufsichtigten Modus installieren   | 656 |
| Upgrade des Operations Center   | 657 |
| Erste Schritte mit dem Operations Center  | 658 |
| Operations Center konfigurieren   | 658 |
| Hub-Server festlegen  | 659 |
| Peripherieserver hinzufügen   | 660 |
| E-Mail-Alerts an Administratoren senden   | 660 |
| Angepassten Text in die Anmeldeanzeige einfügen   | 662 |
| REST-Services aktivieren  | 662 |
| Sichere Kommunikation konfigurieren   | 663 |
| SSL-Kommunikation zwischen dem Operations Center und dem Hub-Server konfigurieren   | 663 |
| SSL-Kommunikation zwischen dem Hub-Server und einem Peripherieserver konfigurieren  | 665 |
| Kennwort für die Truststore-Datei des Operations Center zurücksetzen  | 666 |
| Web-Server starten und stoppen  | 668 |
| Operations Center öffnen  | 668 |
| Diagnoseinformationen mit dem Clientverwaltungsservice erfassen   | 669 |
| Clientverwaltungsservice mit einem grafisch orientierten Assistenten installieren   | 669 |
| Clientverwaltungsservice im unbeaufsichtigten Modus installieren  | 670 |
| Installation prüfen   | 671 |
| Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren   | 672 |
| Clientverwaltungsservice starten und stoppen  | 673 |
| Clientverwaltungsservice deinstallieren   | 673 |
| Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren  | 674 |
| Fehlerbehebung für die Operations Center-Installation   | 674 |
| Grafisch orientierter Installationsassistent kann auf einem AIX-System nicht gestartet werden                                   | 675 |
| Chinesische, japanische oder koreanische Schriftarten werden nicht ordnungsgemäß angezeigt                                      | 675 |
| Operations Center deinstallieren  | 675 |
| Operations Center mit einem grafisch orientierten Assistenten deinstallieren  | 675 |
| Operations Center im Konsolenmodus deinstallieren   | 676 |
| Operations Center im unbeaufsichtigten Modus deinstallieren   | 676 |
| Rollback zu einer vorherigen Version des Operations Center durchführen  | 677 |
| Server konfigurieren  | 677 |
| Server schützen   | 679 |
| Sicherheitskonzepte   | 680 |
| Administratoren verwalten   | 682 |
| Kennwortanforderungen ändern  | 682 |
| IBM Spectrum Protect auf dem System schützen  | 683 |
| Benutzerzugriff auf den Server einschränken   | 683 |
| Zugriff über Porteinschränkungen einschränken   | 684 |
| Speicherungsumgebung vor Ransomware-Attacken schützen   | 685 |
| Kommunikation schützen  | 685 |
| SSL- und TLS-Kommunikation  | 686 |
| Speicheragenten, Server, Clients und das Operations Center für die Verbindung zum Server unter Verwendung von SSL konfigurieren | 687 |
| Server zum Akzeptieren von SSL-Verbindungen konfigurieren   | 688 |
| Clients für die Kommunikation mit dem Server unter Verwendung von SSL konfigurieren   | 689 |
| Server für die Verbindung zu einem anderen Server unter Verwendung von SSL konfigurieren  | 689 |
| Operations Center für die Verbindung zum Hub-Server unter Verwendung von SSL konfigurieren                                      | 690 |
| Speicheragenten für die Verwendung von SSL konfigurieren  | 690 |
| Client für die Verbindung zu einem Speicheragenten unter Verwendung von SSL konfigurieren                                       | 691 |
| Benutzer mithilfe eines LDAP-Servers authentifizieren   | 691 |
| Clientdaten auf einen anderen Server replizieren  | 692 |
| Replikationskompatibilität  | 693 |
| Knotenreplikation aktivieren  | 693 |
| Daten in Verzeichniscontainerspeicherpools schützen   | 694 |
| Replikationseinstellungen ändern  | 695 |
| Unterschiedliche Aufbewahrungsmaßnahmen festlegen   | 696 |
| Clusterumgebungen konfigurieren   | 696 |

|   |     |
|---|-----|
| Übersicht über die Clusterumgebung  | 697 |
| AIX-Clusterumgebung   | 698 |
| Clusteranforderungen  | 698 |
| PowerHA-Übernahme und -Rückübertragung  | 699 |
| PowerHA SystemMirror for AIX installieren und konfigurieren                           | 699 |
| Cluster installieren und konfigurieren  | 700 |
| Konfiguration auf dem Primärknoten  | 700 |
| Konfiguration auf einem Sekundärknoten mit einer gemeinsam genutzten DB2-Instanz      | 700 |
| Konfiguration auf einem Sekundärknoten mit einer separaten DB2-Instanz                | 701 |
| Server auf einem Produktionsknoten installieren                                       | 702 |
| Client auf einem Produktionsknoten installieren                                       | 703 |
| Serverkonfiguration überprüfen  | 703 |
| Standby-Knoten konfigurieren  | 704 |
| Speichereinheiten für austauschbare Datenträger definieren                            | 704 |
| Cluster-Manager konfigurieren   | 705 |
| Fehlerbehebung in der PowerHA-Clusterumgebung   | 705 |
| Linux-Clusterumgebung   | 706 |
| Übersicht über eine Clusterumgebung mit zwei Knoten                                   | 706 |
| Zwei-Knoten-Topologie mit gemeinsam genutzter Platte                                  | 708 |
| Tivoli System Automation-Ressourcengruppen  | 709 |
| Cluster konfigurieren   | 710 |
| Voraussetzungen zum Konfigurieren einer Clusterumgebung                               | 710 |
| Komponenten installieren und konfigurieren  | 711 |
| Serverkomponenten installieren  | 711 |
| Primärknoten konfigurieren  | 711 |
| Sekundärknoten konfigurieren  | 712 |
| Tivoli System Automation installieren   | 713 |
| Kennsatz für die Mountpunkte erstellen  | 713 |
| Tivoli System Automation installieren und konfigurieren                               | 713 |
| Aktivierung der Clusterknoten für die Domäne vorbereiten                              | 714 |
| Datenträgergruppenressourcen konfigurieren  | 714 |
| Ressourcen konfigurieren, die sich nicht in einer Datenträgergruppe befinden          | 715 |
| Basismaßnahme aktivieren  | 715 |
| Mountpunkte zu Verzeichnissen hinzufügen  | 716 |
| Speicherressourcen konfigurieren  | 717 |
| Speicherpool hinzufügen   | 717 |
| Speicherpool löschen  | 718 |
| Mountpunkt löschen  | 718 |
| Upgrade für den Server durchführen, der mit Tivoli System Automation konfiguriert ist | 718 |
| Windows-Clusterumgebung   | 719 |
| Übersicht über die Microsoft-Failoverclusterumgebung                                  | 720 |
| Bandübernahme für Knoten in einem Cluster   | 721 |
| Planung für eine Clusterumgebung  | 721 |
| Arbeitsblatt für die Clusterkonfiguration   | 722 |
| Cluster-Hardware- und -Softwarekonfiguration planen                                   | 722 |
| IBM Spectrum Protect im Microsoft Failovercluster konfigurieren                       | 723 |
| IBM Spectrum Protect in einem Microsoft Failovercluster konfigurieren                 | 723 |
| Clusterressourcengruppe für einen virtuellen Server vorbereiten                       | 724 |
| IBM Spectrum Protect in einem Microsoft Failovercluster installieren                  | 724 |
| Server auf dem Primärknoten initialisieren  | 725 |
| Konfiguration in einem Microsoft Failovercluster überprüfen                           | 725 |
| Übernahme testen  | 725 |
| Clusterumgebung verwalten   | 726 |
| Vorhandenen Server in einen Cluster umlagern  | 726 |
| Server mit Sicherung und Zurückschreibung hinzufügen                                  | 727 |
| Virtuellen Server in einem Cluster verwalten  | 727 |
| Bandübernahme verwalten   | 727 |
| Fehlerbehebung mit dem Clusterprotokoll   | 728 |



|  |     |
|--|-----|
| Clients konfigurieren  | 728 |
| Clients hinzufügen   | 728 |
| Client-Software auswählen und Installation planen  | 729 |
| Regeln zum Sichern und Archivieren von Clientdaten angeben   | 730 |
| Maßnahmen anzeigen   | 731 |
| Maßnahmen editieren  | 731 |
| Sicherungs- und Archivierungsoperationen planen  | 733 |
| Clients registrieren   | 733 |
| Clients installieren und konfigurieren   | 734 |
| Client für die Ausführung geplanter Operationen konfigurieren                                      | 736 |
| Kommunikation durch eine Firewall konfigurieren  | 737 |
| Clientaktualisierungen planen  | 738 |
| Maßnahmen anpassen   | 739 |
| Maßnahmenkonzepte  | 740 |
| Aufbewahrung und Verfall von Sicherungsversionen   | 741 |
| Dateiverfall und Verfallsverarbeitung  | 742 |
| Beispiel: Aufbewahrung, wenn eine Maßnahme nur Zeitsteuerelemente verwendet                        | 743 |
| Beispiel: Aufbewahrung, wenn eine Maßnahme sowohl Versions- als auch Zeitsteuerelemente verwendet  | 743 |
| Interaktionen zwischen Maßnahmeneinstellungen  | 745 |
| Aktivierung der Maßnahme nach Aktualisierungen   | 746 |
| Maßnahme anpassen  | 748 |
| Maßnahme durch Kopieren einer vorhandenen Maßnahme erstellen                                       | 749 |
| Maßnahmendomäne erstellen  | 750 |
| Clientoperationen über Clientoptionsgruppen steuern  | 751 |
| Speicher konfigurieren   | 752 |
| Speicherpooltypen  | 752 |
| Datenduplizierungsoptionen   | 755 |
| Speichereinheiten konfigurieren  | 756 |
| Verzeichniscontainerspeicherpool konfigurieren   | 756 |
| Verzeichniscontainerspeicherpools auf Band kopieren  | 757 |
| Banddatenträger ohne DRM im Rotationsprinzip auslagern   | 759 |
| Schwellenwert für Datenträgerkonsolidierung ändern   | 760 |
| Banddatenträger in Containerkopierspeicherpools konsolidieren                                      | 760 |
| Bestimmen, ob Containerkopierspeicherpools für den Schutz vor Katastrophen verwendet werden können | 761 |
| Cloud-Containerspeicherpool konfigurieren  | 763 |
| Vorbereitungen für Amazon mit S3 treffen (Off-Premises)  | 765 |
| Vorbereitungen für eine Amazon S3-kompatible Einheit treffen                                       | 766 |
| Vorbereitungen für Microsoft Azure treffen (Off-Premises)  | 766 |
| Vorbereitungen für IBM Cloud Object Storage mit Swift treffen (Off-Premises)                       | 767 |
| Vorbereitungen für IBM Cloud Object Storage mit S3 treffen (Off-Premises)                          | 768 |
| Vorbereitungen für IBM Cloud Object Storage mit S3 treffen (On-Premises)                           | 769 |
| Vorbereitungen für OpenStack mit Swift treffen   | 770 |
| Daten für Cloud-Containerspeicherpools verschlüsseln   | 771 |
| Speicherregel für Cloud-Tiering definieren   | 771 |
| Leistung für Cloudobjektspeicher optimieren  | 772 |
| Containerspeicherpools verwalten   | 772 |
| Primären Speicherpool in einen Containerspeicherpool konvertieren                                  | 774 |
| Daten in einem Quellenspeicherpool bereinigen  | 775 |
| Speicherpoolcontainer prüfen   | 776 |
| Speichersystemvoraussetzungen und Reduzierung des Risikos fehlerhafter Daten                       | 776 |
| Speicherlösungen überwachen  | 777 |
| Prüfliste für tägliche Tasks   | 778 |
| Prüfliste für regelmäßige Tasks  | 785 |
| Lizenz Einhaltung überprüfen   | 791 |
| Systemstatus mithilfe von E-Mail-Berichten verfolgen   | 792 |
| Überwachungstools auswählen, konfigurieren und verwenden   | 793 |
| Operationen verwalten  | 795 |
| Serveroperationen verwalten  | 796 |

|   |     |
|---|-----|
| Server stoppen und starten  | 796 |
| Server stoppen  | 796 |
| Server für Verwaltungs- oder Rekonfigurationstasks starten                              | 797 |
| Bestandskapazität verwalten   | 798 |
| Speichernutzung und Prozessorauslastung verwalten                                       | 800 |
| Bestimmen, ob Aspera FASP die Datenübertragung in Ihrer Systemumgebung optimieren kann  | 800 |
| Durchführung eines Upgrades für den Server planen                                       | 802 |
| Geplante Aktivitäten optimieren   | 802 |
| Clientoperationen verwalten   | 803 |
| Bereich einer Clientsicherung ändern  | 804 |
| Fehler in Clientfehlerprotokollen auswerten   | 804 |
| Clientakzeptor stoppen und erneut starten   | 805 |
| Kennwörter zurücksetzen   | 806 |
| Clientknoten stilllegen   | 806 |
| Daten zum Freigeben von Speicherbereich inaktivieren                                    | 808 |
| Client-Upgrades verwalten   | 809 |
| Operations Center verwalten   | 810 |
| Peripherieserver hinzufügen und entfernen   | 810 |
| Peripherieserver hinzufügen   | 810 |
| Peripherieserver entfernen  | 811 |
| Web-Server starten und stoppen  | 811 |
| Assistenten für die Erstkonfiguration erneut starten                                    | 812 |
| Hub-Server ändern   | 813 |
| Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben                         | 813 |
| Virtuelle Bandarchive konfigurieren   | 814 |
| Hinweise zur Verwendung virtueller Bandarchive  | 814 |
| Speicherkapazität für virtuelle Bandarchive   | 815 |
| Laufwerkkonfiguration für virtuelle Bandarchive   | 815 |
| Virtuelles Bandarchiv Ihrer Umgebung hinzufügen   | 816 |
| Alle Laufwerke und Pfade für ein einzelnes Speicherarchiv definieren                    | 816 |
| Beispiel: SCSI-Speicherarchiv oder VTL mit einem einzigen Laufwerkeinheitentyp          | 817 |
| Beispiel: VTL oder SCSI-Speicherarchiv mit mehreren Laufwerkeinheitentypen              | 819 |
| NAS-Dateiserver schützen  | 820 |
| NDMP-Anforderungen  | 821 |
| Schnittstellen für NDMP-Operationen   | 822 |
| Datenformate für NDMP-Sicherungsoperationen   | 823 |
| Verwaltung von NDMP-Operationen   | 823 |
| NAS-Dateiserverknoten verwalten   | 823 |
| In NDMP-Operationen verwendete Einheiten zum Versetzen von Daten verwalten              | 825 |
| IBM Spectrum Protect-Laufwerk für NDMP-Operationen dedizieren                           | 826 |
| Speicherpoolverwaltung für NDMP-Operationen   | 826 |
| Inhaltsverzeichnisse verwalten  | 826 |
| Schließen inaktiver NDMP-Verbindungen verhindern  | 827 |
| TCP-Keepalive-Mechanismus aktivieren  | 827 |
| Inaktivitätsdauer für Verbindungen angeben (AIX, Linux und Windows)                     | 827 |
| IBM Spectrum Protect für NDMP-Operationen konfigurieren                                 | 828 |
| In einer Umgebung ohne Clustering   | 828 |
| IBM Spectrum Protect-Maßnahme für NDMP-Operationen konfigurieren                        | 829 |
| Maßnahmen für Sicherungen, die von einem IBM Spectrum Protect-Server eingeleitet werden | 830 |
| Maßnahmen für Sicherungen, die mit der Clientschnittstelle eingeleitet werden           | 831 |
| Festlegung der NAS-Sicherungsposition   | 831 |
| Bandarchive und -laufwerke für NDMP-Operationen   | 833 |
| Speicherarchivlaufwerknutzung bei der Sicherung auf NAS-Speicherarchiven bestimmen      | 833 |
| Bandarchiv für NDMP-Operationen konfigurieren   | 834 |
| Greifarme des Bandarchivs für NAS-Speicherarchive anschließen                           | 836 |
| Konfiguration 1: An den IBM Spectrum Protect-Server angeschlossenes SCSI-Speicherarchiv | 837 |
| Konfiguration 2: An den NAS-Dateiserver angeschlossenes SCSI-Speicherarchiv             | 838 |
| Konfiguration 3: An den IBM Spectrum Protect-Server angeschlossenes 349x-Speicherarchiv | 838 |

|   |     |
|---|-----|
| Konfiguration 4: An den IBM Spectrum Protect-Server angeschlossenes ACSLS-Speicherarchiv  | 839 |
| NAS-Knoten im IBM Spectrum Protect-Server registrieren  | 840 |
| Einheit zum Versetzen von Daten für einen NAS-Dateiserver definieren  | 840 |
| Pfade für NDMP-Operationen definieren   | 841 |
| Pfade zu Laufwerken definieren  | 841 |
| An einen Dateiserver und den IBM Spectrum Protect-Server angeschlossene Laufwerke   | 841 |
| Nur an einen Dateiserver angeschlossene Laufwerke   | 842 |
| Namen für an einen Dateiserver angeschlossene Einheiten abrufen   | 842 |
| Pfade zu Speicherarchiven definieren  | 844 |
| NDMP-Operationen planen   | 844 |
| Virtuelle Dateibereiche definieren  | 845 |
| Daten mit der Band-zu-Band-Kopierfunktion sichern   | 845 |
| Daten mit der Band-zu-Band-Kopierfunktion versetzen   | 845 |
| In einer NetApp-Clusterumgebung   | 846 |
| Clustergesamtsicherungen auf Bandeinheiten konfigurieren  | 847 |
| Clustergesamtsicherungen mit einem IBM Spectrum Protect-Server als Ziel konfigurieren   | 849 |
| Clusterteilsicherungen mit einem IBM Spectrum Protect-Server als Ziel konfigurieren   | 850 |
| IBM Spectrum Protect für die Optimierung von Clustersicherungen rekonfigurieren   | 852 |
| NAS-Dateiserver mithilfe von NDMP sichern und zurückschreiben   | 854 |
| NAS-Dateiserver: Sicherungen auf einem einzelnen IBM Spectrum Protect-Server  | 854 |
| NDMP-Dateiserver auf einem IBM Spectrum Protect-Server sichern  | 855 |
| Sicherung und Zurückschreibung auf Dateiebene für NDMP-Operationen  | 856 |
| Schnittstellen für Zurückschreibungsoperationen auf Dateiebene  | 857 |
| Zeichen des internationalen Zeichensatzes für NetApp-Dateiserver  | 857 |
| Zurückschreibungsoperationen auf Dateiebene aus einem Sicherungsimage auf Verzeichnisebene  | 858 |
| Sicherungs- und Zurückschreibungsoperationen auf Verzeichnisebene   | 858 |
| Sicherung und Zurückschreibung auf Verzeichnisebene für NDMP-Operationen  | 858 |
| Mit Momentaufnahmen sichern und zurückschreiben   | 858 |
| Sicherungs- und Zurückschreibungsoperationen mit der NetApp-Funktion 'SnapMirror to Tape'   | 859 |
| NDMP-Sicherungsoperationen mithilfe von in Celerra-Dateiserver integrierten Prüfpunkten   | 860 |
| NAS-Knoten replizieren  | 860 |
| Datenschutz mit dem NetApp-Feature SnapLock   | 861 |
| Wiederherstellung und das Feature SnapLock  | 862 |
| Aufbewahrungszeiträume  | 862 |
| Konfiguration des Features SnapLock für die ereignisgesteuerte Aufbewahrung   | 864 |
| Unterbrechungsfreier Datenschutz mit dem SnapLock-Feature   | 865 |
| SnapLock-Datenträger als IBM Spectrum Protect-WORM-FILE-Datenträger konfigurieren   | 865 |
| Daten reparieren und wiederherstellen   | 866 |
| Speicherpools mithilfe eines Zielreplikationsservers reparieren   | 866 |
| Speicherpools mithilfe von Datenträgern in Containerkopierspeicherpools reparieren  | 868 |
| Speicherpools in einer Umgebung mithilfe eines Replikationsservers und mithilfe von Datenträgern in Containerkopierspeicherpools reparieren | 870 |
| Speicherpools auf einem Zielreplikationsserver reparieren   | 871 |
| Reparatur nach einem Katastrophenfall   | 872 |
| Reparatur mithilfe von Datenträgern in Containerkopierspeicherpools   | 872 |
| Reparatur mithilfe eines Zielreplikationsservers  | 873 |
| Reparatur in einer Umgebung mithilfe eines Replikationsservers und mithilfe von Datenträgern in Containerkopierspeicherpools                | 874 |
| Beschädigten Banddatenträger im Containerkopierspeicherpool ersetzen  | 876 |
| Serverbefehle, -optionen und -dienstprogramme   | 876 |
| Server von der Befehlszeile aus verwalten   | 876 |
| Befehle mit dem Verwaltungsclient ausgeben  | 877 |
| Verwaltungsclient starten und stoppen   | 878 |
| Serveraktivitäten über den Verwaltungsclient überwachen   | 878 |
| Mounts für austauschbare Datenträger über den Verwaltungsclient überwachen  | 879 |
| Einzelne Befehle mit dem Verwaltungsclient verarbeiten  | 879 |
| Eine Serie von Befehlen des Verwaltungsclients verarbeiten  | 879 |
| Ausgabe von Befehlen formatieren  | 880 |
| Befehlsausgabe an einer angegebenen Position sichern  | 880 |

|   |     |
|---|-----|
| Verwaltungsclientoptionen   | 881 |
| Befehle im Operations Center ausgeben   | 883 |
| Befehle von der Serverkonsole ausgeben  | 883 |
| Verwaltungsbefehle eingeben   | 883 |
| Syntaxdiagramme lesen   | 884 |
| Fortsetzungszeichen für die Eingabe langer Befehle verwenden  | 887 |
| IBM Spectrum Protect-Objekte benennen   | 887 |
| Platzhalterzeichen zur Angabe von Objektnamen verwenden   | 888 |
| Beschreibungen in Schlüsselwortparametern angeben   | 889 |
| Befehlsverarbeitung steuern   | 889 |
| Serverbefehlsverarbeitung   | 890 |
| Hintergrundprozesse stoppen   | 890 |
| Tasks gleichzeitig auf mehreren Servern ausführen   | 890 |
| Berechtigungsklassen für Befehle  | 892 |
| Befehle, die die Systemberechtigung erfordern   | 893 |
| Befehle, die die Maßnahmenberechtigung erfordern  | 896 |
| Befehle, die die Speicherberechtigung erfordern   | 896 |
| Befehle, die die Bedienerberechtigung erfordern   | 897 |
| Befehle, die jeder Administrator ausgeben kann  | 897 |
| Verwaltungsbefehle  | 898 |
| ACCEPT DATE (Aktuelles Systemdatum akzeptieren)   | 902 |
| ACTIVATE POLICYSET (Neue Maßnahmengruppe aktivieren)  | 903 |
| ASSIGN DEFMGMTCLASS (Standardverwaltungsklasse zuordnen)  | 904 |
| AUDIT-Befehle   | 905 |
| AUDIT CONTAINER-Befehle   | 905 |
| Cloud-Container prüfen  | 905 |
| Verzeichniscontainer prüfen   | 909 |
| AUDIT LDAPDIRECTORY (LDAP-Verzeichnisserver prüfen)   | 913 |
| AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Kassettenarchiv prüfen)                               | 915 |
| AUDIT LIBVOLUME (Datenbankinformationen für einen Banddatenträger prüfen)   | 917 |
| AUDIT LICENSES (Serverspeicherbelegung prüfen)  | 918 |
| AUDIT VOLUME (Datenbankinformationen für Speicherpooldatenträger prüfen)  | 918 |
| BACKUP-Befehle  | 923 |
| BACKUP DB (Datenbank sichern)   | 923 |
| BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)                                    | 927 |
| BACKUP NODE (NAS-Knoten sichern)  | 929 |
| BACKUP STGPOOL (Daten eines primären Speicherpools in einem Kopierspeicherpool sichern)                           | 932 |
| BACKUP VOLHISTORY (Protokolldaten sequenzieller Datenträger speichern)  | 935 |
| BEGIN EVENTLOGGING (Ereignisprotokollierung beginnen)   | 936 |
| CANCEL-Befehle  | 938 |
| CANCEL EXPIRATION (Verfallsprozess abbrechen)   | 938 |
| CANCEL EXPORT (Ausgesetzte Exportoperation löschen)   | 938 |
| CANCEL PROCESS (Verwaltungsprozess abbrechen)   | 939 |
| CANCEL REPLICATION (Knotenreplikationsprozesse abbrechen)   | 941 |
| CANCEL REQUEST (Ladeanforderungen abbrechen)  | 941 |
| CANCEL RESTORE (Wiederanlauffähige Zurückschreibungssitzung abbrechen)  | 942 |
| CANCEL SESSION (Clientsitzungen abbrechen)  | 943 |
| CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)                                       | 944 |
| CHECKOUT LIBVOLUME (Speicherdatenträger aus Kassettenarchiv entnehmen)  | 949 |
| CLEAN DRIVE (Laufwerk reinigen)   | 954 |
| COMMIT (Festschreiben von Befehlen in einem Makro steuern)  | 955 |
| CONVERT STGPOOL (Speicherpool in einen Containerspeicherpool konvertieren)  | 955 |
| COPY-Befehle  | 957 |
| COPY ACTIVE DATA (Aktive Sicherungsdaten aus einem primären Speicherpool in einen Pool für aktive Daten kopieren) | 957 |
| COPY CLOPTSET (Clientoptionsgruppe kopieren)  | 960 |
| COPY DOMAIN (Maßnahmendomäne kopieren)  | 960 |
| COPY MGMTCLASS (Verwaltungsklasse kopieren)   | 962 |
| COPY POLICYSET (Maßnahmengruppe kopieren)   | 963 |

|  |      |
|--|------|
| COPY PROFILE (Profil kopieren)   | 964  |
| COPY SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl kopieren)                                      | 964  |
| COPY SCHEDULE (Kopie eines Zeitplans für Clientoperationen erstellen)                                    | 965  |
| COPY SCHEDULE (Kopie eines Zeitplans für Verwaltungsoperationen erstellen)                               | 966  |
| COPY SCRIPT (IBM Spectrum Protect-Prozedur kopieren)   | 966  |
| COPY SERVERGROUP (Server-Gruppe kopieren)  | 967  |
| DEACTIVATE DATA (Daten für einen Clientknoten inaktivieren)  | 968  |
| DECOMMISSION-Befehle   | 970  |
| DECOMMISSION NODE (Anwendungs- oder Systemknoten stilllegen)   | 970  |
| DECOMMISSION VM (Virtuelle Maschine stilllegen)  | 971  |
| DEFINE-Befehle   | 973  |
| DEFINE ALERTTRIGGER (Alertauslöser definieren)   | 973  |
| DEFINE ASSOCIATION (Clientknoten einem Zeitplan zuordnen)  | 975  |
| DEFINE BACKUPSET (Sicherungsgruppe definieren)   | 976  |
| DEFINE CLIENTACTION (Einmalige Clientaktion definieren)  | 979  |
| DEFINE CLIENTOPT (Option für eine Optionsgruppe definieren)  | 983  |
| DEFINE CLOPTSET (Clientoptionsgruppennamen definieren)   | 985  |
| DEFINE COLLOGROUP (Kollokationsgruppe definieren)  | 986  |
| DEFINE COLLOCMEMBER  | 987  |
| DEFINE COPYGROUP (Kopiengruppe definieren)   | 989  |
| DEFINE COPYGROUP (Sicherungskopiengruppe definieren)   | 990  |
| DEFINE COPYGROUP (Archivierungskopiengruppe definieren)  | 993  |
| DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren)  | 996  |
| DEFINE DEVCLASS (Einheitenklasse definieren)   | 998  |
| 3590   | 999  |
| 3592   | 1001 |
| 4MM  | 1007 |
| 8MM  | 1009 |
| Centera  | 1014 |
| DLT  | 1015 |
| Ecartridge   | 1019 |
| File   | 1024 |
| Generictape  | 1026 |
| LTO  | 1028 |
| NAS  | 1033 |
| Removablefile  | 1035 |
| Server   | 1037 |
| VolSafe  | 1038 |
| DEFINE DEVCLASS - z/OS Media-Server (Einheitenklasse für z/OS Media-Server definieren)                   | 1041 |
| 3590, für z/OS Media-Server  | 1042 |
| 3592, für z/OS Media-Server  | 1045 |
| ECARTRIDGE, für z/OS Media-Server  | 1049 |
| FILE, für z/OS Media-Server  | 1054 |
| DEFINE DOMAIN (Neue Maßnahmendomäne definieren)  | 1056 |
| DEFINE DRIVE (Laufwerk für Kassettenarchiv definieren)   | 1058 |
| DEFINE EVENTSERVER (Server als Ereignissserver definieren)   | 1061 |
| DEFINE GRPMEMBER (Server zu einer Servergruppe hinzufügen)   | 1062 |
| DEFINE LIBRARY (Kassettenarchiv definieren)  | 1063 |
| 349X   | 1064 |
| ACSLs  | 1067 |
| EXTERNAL   | 1069 |
| FILE   | 1070 |
| MANUAL   | 1071 |
| SCSI   | 1072 |
| SHARED   | 1076 |
| VTL  | 1076 |
| ZOSMEDIA   | 1079 |
| DEFINE MACHINE (Maschineninformationen für die Wiederherstellung nach einem Katastrophenfall definieren) | 1080 |

|   |      |
|---|------|
| DEFINE MACHNODEASSOCIATION (Knoten einer Maschine zuordnen)                   | 1081 |
| DEFINE MGMTCLASS (Verwaltungs-kategorie definieren)                           | 1082 |
| DEFINE NODEGROUP (Knotengruppe definieren)                                    | 1084 |
| DEFINE NODEGROUPMEMBER (Eintrag in der Knotengruppe definieren)               | 1085 |
| DEFINE PATH (Pfad definieren)   | 1086 |
| Ziel ist ein Laufwerk   | 1086 |
| Ziel ist ein Kassettenarchiv  | 1091 |
| Ziel ist ein ZOSMEDIA-Kassettenarchiv   | 1094 |
| DEFINE POLICYSET (Maßnahmengruppe definieren)                                 | 1095 |
| DEFINE PROFASSOCIATION (Profilzuordnung definieren)                           | 1096 |
| DEFINE PROFILE (Profil definieren)  | 1100 |
| DEFINE RECMEDMACHASSOCIATION (Wiederh.-Datenträger Maschine zuordnen)         | 1101 |
| DEFINE RECOVERYMEDIA (Wiederherstellungsdatenträger definieren)               | 1101 |
| DEFINE SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl definieren)       | 1103 |
| DEFINE SCHEDULE (Clientzeitplan definieren)                                   | 1103 |
| DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)             | 1113 |
| DEFINE SCRATCHPADENTRY (Scratchpadeintrag definieren)                         | 1120 |
| DEFINE SCRIPT (IBM Spectrum Protect-Prozedur definieren)                      | 1121 |
| DEFINE SERVER (Server für Übertragung zwischen Servern definieren)            | 1123 |
| DEFINE SERVERGROUP (Server-Gruppe definieren)                                 | 1129 |
| DEFINE SPACETRIGGER (Speicherbereichsauslöser definieren)                     | 1130 |
| DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)       | 1132 |
| DEFINE STGPOOL (Speicherpool definieren)                                      | 1135 |
| Cloud-Containerspeicherpool   | 1137 |
| Verzeichniscontainerspeicherpool  | 1141 |
| Containerkopierspeicherpool   | 1144 |
| Primärer Pool mit wahlfreiem Zugriff  | 1147 |
| Primärer Pool mit sequenziellem Zugriff                                       | 1154 |
| Kopienpool  | 1167 |
| Pool für aktive Daten   | 1173 |
| DEFINE STGPOOLDIRECTORY (Speicherpoolverzeichnis definieren)                  | 1179 |
| DEFINE STGRULE (Speicherregel für Speicherpools definieren)                   | 1180 |
| DEFINE SUBSCRIPTION (Profilsubskription definieren)                           | 1182 |
| DEFINE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs definieren) | 1183 |
| DEFINE VOLUME (Datenträger in einem Speicherpool definieren)                  | 1185 |
| DELETE-Befehle  | 1191 |
| DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)             | 1192 |
| DELETE ASSOCIATION (Knotenzuordnung zu einem Zeitplan löschen)                | 1192 |
| DELETE BACKUPSET (Sicherungsgruppe löschen)                                   | 1193 |
| DELETE CLIENTOPT (Option in einer Optionsgruppe löschen)                      | 1197 |
| DELETE CLOPTSET (Clientoptionsgruppe löschen)                                 | 1198 |
| DELETE COLLOGGROUP (Kollokationsgruppe löschen)                               | 1198 |
| DELETE COLLOGMEMBER (Kollokationsgruppenmitglied löschen)                     | 1199 |
| DELETE COPYGROUP (Sicherungs- oder Archivierungskopiengruppe löschen)         | 1202 |
| DELETE DATAMOVER (Einheit zum Versetzen von Daten löschen)                    | 1203 |
| DELETE DEDUPSTATS (Dateneduplizierungsstatistikdaten löschen)                 | 1203 |
| DELETE DEVCLASS (Einheitenklasse löschen)                                     | 1206 |
| DELETE DOMAIN (Maßnahmendomäne löschen)                                       | 1207 |
| DELETE DRIVE (Laufwerk aus einem Kassettenarchiv löschen)                     | 1208 |
| DELETE EVENT (Ereignissätze löschen)  | 1208 |
| DELETE EVENTSERVER (Definition des Ereignisservers löschen)                   | 1210 |
| DELETE FILESPACE (Clientknotendaten aus dem Server löschen)                   | 1211 |
| DELETE GRPMEMBER (Server aus einer Servergruppe löschen)                      | 1214 |
| DELETE LIBRARY (Kassettenarchiv löschen)                                      | 1214 |
| DELETE MACHINE (Maschineninformationen löschen)                               | 1215 |
| DELETE MACHNODEASSOCIATION (Zuordnung zwischen Maschine und Knoten löschen)   | 1216 |
| DELETE MGMTCLASS (Verwaltungs-kategorie löschen)                              | 1217 |
| DELETE NODEGROUP (Knotengruppe löschen)                                       | 1218 |

|   |      |
|---|------|
| DELETE NODEGROUPMEMBER (Eintrag aus der Knotengruppe löschen)   | 1218 |
| DELETE PATH (Pfad löschen)  | 1219 |
| DELETE POLICYSET (Maßnahmengruppe löschen)  | 1220 |
| DELETE PROFASSOCIATION (Profilzuordnung löschen)  | 1221 |
| DELETE PROFILE (Profil löschen)   | 1223 |
| DELETE RECMEDMACHASSOCIATION (Zuordnung Datenträger/Maschine löschen)                                   | 1225 |
| DELETE RECOVERYMEDIA (Wiederherstellungsdatenträger löschen)  | 1225 |
| DELETE SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl löschen)                                    | 1226 |
| DELETE SCHEDULE (Clientzeitplan löschen)  | 1226 |
| DELETE SCHEDULE (Verwaltungszeitplan löschen)   | 1227 |
| DELETE SCRATCHPADENTRY (Scratchpadeintrag löschen)  | 1227 |
| DELETE SCRIPT (Befehlszeilen aus Prozedur oder gesamte Prozedur löschen)                                | 1228 |
| DELETE SERVER (Server-Definition löschen)   | 1229 |
| DELETE SERVERGROUP (Servergruppe löschen)   | 1230 |
| DELETE SPACETRIGGER (Speicherbereichsauslöser für Speicherpool löschen)                                 | 1230 |
| DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)                                    | 1231 |
| DELETE STGPOOL (Speicherpool löschen)   | 1232 |
| DELETE STGPOOLDIRECTORY (Speicherpoolverzeichnis löschen)   | 1233 |
| DELETE STGRULE (Speicherregeln für Speicherpools löschen)   | 1234 |
| DELETE SUBSCRIBER (Subskriptionen aus Konfigurationsmanagerdatenbank löschen)                           | 1235 |
| DELETE SUBSCRIPTION (Profilsubskription löschen)  | 1235 |
| DELETE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs löschen)                              | 1236 |
| DELETE VOLHISTORY (Protokolldaten sequenzieller Datenträger löschen)                                    | 1237 |
| DELETE VOLUME (Speicherpooldatenträger löschen)   | 1241 |
| DISABLE-Befehle   | 1243 |
| DISABLE EVENTS (Ereignisse für Ereignisprotokollierung inaktivieren)                                    | 1243 |
| DISABLE REPLICATION (Verarbeitung abgehender Replikation auf einem Server verhindern)                   | 1246 |
| DISABLE SESSIONS (Verhindern, dass neue Sitzungen auf IBM Spectrum Protect zugreifen)                   | 1246 |
| DISMOUNT-Befehl   | 1248 |
| DISPLAY OBJNAME (Vollständigen Objektnamen anzeigen)  | 1248 |
| ENABLE-Befehle  | 1249 |
| ENABLE EVENTS (Server- oder Clientereignisse zum Protokollieren aktivieren)                             | 1249 |
| ENABLE REPLICATION (Verarbeitung abgehender Replikation auf einem Server ermöglichen)                   | 1251 |
| ENABLE SESSIONS (Benutzeraktivität auf dem Server wiederaufnehmen)                                      | 1252 |
| ENCRYPT STGPOOL (Daten in einem Speicherpool verschlüsseln)   | 1254 |
| END EVENTLOGGING (Ereignisprotokollierung stoppen)  | 1255 |
| EXPIRE INVENTORY (Datenträgerbestandsverfall manuell starten)   | 1256 |
| EXPORT-Befehle  | 1259 |
| EXPORT ADMIN (Administratorinformationen exportieren)   | 1260 |
| EXPORT ADMIN (Administratordefinitionen auf sequenzielle Datenträger exportieren)                       | 1261 |
| EXPORT ADMIN (Administratorinformationen direkt auf einen anderen Server exportieren)                   | 1264 |
| EXPORT NODE (Clientknoteninformationen exportieren)   | 1265 |
| EXPORT NODE (Knotendefinitionen auf sequenzielle Datenträger exportieren)                               | 1267 |
| EXPORT NODE (Knotendefinitionen oder Dateidaten direkt auf einen anderen Server exportieren)            | 1274 |
| EXPORT POLICY (Maßnahmeninformationen exportieren)  | 1281 |
| EXPORT POLICY (Maßnahmeninformationen auf sequenzielle Datenträger exportieren)                         | 1282 |
| EXPORT POLICY (Eine Maßnahme direkt auf einen anderen Server exportieren)                               | 1284 |
| EXPORT SERVER (Serverinformationen exportieren)   | 1285 |
| EXPORT SERVER (Server auf sequenzielle Datenträger exportieren)   | 1287 |
| EXPORT SERVER (Serversteuerungsinformationen und Clientdateidaten auf einen anderen Server exportieren) | 1293 |
| EXTEND DBSPACE (Speicherbereich für die Datenbank erhöhen)  | 1299 |
| GENERATE-Befehle  | 1301 |
| GENERATE BACKUPSET (Sicherungsgruppe mit Daten des Clients für Sichern/Archivieren generieren)          | 1301 |
| GENERATE BACKUPSETTOC (Inhaltsverzeichnis für eine Sicherungsgruppe generieren)                         | 1307 |
| GENERATE DEDUPSTATS (Dateneduplizierungsstatistikdaten generieren)                                      | 1309 |
| GRANT-Befehle   | 1311 |
| GRANT AUTHORITY (Administratorberechtigung hinzufügen)  | 1311 |
| GRANT PROXYNODE (Proxyberechtigung einem Clientknoten erteilen)   | 1314 |

|   |      |
|---|------|
| HALT (Server abschalten)  | 1315 |
| HELP (Hilfe für Befehle und Fehlernachrichten anfordern)  | 1316 |
| IDENTIFY DUPLICATES (Doppelte Daten in einem Speicherpool identifizieren)   | 1317 |
| Befehle IMPORT  | 1320 |
| IMPORT ADMIN (Administratorinformationen importieren)   | 1320 |
| IMPORT NODE (Clientknoteninformationen importieren)   | 1323 |
| IMPORT POLICY (Maßnahmeninformationen importieren)  | 1329 |
| IMPORT SERVER (Serverinformationen importieren)   | 1331 |
| INSERT MACHINE (Maschinenkenndaten oder Wiederh.-Anweisungen einfügen)  | 1335 |
| ISSUE MESSAGE (Nachricht aus einem Server-Script ausgeben)  | 1336 |
| LABEL LIBVOLUME (Datenträger im Kassettenarchiv Kennsatz zuordnen)  | 1337 |
| LOAD DEFALERTTRIGGERS (Standardgruppe von Alertauslösern laden)   | 1343 |
| LOCK-Befehle  | 1344 |
| LOCK ADMIN (Administrator sperren)  | 1344 |
| LOCK NODE (Clientknoten sperren)  | 1345 |
| LOCK PROFILE (Profil sperren)   | 1346 |
| MACRO (Makro aufrufen)  | 1347 |
| MIGRATE STGPOOL (Speicherpool in nächsten Speicherpool umlagern)  | 1348 |
| MOVE-Befehle  | 1350 |
| MOVE CONTAINER (Container versetzen)  | 1350 |
| MOVE DATA (Dateien auf einem Speicherpooldatenträger versetzen)   | 1351 |
| MOVE DRMEDIA (DRM-Datenträger aus- und einlagern)   | 1354 |
| MOVE GRPMEMBER (Servergruppenteil versetzen)  | 1367 |
| MOVE MEDIA (Speicherpooldatenträger mit sequenziellem Zugriff versetzen)  | 1368 |
| MOVE NODEDATA (Daten nach Knoten in einem Speicherpool mit sequenziellem Zugriff versetzen)                           | 1374 |
| Dateibereiche für einen oder mehrere Knoten oder eine Kollokationsgruppe  | 1375 |
| Ausgewählte Dateibereiche eines einzelnen Knotens   | 1377 |
| NOTIFY SUBSCRIBERS (Verwaltete Server auf Profilaktualisierung hinweisen)   | 1380 |
| PERFORM LIBACTION (Alle Laufwerke und Pfade für ein Kassettenarchiv definieren oder löschen)                          | 1381 |
| PING SERVER (Verbindung zwischen Servern testen)  | 1384 |
| PREPARE (Wiederherstellungsplandatei erstellen)   | 1385 |
| PROTECT STGPOOL (Daten schützen, die zu einem Speicherpool gehören)   | 1391 |
| QUERY-Befehle   | 1395 |
| QUERY ACTLOG (Aktivitätenprotokoll abfragen)  | 1397 |
| QUERY ADMIN (Administratorinformationen anzeigen)   | 1402 |
| QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)   | 1405 |
| QUERY ALERTSTATUS (Status eines Alert abfragen)   | 1406 |
| QUERY ASSOCIATION (Zuordnung zwischen Clientknoten und Zeitplan abfragen)   | 1410 |
| QUERY AUDITOCUPANCY (Speicherauslastung des Clientknotens abfragen)   | 1411 |
| QUERY BACKUPSET (Sicherungsgruppe abfragen)   | 1413 |
| QUERY BACKUPSETCONTENTS (Inhalt einer Sicherungsgruppe abfragen)  | 1417 |
| QUERY CLEANUP (Bereinigung abfragen, die in einem Quellenspeicherpool erforderlich ist)                               | 1418 |
| QUERY CLOPTSET (Clientoptionsgruppe abfragen)   | 1420 |
| QUERY COLLOGROUP (Kollokationsgruppe abfragen)  | 1421 |
| QUERY CONTAINER (Containerinformationen anzeigen)   | 1423 |
| QUERY CONTENT (Inhalt eines Speicherpooldatenträgers abfragen)  | 1427 |
| QUERY CONVERSION (Konvertierungsstatus eines Speicherpools abfragen)  | 1432 |
| QUERY COPYGROUP (Kopiengruppen abfragen)  | 1433 |
| QUERY DAMAGED (Beschädigte Daten in einem Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool abfragen) | 1437 |
| QUERY DATAMOVER (Definitionen der Einheit zum Versetzen von Daten anzeigen)   | 1440 |
| QUERY DB (Datenbankinformationen anzeigen)  | 1442 |
| QUERY DBSPACE (Datenbankspeicherbereich anzeigen)   | 1444 |
| QUERY DEDUPSTATS (Datendeduplizierungsstatistikdaten abfragen)  | 1445 |
| QUERY DEVCLASS (Informationen über Einheitenklassen anzeigen)   | 1450 |
| QUERY DIRSPACE (Speichernutzung von FILE-Verzeichnissen abfragen)   | 1454 |
| QUERY DOMAIN (Maßnahmendomäne abfragen)   | 1455 |
| QUERY DRIVE (Informationen über ein Laufwerk abfragen)  | 1457 |



|  |      |
|--|------|
| QUERY DRMEDIA (Fehlerbehebungsdatenträger abfragen)  | 1460 |
| QUERY DRMSTATUS (Disaster Recovery Manager-Systemparameter abfragen)   | 1467 |
| QUERY ENABLED (Aktivierte Ereignisse abfragen)   | 1469 |
| QUERY EVENT (Geplante und abgeschlossene Ereignisse abfragen)  | 1471 |
| QUERY EVENT (Clientzeitpläne anzeigen)   | 1471 |
| QUERY EVENT (Ereignisse für Verwaltungszeitpläne anzeigen)   | 1477 |
| QUERY EVENTRULES (Regeln für Server- oder Clientereignisse abfragen)   | 1480 |
| QUERY EVENTSERVER (Ereignisserver abfragen)  | 1482 |
| QUERY EXPORT (Aktive oder ausgesetzte Exportoperationen abfragen)  | 1482 |
| QUERY EXTENTUPDATES (Aktualisierte Datenbereiche abfragen)   | 1487 |
| QUERY FILESPACE (Dateibereiche abfragen)   | 1488 |
| QUERY LIBRARY (Kassettenarchiv abfragen)   | 1493 |
| QUERY LIBVOLUME (Datenträger im Kassettenarchiv abfragen)  | 1496 |
| QUERY LICENSE (Lizenzinformationen anzeigen)   | 1498 |
| QUERY LOG (Informationen zum Wiederherstellungsprotokoll anzeigen)   | 1500 |
| QUERY MACHINE (Maschineninformationen abfragen)  | 1502 |
| QUERY MEDIA (Speicherpooldatenträger mit sequenziellem Zugriff abfragen)   | 1504 |
| QUERY MGMTCLASS (Verwaltungsklasse abfragen)   | 1509 |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen) | 1512 |
| QUERY MONITORSTATUS (Überwachungsstatus abfragen)  | 1514 |
| QUERY MOUNT (Informationen zu bereitgestellten Datenträgern mit sequenziellem Zugriff anzeigen)                  | 1517 |
| QUERY NASBACKUP (NAS-Sicherungsimages abfragen)  | 1519 |
| QUERY NODE (Knoten abfragen)   | 1522 |
| QUERY NODEDATA (Clientdaten auf Datenträgern abfragen)   | 1531 |
| QUERY NODEGROUP (Knotengruppe abfragen)  | 1533 |
| QUERY OCCUPANCY (Clientdateibereiche in Speicherpools abfragen)  | 1535 |
| QUERY OPTION (Serveroptionen abfragen)   | 1538 |
| QUERY PATH (Pfaddefinition anzeigen)   | 1539 |
| QUERY POLICYSET (Maßnahmengruppe abfragen)   | 1542 |
| QUERY PROCESS (Serverprozesse abfragen)  | 1544 |
| QUERY PROFILE (Profil abfragen)  | 1548 |
| QUERY PROTECTSTATUS (Status des Speicherpoolschutzes abfragen)   | 1550 |
| QUERY PROXYNODE (Proxyberechtigung für einen Clientknoten abfragen)  | 1552 |
| QUERY PVUESTIMATE (Prozessor-Value-Unit-Schätzung anzeigen)  | 1553 |
| QUERY RECOVERYMEDIA (Wiederherstellungsdatenträger abfragen)   | 1556 |
| QUERY REPLICATION (Knotenreplikationsprozesse abfragen)  | 1558 |
| QUERY REPLNODE (Informationen zum Replikationsstatus für einen Clientknoten anzeigen)                            | 1566 |
| QUERY REPLRULE (Replikationsregeln abfragen)   | 1568 |
| QUERY REPLSERVER (Replikationsserver abfragen)   | 1570 |
| QUERY REQUEST (Anstehende Ladeanforderungen abfragen)  | 1572 |
| QUERY RESTORE (Wiederanlauffähige Zurückschreibungssitzungen abfragen)   | 1573 |
| QUERY RPFCONTENT (Inhalt der auf Zielsever gespeicherten Plandatei abfragen)                                     | 1575 |
| QUERY RPFFILE (Auf Zielsever gespeicherte Infos über Plandateien abfragen)                                       | 1576 |
| QUERY SAN (Einheiten in dem SAN abfragen)  | 1578 |
| QUERY SCHEDULE (Zeitpläne abfragen)  | 1580 |
| QUERY SCHEDULE (Clientzeitpläne abfragen)  | 1580 |
| QUERY SCHEDULE (Verwaltungszeitplan abfragen)  | 1583 |
| QUERY SCRATCHPADENTRY (Scratchpadeintrag abfragen)   | 1585 |
| QUERY SCRIPT (IBM Spectrum Protect-Prozeduren abfragen)  | 1587 |
| QUERY SERVER (Server abfragen)   | 1589 |
| QUERY SERVERGROUP (Servergruppe abfragen)  | 1592 |
| QUERY SESSION (Clientsitzungen abfragen)   | 1593 |
| QUERY SHREDSTATUS (Status für Schreddern abfragen)   | 1597 |
| QUERY SPACETRIGGER (Speicherbereichsauslöser abfragen)   | 1598 |
| QUERY STATUS (Systemparameter abfragen)  | 1600 |
| QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)  | 1608 |
| QUERY STGPOOL (Speicherpools abfragen)   | 1610 |
| QUERY STGPOOLDIRECTORY (Speicherpoolverzeichnis abfragen)  | 1624 |

|   |      |
|---|------|
| QUERY STGRULE (Speicherregelinformationen anzeigen)   | 1626 |
| QUERY SUBSCRIBER (Informationen zu Subskribenten anzeigen)  | 1628 |
| QUERY SUBSCRIPTION (Subskriptionsinformationen anzeigen)  | 1629 |
| QUERY SYSTEM (Systemkonfiguration und Kapazität abfragen)   | 1630 |
| QUERY TAPEALERTMSG (Status des Befehls SET TAPEALERTMSG anzeigen)   | 1631 |
| QUERY TOC (Inhaltsverzeichnis für ein Sicherungsimagen anzeigen)  | 1632 |
| QUERY VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs abfragen)  | 1634 |
| QUERY VOLHISTORY (History-Daten für sequentielle Datenträger anzeigen)  | 1635 |
| QUERY VOLUME (Speicherpooldatenträger abfragen)   | 1641 |
| QUIT (Interaktiven Modus des Verwaltungsclient verlassen)   | 1647 |
| RECLAIM STGPOOL (Datenträger im Speicherpool mit sequenziellem Zugriff wiederherstellen)                              | 1648 |
| RECONCILE VOLUMES (Unterschiede abstimmen)  | 1650 |
| REGISTER-Befehle  | 1651 |
| REGISTER ADMIN (Administrator-ID registrieren)  | 1652 |
| REGISTER LICENSE (Neue Lizenz registrieren)   | 1655 |
| REGISTER NODE (Knoten registrieren)   | 1656 |
| REMOVE-Befehle  | 1671 |
| REMOVE ADMIN (Benutzer-ID mit Administratorberechtigung löschen)  | 1671 |
| REMOVE DAMAGED (Beschädigte Daten aus einem Quellenspeicherpool entfernen)  | 1672 |
| REMOVE NODE (Knoten oder zugehörigen Maschinenknoten löschen)   | 1673 |
| REMOVE REPLNODE (Clientknoten aus Replikation entfernen)  | 1674 |
| REMOVE REPLSERVER (Replikationsserver entfernen)  | 1675 |
| RENAME-Befehle  | 1676 |
| RENAME ADMIN (Administrator umbenennen)   | 1676 |
| RENAME FILESPACE (Clientdateibereich auf dem Server umbenennen)   | 1677 |
| RENAME NODE (Knoten umbenennen)   | 1680 |
| RENAME SCRIPT (IBM Spectrum Protect-Prozedur umbenennen)  | 1681 |
| RENAME SERVERGROUP (Servergruppe umbenennen)  | 1682 |
| RENAME STGPOOL (Den Namen eines Speicherpools ändern)   | 1682 |
| REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)  | 1683 |
| REPLICATE NODE (Daten in Dateibereichen replizieren, die zu einem Clientknoten gehören)                               | 1685 |
| REPLY (Verarbeitung einer Anforderung fortsetzen)   | 1693 |
| RESET PASSEXP (Kennwortablaufdauer zurücksetzen)  | 1693 |
| RESTART EXPORT (Ausgesetzte Exportoperation erneut starten)   | 1694 |
| RESTORE-Befehle   | 1695 |
| RESTORE NODE (NAS-Knoten zurückschreiben)   | 1695 |
| RESTORE STGPOOL (Speicherpooldaten aus einem Kopienpool oder einem Pool für aktive Daten zurückschreiben)             | 1700 |
| RESTORE VOLUME (Daten primärer Datenträger aus Kopienpool oder Pool für aktive Daten zurückschreiben)                 | 1703 |
| REVOKE-Befehle  | 1706 |
| REVOKE AUTHORITY (Administratorberechtigung entziehen)  | 1706 |
| REVOKE PROXYNODE (Proxyberechtigung für einen Clientknoten entziehen)   | 1708 |
| ROLLBACK (Nicht festgeschriebene Änderungen in einem Makro rückgängig machen)   | 1709 |
| RUN (IBM Spectrum Protect-Prozedur ausführen)   | 1710 |
| SELECT (SQL-Abfrage für die IBM Spectrum Protect-Datenbank ausführen)   | 1712 |
| SET-Befehle   | 1720 |
| SET ACCOUNTING (Abrechnungssätze aktivieren/inaktivieren)   | 1721 |
| SET ACTLOGRETENTION (Aufbewahrungsdauer für das Aktivitätenprotokoll definieren)                                      | 1722 |
| SET ALERTACTIVEDURATION (Dauer eines aktiven Alert definieren)  | 1723 |
| SET ALERTCLOSEDDURATION (Dauer eines geschlossenen Alert definieren)  | 1724 |
| SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren)                      | 1724 |
| SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)  | 1725 |
| SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)  | 1726 |
| SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)   | 1727 |
| SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren) | 1727 |
| SET ALERTINACTIVEDURATION (Dauer eines inaktiven Alert definieren)  | 1728 |
| SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)  | 1729 |
| SET ALERTUPDATEINTERVAL (Häufigkeit definieren, mit der der Alertmonitor Alerts aktualisiert und bereinigt)           | 1729 |

|  |      |
|--|------|
| SET ARCHIVERETENTIONPROTECTION (Aufbewahrungsschutz für Daten aktivieren)  | 1730 |
| SET ARREPLRULEDEFAULT (Serverreplikationsregel für Archivierungsdaten definieren)                                      | 1731 |
| SET BKREPLRULEDEFAULT (Serverreplikationsregel für Sicherungsdaten definieren)   | 1732 |
| SET CLIENTACTDURATION (Verweildauer für Clientaktion definieren)   | 1734 |
| SET CONFIGMANAGER (Konfigurationsmanager angeben)  | 1735 |
| SET CONFIGREFRESH (Aktualisierung der Konfiguration verwalteter Server definieren)                                     | 1735 |
| SET CONTEXTMESSAGING (Anzeigen von Nachrichtenkontext aktivieren oder inaktivieren)                                    | 1736 |
| SET CPUINFOREFRESH (Aktualisierungsintervall für Informationssuche auf Client-Workstation)                             | 1737 |
| SET CROSSDEFINE (Querdefinition von Servern angeben)   | 1737 |
| SET DBRECOVERY (Einheitenklasse für automatische Sicherungen definieren)   | 1738 |
| SET DEDUPVERIFICATIONLEVEL (Prozentsatz der zu prüfenden Bereiche definieren)  | 1740 |
| SET DEFAULTAUTHENTICATION (Standardauthentifizierungsmethode für Befehle REGISTER NODE und REGISTER ADMIN definieren)  | 1741 |
| SET DEPLOYPKGMR (Implementierungspaketmanager aktivieren)  | 1742 |
| SET DEPLOYREPOSITORY (Downloadpfad für Clientimplementierungspakete definieren)  | 1743 |
| SET DEPLOYMAXPKGS (Maximale Anzahl Clientimplementierungspakete definieren, die gespeichert werden sollen)             | 1744 |
| SET DISSIMILARPOLICIES (Die Maßnahmen auf dem Zielreplikationsserver für die Verwaltung replizierter Daten aktivieren) | 1744 |
| SET DRMACTIVEDATASTGPOOL (Von DRM zu verwaltende Pools für aktive Daten angeben)                                       | 1745 |
| SET DRMCHECKLABEL (Kennsatzprüfung angeben)  | 1746 |
| SET DRMCMDFILENAME (Namen einer Datei angeben, die Befehle enthalten soll)   | 1747 |
| SET DRMCOPYCONTAINERSTGPOOL (Containerkopierspeicherpools angeben, die von DRM-Befehlen verarbeitet werden sollen)     | 1747 |
| SET DRMCOPYSTGPOOL (Von DRM zu verwaltende Kopierspeicherpools angeben)  | 1748 |
| SET DRMCOURIERNAME (Kuriernamen angeben)   | 1749 |
| SET DRMDBBACKUPEXPIREDAYS (Verfall für DB-Sicherungsreihe angeben)   | 1750 |
| SET DRMFILPROCESS (Dateiverarbeitung angeben)  | 1751 |
| SET DRMINSTRPREFIX (Präfix für Wiederherstellungsanweisungsdateinamen angeben)   | 1751 |
| SET DRMNOTMOUNTABLENAME (Nicht mountfähigen Standort angeben)  | 1753 |
| SET DRMPPLANPREFIX (Präfix für Wiederherstellungsplandateinamen angeben)   | 1754 |
| SET DRMPPLANVPOSTFIX (Namen für Ersatzdatenträger angeben)   | 1756 |
| SET DRMPRIMSTGPOOL (Von DRM zu verwaltende primäre Speicherpools angeben)  | 1757 |
| SET DRMRPFEXPIREDAYS (Kriterien für Verfall von Wiederherstellungsplandateien definieren)                              | 1757 |
| SET DRMVaultNAME (Aufbewahrungsort angeben)  | 1758 |
| SET EVENTRETENTION (Aufbewahrungszeitraum für Ereignissätze definieren)  | 1759 |
| SET FAILOVERHLADDRESS (Adresse höherer Ebene für Übernahme definieren)   | 1760 |
| SET INVALIDPWLIMIT (Anzahl der ungültigen Anmeldeversuche definieren)  | 1761 |
| SET LDAPPASSWORD (LDAP-Kennwort für den Server definieren)   | 1761 |
| SET LDAPUSER (ID für einen LDAP-Verzeichnisserver angeben)   | 1762 |
| SET LICENSEAUDITPERIOD (Dauer für Lizenzprüfung definieren)  | 1763 |
| SET MAXCMDRETRIES (Maximale Anzahl Befehlswiederholungen definieren)   | 1764 |
| SET MAXSCHEDULESESSIONS (Maximale Anzahl geplanter Sitzungen definieren)   | 1765 |
| SET MINPWLENGTH (Mindestlänge für Kennwort definieren)   | 1765 |
| SET MONITOREDSEVERGROUP (Gruppe überwachter Server definieren)   | 1766 |
| SET MONITORINGADMIN (Name des Überwachungsadministrators definieren)   | 1767 |
| SET NODEATRISKINTERVAL (Gibt den Gefährdungsmodus für einen einzelnen Knoten an)                                       | 1768 |
| SET PASSEXP (Ablaufdatum für Kennwort definieren)  | 1769 |
| SET PRODUCTOFFERING (Produktangebot definieren, das für Ihr Unternehmen lizenziert ist)                                | 1770 |
| SET QUERYSCHEDPERIOD (Zeitraum für Abfrage von Clientknoten definieren)  | 1772 |
| SET RANDOMIZE (Zufallsgenerierung von geplanten Startzeiten definieren)  | 1772 |
| SET REPRECOVERDAMAGED (Angabe, ob beschädigte Dateien von einem Replikationsserver wiederhergestellt werden)           | 1773 |
| SET REPRETENTION (Aufbewahrungszeitraum für Replikationsdatensätze definieren)   | 1775 |
| SET REPLSERVER (Zielreplikationsserver definieren)   | 1776 |
| SET RETRYPERIOD (Zeitintervall zwischen Wiederholungsversuchen definieren)   | 1777 |
| SET SCHEDMODES (Modus für zentrale Zeitplanung auswählen)  | 1778 |
| SET SCRATCHPADRETENTION (Aufbewahrungszeitraum für Scratchpad definieren)  | 1779 |
| SET SERVERHLADDRESS (Serveradresse der höheren Ebene definieren)   | 1779 |
| SET SERVERLLADDRESS (Serveradresse der unteren Ebene definieren)   | 1780 |
| SET SERVERNAME (Servernamen angeben)   | 1780 |

|   |      |
|---|------|
| SET SERVERPASSWORD (Kennwort für Server definieren)   | 1781 |
| SET SPREPLRUDEFAULT (Serverreplikationsregel für speicherverwaltete Daten definieren)   | 1782 |
| SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)        | 1783 |
| SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)   | 1784 |
| SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)   | 1785 |
| SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll) | 1786 |
| SET SUBFILE (Subdateisicherung für Clientknoten definieren)   | 1788 |
| SET SUMMARYRETENTION (Anzahl Tage für Aufbewahren in Aktivitätsübersichtstabelle definieren)  | 1788 |
| SET TAPEALERTMSG (Bandalerts aktivieren oder inaktivieren)  | 1789 |
| SET TOCLOADRETENTION (Aufbewahrungszeitraum für Laden für Inhaltsverzeichnis definieren)  | 1790 |
| SET VMATRISKINTERVAL (Gibt den Gefährdungsmodus für einen einzelnen VM-Dateibereich an)   | 1791 |
| SETOPT (Serveroption für dynamisches Aktualisieren definieren)  | 1792 |
| SHRED DATA (Daten schreddern)   | 1793 |
| SUSPEND EXPORT (Momentan aktive Exportoperation aussetzen)  | 1795 |
| UNLOCK-Befehle  | 1796 |
| UNLOCK ADMIN (Sperrung für einen Administrator aufheben)  | 1796 |
| UNLOCK NODE (Clientknoten freigeben)  | 1797 |
| UNLOCK PROFILE (Profil freigeben)   | 1797 |
| UPDATE-Befehle  | 1798 |
| UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)   | 1799 |
| UPDATE ALERTSTATUS (Status eines Alert aktualisieren)   | 1800 |
| UPDATE ADMIN (Administrator aktualisieren)  | 1802 |
| UPDATE BACKUPSET (Aufbewahrungszeitraum einer Sicherungsgruppe aktualisieren)   | 1805 |
| UPDATE CLIENTOPT (Folgenummer einer Clientoption aktualisieren)   | 1809 |
| UPDATE CLOPTSET (Beschreibung einer Clientoptionsgruppe aktualisieren)  | 1810 |
| UPDATE COLLOGGROUP (Kollokationsgruppe aktualisieren)   | 1811 |
| UPDATE COPYGROUP (Kopiengruppe aktualisieren)   | 1812 |
| UPDATE COPYGROUP (Sicherungskopiengruppe aktualisieren)   | 1812 |
| UPDATE COPYGROUP (Definierte Archivierungskopiengruppe aktualisieren)   | 1815 |
| UPDATE DATAMOVER (Einheit zum Versetzen von Daten aktualisieren)  | 1817 |
| UPDATE DEVCLASS (Attribute einer Einheitenklasse aktualisieren)   | 1818 |
| 3590  | 1819 |
| 3592  | 1822 |
| 4MM   | 1827 |
| 8MM   | 1829 |
| Centera   | 1834 |
| DLT   | 1835 |
| Ecartridge  | 1839 |
| File  | 1843 |
| Generictape   | 1847 |
| LTO   | 1849 |
| NAS   | 1853 |
| Removablefile   | 1855 |
| Server  | 1856 |
| VolSafe   | 1858 |
| UPDATE DEVCLASS - z/OS Media-Server (Einheitenklasse für z/OS Media-Server aktualisieren)   | 1860 |
| 3590, für z/OS Media-Server   | 1861 |
| 3592, für z/OS Media-Server   | 1864 |
| ECARTRIDGE, für z/OS Media-Server   | 1868 |
| FILE, für z/OS Media-Server   | 1871 |
| UPDATE DOMAIN (Maßnahmendomäne aktualisieren)   | 1874 |
| UPDATE DRIVE (Laufwerk aktualisieren)   | 1875 |
| UPDATE FILESPACE (Knotenreplikationsregeln für Dateibereich aktualisieren)  | 1878 |
| UPDATE LIBRARY (Kassettenarchiv aktualisieren)  | 1881 |
| 349X  | 1883 |
| ACSLs   | 1885 |

|  |      |
|--|------|
| EXTERNAL   | 1886 |
| FILE   | 1887 |
| MANUAL   | 1888 |
| SCSI   | 1889 |
| SHARED   | 1891 |
| VTL  | 1892 |
| UPDATE LIBVOLUME (Status eines Speicherdatenträgers ändern)                                  | 1894 |
| UPDATE MACHINE (Maschineninformationen aktualisieren)  | 1895 |
| UPDATE MGMTCLASS (Verwaltungsklasse aktualisieren)   | 1896 |
| UPDATE NODE (Attribute eines Knotens aktualisieren)  | 1898 |
| UPDATE NODEGROUP (Knotengruppe aktualisieren)  | 1912 |
| UPDATE PATH (Pfad ändern)  | 1913 |
| Ziel ist ein Laufwerk  | 1914 |
| Ziel ist ein Kassettenarchiv   | 1918 |
| Ziel ist ein ZOSMEDIA-Kassettenarchiv  | 1920 |
| UPDATE POLICYSET (Beschreibung einer Maßnahmengruppe aktualisieren)                          | 1921 |
| UPDATE PROFILE (Profilbeschreibung aktualisieren)  | 1921 |
| UPDATE RECOVERYMEDIA (Wiederherstellungsdatenträger aktualisieren)                           | 1922 |
| UPDATE REPLRULE (Replikationsregeln aktualisieren)   | 1924 |
| UPDATE SCHEDULE (Zeitplan aktualisieren)   | 1925 |
| UPDATE SCHEDULE (Clientzeitplan aktualisieren)   | 1925 |
| UPDATE SCHEDULE (Verwaltungszeitplan aktualisieren)  | 1935 |
| UPDATE SCRATCHPADENTRY (Scratchpadeintrag aktualisieren)                                     | 1942 |
| UPDATE SCRIPT (IBM Spectrum Protect-Prozedur aktualisieren)                                  | 1942 |
| UPDATE SERVER (Server aktualisieren, der für die Übertragung zwischen Servern definiert ist) | 1944 |
| UPDATE SERVERGROUP (Beschreibung einer Servergruppe aktualisieren)                           | 1949 |
| UPDATE SPACETRIGGER (Speicherbereichsauslöser aktualisieren)                                 | 1949 |
| UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)                   | 1951 |
| UPDATE STGPOOL (Speicherpool aktualisieren)  | 1954 |
| Cloud-Containerspeicherpool  | 1955 |
| Verzeichniscontainerspeicherpool   | 1958 |
| Containerkopierspeicherpool  | 1961 |
| Primärer Pool mit wahlfreiem Zugriff   | 1964 |
| Primärer Pool mit sequenziellem Zugriff  | 1971 |
| Kopienpool   | 1982 |
| Pool für aktive Daten  | 1987 |
| UPDATE STGPOOLDIRECTORY (Speicherpoolverzeichnis aktualisieren)                              | 1991 |
| UPDATE STGRULE (Speicherregel für einen oder mehrere Speicherpools aktualisieren)            | 1993 |
| UPDATE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs aktualisieren)             | 1995 |
| UPDATE VOLHISTORY (History-Daten für sequentielle Datenträger aktualisieren)                 | 1996 |
| UPDATE VOLUME (Speicherpooldatenträger ändern)   | 1997 |
| VALIDATE-Befehle   | 2001 |
| VALIDATE ASPERA (Aspera FASP-Konfiguration validieren)                                       | 2001 |
| VALIDATE CLOUD (Cloudberechtigungs-nachweise prüfen)   | 2004 |
| VALIDATE LANFREE (LAN-unabhängige Pfade prüfen)  | 2005 |
| VALIDATE POLICYSET (Maßnahmengruppe prüfen)  | 2006 |
| VALIDATE REPLICATION (Replikation für einen Clientknoten überprüfen)                         | 2008 |
| VALIDATE REPLPOLICY (Die Maßnahmen auf dem Zielreplikationsserver prüfen)                    | 2011 |
| VARY (Datenträger mit wahlfreiem Zugriff an-/abhängen)                                       | 2013 |
| Serveroptionen   | 2014 |
| Serveroptionen ändern  | 2021 |
| Arten von Serveroptionen   | 2022 |
| Serverübertragungsoptionen   | 2022 |
| Optionen für den Serverspeicher  | 2024 |
| Client/Server-Optionen   | 2025 |
| Optionen für Datum, Zahlen, Uhrzeit und Sprache  | 2026 |
| Datenbankoptionen  | 2026 |
| Datenübertragungsoptionen  | 2026 |

|  |      |
|--|------|
| Nachrichtenoptionen                                  | 2027 |
| Optionen für die Aufzeichnung des Ereignisprotokolls | 2027 |
| Optionen für Sicherheit und Lizenzierung             | 2028 |
| Weitere Optionen                                     | 2028 |
| 3494SHARED   | 2029 |
| ACSACCESSID  | 2029 |
| ACSLOCKDRIVE   | 2030 |
| ACSQUICKINIT   | 2030 |
| ACSTIMEOUTX  | 2031 |
| ACTIVELOGDIRECTORY                                   | 2031 |
| ACTIVELOGSIZE  | 2031 |
| ADMINCOMMTIMEOUT                                     | 2032 |
| ADMINIDLETIMEOUT                                     | 2032 |
| ADMINONCLIENTPORT                                    | 2033 |
| ADSMGROUPNAME  | 2033 |
| ALIASHALT  | 2034 |
| ALLOWDESAUTH   | 2034 |
| ALLOWREORGINDEX                                      | 2035 |
| ALLOWREORGTABLE                                      | 2035 |
| ARCHFAILOVERLOGDIRECTORY                             | 2035 |
| ARCHLOGCOMPRESS                                      | 2036 |
| ARCHLOGDIRECTORY                                     | 2036 |
| ARCHLOGUSEDTHRESHOLD                                 | 2037 |
| ASSISTVCRRECOVERY                                    | 2037 |
| AUDITSTORAGE   | 2038 |
| BACKUPINITIATIONROOT                                 | 2038 |
| CHECKTAPEPOS   | 2039 |
| CLIENTDEDUPTXNLIMIT                                  | 2040 |
| CLIENTDEPLOYCATALOGURL                               | 2040 |
| CLIENTDEPLOYUSELOCALCATALOG                          | 2041 |
| COMMMETHOD   | 2041 |
| COMMTIMEOUT  | 2042 |
| CONTAINERRESOURCESTIMEOUT                            | 2043 |
| DATEFORMAT   | 2043 |
| DBDIAGLOGSIZE  | 2044 |
| DBDIAGPATHFSTHRESHOLD                                | 2045 |
| DBMEMPERCENT   | 2045 |
| DBMTCPPORT   | 2046 |
| DEDUPREQUIRESBACKUP                                  | 2046 |
| DEDUPTIER2FILESIZE                                   | 2047 |
| DEDUPTIER3FILESIZE                                   | 2047 |
| DEVCONFIG  | 2048 |
| DISABLEREORGTABLE                                    | 2048 |
| DISABLESCHEDS  | 2049 |
| DISPLAYLFINFO  | 2049 |
| DNSLOOKUP  | 2050 |
| DRIVEACQUIRERETRY                                    | 2050 |
| ENABLENASDEDUP                                       | 2051 |
| EVENTSERVER  | 2051 |
| EXPINTERVAL  | 2052 |
| EXPQUIET   | 2052 |
| FASPBEGPORT  | 2053 |
| FASPENDPORT  | 2053 |
| FASPTARGETRATE                                       | 2054 |
| FFDCLOGLEVEL   | 2054 |
| FFDCLOGNAME  | 2055 |
| FFDCMAXLOGSIZE                                       | 2055 |
| FFDCNUMLOGS  | 2056 |

|                       |      |
|-----------------------|------|
| FILEEXIT              | 2056 |
| FILETEXTEXIT          | 2057 |
| FSUSEDTHRESHOLD       | 2058 |
| IDLETIMEOUT           | 2058 |
| KEEPALIVE             | 2058 |
| KEEPALIVETIME         | 2059 |
| KEEPALIVEINTERVAL     | 2060 |
| LANGUAGE              | 2060 |
| LDAPCACHEDURATION     | 2062 |
| LDAPURL               | 2063 |
| MAXSESSIONS           | 2064 |
| MESSAGEFORMAT         | 2064 |
| MIRRORLOGDIRECTORY    | 2064 |
| MOVEBATCHSIZE         | 2065 |
| MOVESIZETHRESH        | 2065 |
| MSGINTERVAL           | 2066 |
| NAMEDPIPENAME         | 2066 |
| NDMPCONNECTIONTIMEOUT | 2066 |
| NDMPCONTROLPORT       | 2067 |
| NDMPENABLEKEEPALIVE   | 2067 |
| NDMPKEEPIDLEMINUTES   | 2068 |
| NDMPPORTRANGE         | 2068 |
| NDMPREFDATAINTERFACE  | 2069 |
| NOPREEMPT             | 2069 |
| NORETRIEVEDATE        | 2070 |
| NPAUDITFAILURE        | 2070 |
| NPAUDITSUCCESS        | 2071 |
| NPBUFFERSIZE          | 2071 |
| NUMBERFORMAT          | 2072 |
| NUMOPENVOLSALLOWED    | 2072 |
| PUSHSTATUS            | 2073 |
| QUERYAUTH             | 2073 |
| RECLAIMDELAY          | 2074 |
| RECLAIMPERIOD         | 2074 |
| REORGBEGINTIME        | 2075 |
| REORGDURATION         | 2075 |
| REPORTRETRIEVE        | 2076 |
| REPLBATCHSIZE         | 2076 |
| REPLSIZETHRESH        | 2077 |
| REQSYSAUTHOUTFILE     | 2077 |
| RESOURCETIMEOUT       | 2078 |
| RESTHTTPSPORT         | 2078 |
| RESTOREINTERVAL       | 2079 |
| RETENTIONEXTENSION    | 2079 |
| SANDISCOVERY          | 2080 |
| SANDISCOVERYTIMEOUT   | 2081 |
| SANREFRESHTIME        | 2081 |
| SEARCHMPQUEUE         | 2081 |
| SECUREPIPES           | 2082 |
| SERVERDEDUPTXNLIMIT   | 2082 |
| SHMPORT               | 2083 |
| SHREDDING             | 2084 |
| SNMPHEARTBEATINTERVAL | 2084 |
| SNMPMESSAGECATEGORY   | 2085 |
| SNMPSUBAGENT          | 2085 |
| SNMPSUBAGENTHOST      | 2086 |
| SNMPSUBAGENTPORT      | 2086 |
| SSLFIPSMODE           | 2086 |

|  |      |
|--|------|
| SSLINITTIMEOUT   | 2087 |
| SSLTCPADMINPORT  | 2087 |
| SSLTCPPOINT  | 2088 |
| TCPADMINPORT   | 2088 |
| TCPBUFSIZE   | 2089 |
| TCPNODELAY   | 2090 |
| TCPPOINT   | 2090 |
| TCPWINDOWSIZE  | 2091 |
| TECBEGINEVENTLOGGING   | 2091 |
| TECHOST  | 2092 |
| TECPOINT   | 2092 |
| TECUTF8EVENT   | 2092 |
| THROUGHPUTDATATHRESHOLD  | 2093 |
| THROUGHPUTTIMETHRESHOLD  | 2093 |
| TIMEFORMAT   | 2094 |
| TXNGROUPMAX  | 2094 |
| UNIQUETDPTEEVENTS  | 2095 |
| UNIQUETECEVENTS  | 2095 |
| USEREXIT   | 2096 |
| VERBCHECK  | 2096 |
| VOLUMEHISTORY  | 2097 |
| Serverdienstprogramme  | 2097 |
| DSMMAXSG (Blockgröße für das Schreiben von Daten erhöhen)                                  | 2098 |
| DSMSERV (Server starten)   | 2099 |
| Serverstartscript: rc.dsmserv  | 2101 |
| Serverstartscript: dsmserv.rc  | 2101 |
| DSMSERV DISPLAY DBSPACE (Informationen zum Datenbankspeicherbereich anzeigen)              | 2102 |
| DSMSERV DISPLAY LOG (Informationen zum Wiederherstellungsprotokoll anzeigen)               | 2103 |
| DSMSERV EXTEND DBSPACE (Speicherbereich für die Datenbank vergrößern)                      | 2105 |
| DSMSERV FORMAT (Datenbank und Protokoll formatieren)                                       | 2106 |
| DSMSERV INSERTDB (Serverdatenbank in eine leere Datenbank versetzen)                       | 2108 |
| DSMSERV LOADFORMAT (Datenbank formatieren)   | 2110 |
| DSMSERV REMOVEDB (Datenbank entfernen)   | 2112 |
| DSMSERV RESTORE DB (Datenbank zurückschreiben)   | 2113 |
| DSMSERV RESTORE DB (Datenbank mit dem neuesten Stand zurückschreiben)                      | 2113 |
| DSMSERV RESTORE DB (Datenbank nach Zeitpunkt zurückschreiben)                              | 2116 |
| DSMSERV UPDATE (Registry-Einträge für eine Serverinstanz erstellen)                        | 2120 |
| DSMULOG (IBM Spectrum Protect-Servernachrichten in einer Benutzerprotokolldatei speichern) | 2120 |
| Einheitendienstprogramme   | 2121 |
| AIX: tsmdlst (Informationen zu Einheiten anzeigen)   | 2121 |
| Linux: autoconf (Einheiten automatisch konfigurieren)                                      | 2122 |
| Windows: tsmdlst (Informationen zu Einheiten anzeigen)                                     | 2123 |
| Server-Scripts und Makros für die Automatisierung  | 2125 |
| Server-Scripts   | 2126 |
| Server-Script definieren   | 2126 |
| Befehle parallel oder seriell ausführen  | 2127 |
| Befehle über mehrere Befehlszeilen fortsetzen  | 2128 |
| Substitutionsvariablen in ein Script einschließen  | 2128 |
| Logikablaufanweisungen in ein Script einschließen  | 2128 |
| Klausel IF angeben   | 2129 |
| Anweisung EXIT angeben   | 2129 |
| Anweisung GOTO angeben   | 2129 |
| Befehle SELECT in einem Script verwenden   | 2130 |
| Script aktualisieren   | 2130 |
| Neuen Befehl anfügen   | 2131 |
| Vorhandenen Befehl ersetzen  | 2131 |
| Befehl und Zeilennummer hinzufügen   | 2131 |
| Befehl aus einem Server-Script löschen   | 2132 |



|   |      |
|---|------|
| Server-Script zum Erstellen eines anderen Server-Scripts abfragen | 2132 |
| Server-Script ausführen   | 2132 |
| Makros des Verwaltungsclients                                     | 2133 |
| Befehle in ein Makro schreiben                                    | 2133 |
| Kommentare in ein Makro schreiben                                 | 2134 |
| Fortsetzungszeichen in ein Makro einschließen                     | 2134 |
| Substitutionsvariablen in ein Makro einschließen                  | 2135 |
| Makro ausführen   | 2135 |
| Befehlsverarbeitung in einem Makro                                | 2135 |
| Rückkehrcodes für die Verwendung in IBM Spectrum Protect-Scripts  | 2136 |
| PDF-Dateien   | 2138 |

|                |      |
|----------------|------|
| <b>Clients</b> | 2139 |
|----------------|------|

|            |      |
|------------|------|
| <b>API</b> | 2139 |
|------------|------|

|                 |      |
|-----------------|------|
| <b>Leistung</b> | 2139 |
|-----------------|------|

|                       |      |
|-----------------------|------|
| <b>Fehlerbehebung</b> | 2139 |
|-----------------------|------|

|   |      |
|---|------|
| <b>Nachrichten, Rückkehrcodes und Fehlercodes</b> | 2139 |
|---|------|

|   |      |
|---|------|
| Einführung in Nachrichten   | 2140 |
| Format der IBM Spectrum Protect-Server- und -Clientnachrichten                      | 2140 |
| Rückkehrcodenachrichten interpretieren  | 2141 |
| Erstes Beispiel für den Befehl QUERY EVENT  | 2141 |
| Zweites Beispiel für den Befehl DEFINE VOLUME                                       | 2142 |
| ANE-Nachrichten   | 2142 |
| ANR-Nachrichten   | 2142 |
| ANS-Nachrichten 0000-9999   | 2142 |
| API-Rückkehrcodes   | 2142 |
| E/A-Codebeschreibungen in Servernachrichten   | 2142 |
| Übersicht über Beendigungscode- und Operationscodebeschreibungen für Einheitsreiber | 2144 |
| Beendigungscodewerte, die auf alle Einheitenklassen zutreffen                       | 2144 |
| Beendigungscodewerte für Datenträgerwechsler  | 2145 |
| Beendigungscodewerte für Bandlaufwerke  | 2146 |
| Beschreibungen der ASC- und ASCQ-Standardcodes                                      | 2148 |
| Einheitenfehlercodes im AIX-Systemfehlerprotokoll                                   | 2151 |
| Rückkehrcodes für IBM Global Security Kit   | 2152 |

|                |      |
|----------------|------|
| <b>Glossar</b> | 2162 |
|----------------|------|

|   |      |
|---|------|
| A | 2162 |
| B | 2164 |
| C | 2164 |
| D | 2165 |
| E | 2167 |
| F | 2168 |
| G | 2168 |
| H | 2169 |
| I | 2169 |
| J | 2170 |
| K | 2170 |
| L | 2171 |
| M | 2172 |
| N | 2173 |
| O | 2173 |
| P | 2173 |

|   |      |
|---|------|
| Q | 2174 |
| R | 2175 |
| S | 2175 |
| T | 2177 |
| U | 2177 |
| V | 2178 |
| W | 2180 |
| Z | 2180 |

# Dokumentation für IBM Spectrum Protect

---

IBM Spectrum Protect stellt automatisierte, zentral geplante, maßnahmenverwaltete Sicherungs-, Archivierungs- und Speicherverwaltungsfunktionen für Dateiserver, Workstations, virtuelle Maschinen und Anwendungen bereit. Verwenden Sie die IBM Spectrum Protect-Dokumentation, die Sie beim Definieren, Konfigurieren und Verwalten Ihrer Datenschutzlösungen unterstützt.

## Einführung

Installation und Upgrade für Server durchführen  
Operations Center installieren und Operations Center-Upgrade durchführen  
Datenschutzlösungen auswählen und implementieren  
Neuerungen für den Server  
[📄 Videos mit den Neuerungen](#)  
PDF-Dateien

## Allgemeine Tasks

Tägliche Überwachungstasks  
Clients hinzufügen  
Clientdaten auf einen anderen Server replizieren  
Server, Clients und Operations Center verwalten  
Speicher konfigurieren  
Serverbefehle, -optionen und -dienstprogramme

## Fehlerbehebung und Unterstützung

Fehler beheben  
Leistung optimieren  
[📄 Neueste Fixpacks für IBM Spectrum Protect-Clients und -Server](#)  
[📄 IBM Software Support](#)

## Weitere Informationen

[📄 Hinweise für Benutzer des IBM® Knowledge Center Produktsuites und zugehörige Produkte](#)  
[📄 Homepage der Produktfamilie](#)  
[📄 Wiki für IBM Spectrum Protect-Produkte](#)  
[📄 IBM Spectrum Protect Developer Center](#)  
[📄 IBM Redbooks-Veröffentlichungen](#)  
[📄 IBM Skills Gateway for Systems Behindertengerechte Bedienung](#)  
Rechtliche Hinweise zum Produkt

© Copyright IBM Corp. 1993, 2017

## Funktionen zur behindertengerechten Bedienung für die IBM Spectrum Protect-Produktfamilie

---

Funktionen zur behindertengerechten Bedienung helfen Benutzern mit Behinderungen, wie eingeschränkter Beweglichkeit oder Sehfähigkeit, damit sie informationstechnologische Inhalte erfolgreich verwenden können.

## Übersicht

---

Die IBM Spectrum Protect-Produktfamilie umfasst die folgenden bedeutenden Funktionen zur behindertengerechten Bedienung:

- Bedienung ausschließlich über die Tastatur
- Operationen, die ein Sprachausgabeprogramm verwenden

Die IBM Spectrum Protect-Produktfamilie verwendet den neuesten W3C-Standard WAI-ARIA 1.0, um die Einhaltung von US Section 508 und der Web Content Accessibility Guidelines (WCAG) 2.0 sicherzustellen. Um die Funktionen zur behindertengerechten Bedienung zu nutzen, verwenden Sie das neueste Release Ihres Sprachausgabeprogramms in Verbindung mit dem neuesten Web-Browser, der von diesem Produkt unterstützt wird.

Die Produktdokumentation im IBM Knowledge Center ist für die behindertengerechte Bedienung aktiviert. Eine Beschreibung der Funktionen zur behindertengerechten Bedienung im IBM Knowledge Center finden Sie im Abschnitt 'Accessibility' der IBM Knowledge Center-Hilfe .

## Navigation mithilfe der Tastatur

---

Dieses Produkt verwendet Standardnavigationstasten.

## Schnittstelleninformationen

---

In den Benutzerschnittstellen gibt es keine Inhalte, die 2 - 55 Mal in der Sekunde blinken.

Die Webbenutzerschnittstellen basieren auf Cascading Style Sheets, um Inhalte ordnungsgemäß wiederzugeben und um positive Erfahrungen zu ermöglichen. Die Anwendung bietet eine funktional entsprechende Möglichkeit für Benutzer mit eingeschränktem Sehvermögen, um die Systemanzeigeeinstellungen des Benutzers einschließlich des Modus für kontraststarke Anzeige zu verwenden. Sie können die Schriftgröße über die Einstellungen für die Einheit oder für den Web-Browser steuern.

Die Webbenutzerschnittstellen beinhalten WAI-ARIA-Navigationsmarkierungen, mit deren Hilfe Sie schnell zu Funktionsbereichen in der Anwendung navigieren können.

## Software anderer Anbieter

---

Die IBM Spectrum Protect-Produktfamilie enthält bestimmte Software anderer Anbieter, die nicht der IBM Lizenzvereinbarung unterliegt. IBM gibt keine Erklärung zu den Funktionen zur behindertengerechten Bedienung dieser Produkte ab. Wenden Sie sich an den Softwareanbieter, um Informationen zur behindertengerechten Bedienung der Produkte zu erhalten.

## Zugehörige Informationen zur behindertengerechten Bedienung

---

Neben dem standardmäßigen IBM Help-Desk und den Support-Websites bietet IBM einen TTY-Telefonservice für gehörlose oder hörgeschädigte Kunden für den Zugriff auf Vertriebs- und Support-Services:

TTY-Service  
800-IBM-3383 (800-426-3383)  
(innerhalb von Nordamerika)

Weitere Informationen zum Engagement von IBM im Bereich der behindertengerechten Bedienung finden Sie in IBM Accessibility.

## Produktsuites und zugehörige Produkte

---

IBM Spectrum Protect-Suites und zugehörige Speicherprodukte verbessern und erweitern die Features des IBM Spectrum Protect-Basisprodukts.

## Produktsuites und Lizenzoptionen

---

Die Produkte IBM Spectrum Protect und IBM Spectrum Protect Extended Edition stellen die Kernkomponenten für automatisierte und zentrale Sicherungs- und Zurückschreibungsoperationen bereit. Die Serverkomponente und die Clientkomponente für Sichern/Archivieren stellen Basisfunktionen wie z. B. Sicherungs- und Zurückschreibungsoperationen sowie Archivierungs- und Abrufoperationen für Dateien, Verzeichnisse und Plattenimages zur Verfügung.

Die Produktdokumentation enthält Informationen sowohl für IBM Spectrum Protect als auch für IBM Spectrum Protect Extended Edition.

Produktsuites, die IBM Spectrum Protect mit zugehörigen Produkten kombinieren, bieten unter Umständen eine einfachere Möglichkeit, um IBM Spectrum Protect-Software zu kaufen und zu verwalten. Die Suites umfassen Produkte, die einen Bereich von Datenschutz- und Wiederherstellungsanforderungen mit vereinfachter Lizenzierung erfüllen können. Weitere Informationen zu IBM Spectrum Protect-Produktsuites.

## Zugehörige Produkte

---

Sie können IBM Spectrum Protect mit Funktionen und Features erweitern, die in zugehörigen Produkten verfügbar sind.

| Produkt | Wichtige Vorteile | Links |
|---------|-------------------|-------|
|---------|-------------------|-------|

| Produkt                                       | Wichtige Vorteile  | Links   |
|---|--|---|
| IBM Spectrum Copy Data Management             | Katalogisiert NetApp- und VMware-Momentaufnahmen, um die rollenabhängige Verwaltung und Wiederherstellung von Sicherungsdaten zu erleichtern.  | <ul style="list-style-type: none"> <li>• Weitere Informationen und Kauf</li> <li>• Produktdokumentation</li> </ul>  |
| IBM Spectrum Protect High Speed Data Transfer | Verwenden Sie dieses Produkt für die Aktivierung der FASP-Technologie (FASP = Fast Adaptive Secure Protocol), um die Datenübertragung in einer Umgebung zu verbessern, in der WAN-Leistungsprobleme erkannt werden.  | <ul style="list-style-type: none"> <li>• Weitere Informationen und Kauf</li> <li>• Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann</li> </ul>                          |
| IBM Spectrum Protect for Data Retention       | <p>Stellt beim Archivieren von Geschäftsaufzeichnungen, Dateien oder Daten einen langfristigen Aufbewahrungsschutz zur Verfügung.</p> <p>Die Archivierung von Daten zur Einhaltung gesetzlicher Bestimmungen erfordert zusätzliche Sicherheitseinrichtungen oder zusätzlichen Schutz, der als Aufbewahrungsschutz für Daten bezeichnet wird. Mit diesen Sicherheitseinrichtungen kann sichergestellt werden, dass Daten entweder versehentlich oder mutwillig nicht frühzeitig gelöscht werden. Um die gesetzlichen Bestimmungen einzuhalten, stellt IBM Spectrum Protect for Data Retention einen zusätzlichen Schutz für Daten bereit, die von IBM Spectrum Protect archiviert werden.</p> | <ul style="list-style-type: none"> <li>• Weitere Informationen und Kauf</li> <li>• Produktdokumentation</li> </ul> <p>Tipp: Dokumentation für dieses Produkt ist in der IBM Spectrum Protect-Dokumentation enthalten.</p> |
| IBM Spectrum Protect Snapshot                 | <p>Schützt Daten mit integrierten, anwendungsgesteuerten Momentaufnahmesicherungs- und -zurückschreibungsfunktionen.</p> <p>Daten, die von IBM® DB2-, SAP-, Oracle-, Microsoft Exchange- und Microsoft SQL Server-Anwendungen gespeichert werden, können mit IBM Spectrum Protect Snapshot-Software geschützt werden. Mit der Software können Sie Momentaufnahmen auf Datenträgerebene für Dateisysteme und kundenspezifische Anwendungen erstellen und verwalten. Sie können auswählen, ob IBM Spectrum Protect Snapshot in IBM Spectrum Protect integriert werden soll.</p>  | <ul style="list-style-type: none"> <li>• Weitere Informationen und Kauf</li> <li>• Produktdokumentation</li> </ul>  |

| Produkt   | Wichtige Vorteile   | Links  |
|---|---|--|
| IBM Spectrum Protect for Databases                    | Schützt Oracle-Daten und Microsoft SQL-Daten durch automatische Tasks, Dienstprogramme und Schnittstellen. Diese Software erstellt konsistente und zentrale Onlinesicherungen, um Ausfallzeiten zu vermeiden, kritische Unternehmensdaten zu schützen und Betriebskosten zu minimieren.<br>Tipp: Unterstützung für Onlinesicherungen von IBM DB2- und IBM Informix-Datenbanken ist mit IBM Spectrum Protect-Servern eingeschlossen. Sie müssen nicht IBM Spectrum Protect for Databases installieren, um diese Datenbanken zu sichern. Weitere Informationen finden Sie in der Dokumentation für die Produkte DB2 und Informix. | <ul style="list-style-type: none"> <li>• Weitere Informationen und Kauf</li> <li>• Produktdokumentation</li> </ul>   |
| IBM Spectrum Protect for Enterprise Resource Planning | Stellt Schutz bereit, der für SAP-Systemdaten angepasst ist.  | <ul style="list-style-type: none"> <li>• Weitere Informationen und Kauf</li> <li>• Produktdokumentation</li> </ul>   |
| IBM Spectrum Protect for Mail                         | Automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass Microsoft Exchange-Server oder IBM Domino-Server heruntergefahren werden.  | <ul style="list-style-type: none"> <li>• Weitere Informationen und Kauf</li> <li>• Produktdokumentation</li> </ul>   |
| IBM Spectrum Protect for Space Management             | Ein Produkt für die hierarchische Speicherverwaltung, mit dem Speicherkosten für Informationen reduziert werden, auf die selten zugegriffen wird, ohne dass sich die Art und Weise ändert, wie Benutzer und Anwendungen mit ihren Daten interagieren. Verwenden Sie dieses Produkt auf AIX- und Linux-Betriebssystemen.   | <ul style="list-style-type: none"> <li>• Weitere Informationen und Kauf</li> <li>• Produktdokumentation</li> </ul>   |
| IBM Spectrum Protect HSM for Windows                  | Ein Produkt für die hierarchische Speicherverwaltung, mit dem Speicherkosten für Informationen reduziert werden, auf die selten zugegriffen wird, ohne dass sich die Art und Weise ändert, wie Benutzer und Anwendungen mit ihren Daten interagieren. Verwenden Sie dieses Produkt auf Windows-Betriebssystemen.  | <ul style="list-style-type: none"> <li>• Weitere Informationen und Kauf</li> <li>• Produktdokumentation</li> </ul>   |
| IBM Spectrum Protect for SAN                          | Arbeitet mit Servern und Client-Computern, um Daten über ein Speicherbereichsnetz (SAN) anstelle eines LAN zu übertragen. Das Produkt ist ein Speicheragent, der LAN-unabhängige Sicherungs- und Zurückschreibungsoperationen ermöglicht.   | <ul style="list-style-type: none"> <li>• Weitere Informationen und Kauf</li> <li>• Produktdokumentation</li> </ul> <p>Version der Produktdokumentation: Die Dokumentation für IBM Tivoli Storage Manager for Storage Area Networks Version 7.1 ist für die Verwendung mit der IBM Spectrum Protect-Produktfamilie Version 8.1 anwendbar.</p> |
| IBM Spectrum Protect for Virtual Environments         | Stellt Schutz bereit, der für virtuelle VMware- und Hyper-V-Umgebungen angepasst ist.   | <ul style="list-style-type: none"> <li>• Weitere Informationen und Kauf</li> <li>• Produktdokumentation</li> </ul>   |
| IBM Tivoli Storage Manager for z/OS Media             | Verwaltet z/OS-Platten- und -Bandressourcen für IBM Spectrum Protect-Server, die auf AIX- oder Linux on System z-Systemen ausgeführt werden.  | <ul style="list-style-type: none"> <li>• Produktdokumentation</li> </ul>   |

Sie können vorgefertigte PDF-Dateien aus dem IBM® Knowledge Center oder von einer FTP-Download-Site herunterladen.

## Vorgefertigte PDF-Dateien

---

In den folgenden Abschnitten sind die vorgefertigten PDF-Dateien aufgeführt, die für dieses Release verfügbar sind:

- Datenschutzlösungen
- Server

## Paket der PDF-Dateien

---

Laden Sie ein Paket, das alle PDF-Dateien für dieses Release enthält, von der folgenden FTP-Site herunter:

<ftp://public.dhe.ibm.com/software/products/ISP/current/>

## Aktualisierungen in diesem Release

---

Lesen Sie die Informationen zu den neuen Funktionen und funktionalen Erweiterungen, die in den Produkten verfügbar sind, um die potenziellen Vorteile für Ihre Speicherverwaltungsoperationen erkennen zu können. Die Releaseinformationen enthalten Links, auf die Sie zugreifen können, um wichtige Informationen abzurufen, bevor Sie Produkte und Komponenten installieren oder aktualisieren.

| Komponente        | Zusammenfassung der Aktualisierungen | Releaseinformationen für Version 8.1 |
|-------------------|--------------------------------------|--------------------------------------|
| Serverkomponenten | Aktualisierungen                     | Releaseinformationen                 |

## IBM Spectrum Protect-Konzepte

---

IBM Spectrum Protect stellt eine umfassende Datenschutzzumgebung bereit.

- Übersicht über IBM Spectrum Protect  
IBM Spectrum Protect stellt zentralen automatisierten Datenschutz bereit, mit dessen Hilfe die Wahrscheinlichkeit eines Datenverlusts verringert und die Erfüllung von Anforderungen hinsichtlich Datenschutz und Verfügbarkeit gewährleistet werden kann.
- Konzepte der Datenspeicherung in IBM Spectrum Protect  
IBM Spectrum Protect stellt Funktionen zum Speichern von Daten in Einheitspeicher und externem Speicher bereit.
- Datenschutzstrategien bei IBM Spectrum Protect  
IBM Spectrum Protect stellt Möglichkeiten zur Implementierung verschiedener Datenschutzstrategien bereit.

## Übersicht über IBM Spectrum Protect

---

IBM Spectrum Protect stellt zentralen automatisierten Datenschutz bereit, mit dessen Hilfe die Wahrscheinlichkeit eines Datenverlusts verringert und die Erfüllung von Anforderungen hinsichtlich Datenschutz und Verfügbarkeit gewährleistet werden kann.

- **Datenschutzkomponenten**  
Die Datenschutzlösungen, die von IBM Spectrum Protect bereitgestellt werden, umfassen einen Server, Clientsysteme und -anwendungen sowie Speichermedien. IBM Spectrum Protect stellt Managementschnittstellen für die Überwachung und das Zurückmelden des Datenschutzstatus bereit.
- **Datenschutzservices**  
IBM Spectrum Protect stellt Datenschutzservices zum Speichern und Wiederherstellen von Daten für verschiedene Clienttypen bereit. Die Datenschutzservices werden über Maßnahmen implementiert, die auf dem Server definiert sind. Die Datenschutzservices können mithilfe der Clientzeitplanung automatisiert werden.
- **Prozesse zur Verwaltung des Datenschutzes mit IBM Spectrum Protect**  
Der IBM Spectrum Protect-Serverbestand übernimmt eine wichtige Rolle in den Prozessen für den Datenschutz. Sie definieren Maßnahmen, die der Server zum Verwalten des Datenspeichers verwendet.
- **Benutzerschnittstellen für die IBM Spectrum Protect-Umgebung**  
Für Überwachungs- und Konfigurationstasks stellt IBM Spectrum Protect verschiedene Schnittstellen, einschließlich des Operations Center, einer Befehlszeilenschnittstelle und einer SQL-Verwaltungsschnittstelle, bereit.

## Datenschutzkomponenten

---

Die Datenschutzlösungen, die von IBM Spectrum Protect bereitgestellt werden, umfassen einen Server, Clientsysteme und -anwendungen sowie Speichermedien. IBM Spectrum Protect stellt Managementschnittstellen für die Überwachung und das Zurückmelden des Datenschutzstatus bereit.

## Server

Clientsysteme senden Daten zur Speicherung als Sicherungen oder archivierte Daten an den Server. Der Server umfasst einen *Bestand*, der ein Repository der Informationen zu Clientdaten ist.

Der Bestand umfasst die folgenden Komponenten:

### Datenbank

Informationen zu jeder Datei, jedem logischen Datenträger oder jeder Datenbank, die bzw. den der Server sichert, archiviert oder umlagert, werden in der Serverdatenbank gespeichert. Die Serverdatenbank enthält auch Informationen zu der Maßnahme und den Zeitplänen für Datenschutzservices.

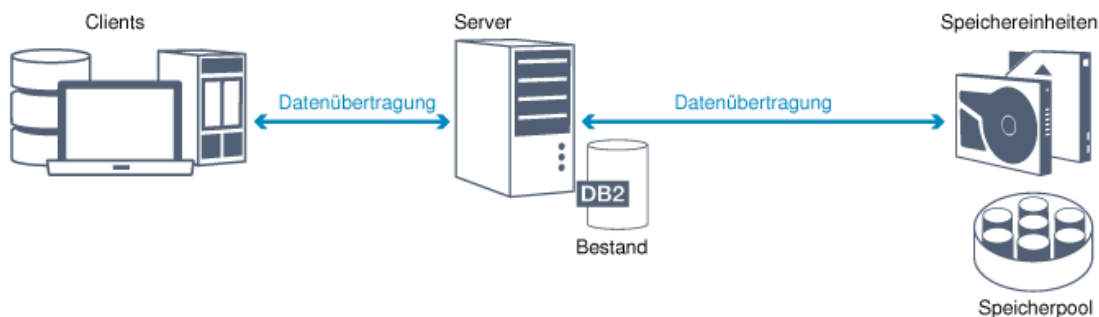
### Wiederherstellungsprotokoll

Aufzeichnungen von Datenbanktransaktionen werden in diesem Protokoll aufbewahrt. Die Datenbank verwendet das Wiederherstellungsprotokoll, um Datenkonsistenz in der Datenbank zu gewährleisten.

## Clientsysteme und -anwendungen

*Clients* sind Anwendungen, virtuelle Maschinen und Systeme, die geschützt werden müssen. Die Clients senden Daten an den Server (siehe Abbildung 1).

Abbildung 1. Komponenten in der Datensuchtlösung



### Client-Software

Damit IBM Spectrum Protect Clientdaten schützen kann, muss auf dem Clientsystem die entsprechende Software installiert sein und der Client muss beim Server registriert sein.

### Clientknoten

Ein *Clientknoten* ist äquivalent zu einem Computer, einer virtuellen Maschine oder einer Anwendung, wie beispielsweise ein Client für Sichern/Archivieren, der auf einer Workstation für Dateisystemsicherungen installiert ist. Jeder Clientknoten muss beim Server registriert sein. Auf einem einzelnen Computer können mehrere Knoten registriert sein.

## Speichermedien

Der Server speichert Clientdaten auf Speichermedien. Die folgenden Typen von Medien werden verwendet:

### Speichereinheiten

Der Server kann Daten auf Festplattenlaufwerke, Plattenarrays und -subsysteme, Standalone-Bandlaufwerke, Bandarchive und andere Typen von Speicher mit wahlfreiem und sequenziellem Zugriff schreiben. Speichereinheiten können direkt mit dem Server verbunden werden oder über ein lokales Netz (LAN) oder ein Speicherbereichsnetz (SAN).

### Speicherpools

Speichereinheiten, die mit dem Server verbunden sind, werden in *Speicherpools* gruppiert. Jeder Speicherpool stellt eine Gruppe von Speichereinheiten desselben Datenträgertyps dar, wie beispielsweise Platten- oder Bandlaufwerke. IBM Spectrum Protect speichert alle Clientdaten in Speicherpools. Sie können Speicherpools in einer *Hierarchie* anordnen, sodass Datenspeicher aus Plattenspeicher in kostengünstigeren Speicher, wie beispielsweise Bänder, übertragen werden kann.

## Datenschutzservices

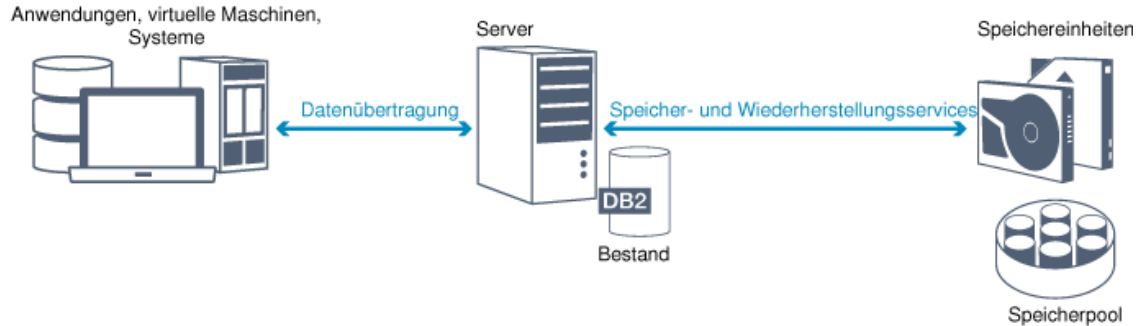
IBM Spectrum Protect stellt Datenschutzservices zum Speichern und Wiederherstellen von Daten für verschiedene Clienttypen bereit. Die Datenschutzservices werden über Maßnahmen implementiert, die auf dem Server definiert sind. Die Datenschutzservices können mithilfe der Clientzeitplanung automatisiert werden.



## Typen von Datenschutzservices

IBM Spectrum Protect stellt Services zum Speichern und Wiederherstellen von Clientdaten bereit (siehe Abbildung 1).

Abbildung 1. Datenschutzservices



IBM Spectrum Protect stellt die folgenden Typen von Datenschutzservices bereit:

### Sicherungs- und Zurückschreibungsservices

Sie führen einen Sicherungsprozess aus, um eine Kopie eines *Datenobjekts* zu erstellen, das für die Wiederherstellung verwendet werden kann, wenn das ursprüngliche Datenobjekt verloren geht. Ein Datenobjekt kann eine Datei, ein Verzeichnis oder ein benutzerdefiniertes Datenobjekt, wie beispielsweise eine Datenbank, sein.

Um die Nutzung von Systemressourcen während der Sicherungsoperation zu minimieren, verwendet IBM Spectrum Protect die *progressive Teilsicherung*. Bei dieser Sicherungsmethode wird eine erste Gesamtsicherung aller Datenobjekte erstellt und in nachfolgenden Sicherungsoperationen werden nur geänderte Daten in den Speicher versetzt. Verglichen mit Teil- und Differenzsicherungen, bei denen regelmäßige Gesamtsicherungen erforderlich sind, bietet die progressive Teilsicherung die folgenden Vorteile:

- Die Datenredundanz wird reduziert.
- Es wird weniger Netzbandbreite verwendet.
- Es ist weniger Speicherbereich im Speicherpool erforderlich.

Um die Speicherkapazitätsanforderungen und Netzbandbreitennutzung weiter zu reduzieren, schließt IBM Spectrum Protect die *Datendeduplizierung* für Datensicherungen ein. Beim Datendeduplizierungsverfahren werden doppelte Datenbereiche aus Sicherungen entfernt.

Sie führen einen Zurückschreibungsprozess aus, um ein Objekt aus einem Speicherpool auf den Client zu kopieren. Sie können eine einzelne Datei, alle Dateien in einem Verzeichnis oder alle Daten auf einem Computer zurückschreiben.

### Archivierungs- und Abrufservices

Der Archivierungsservice dient zum Aufbewahren von Daten für die Langzeitspeicherung, wie beispielsweise für die Einhaltung gesetzlicher Bestimmungen. Vom Archivierungsservice werden die folgenden Funktionen bereitgestellt:

- Beim Archivieren von Daten können Sie angeben, wie lange die Daten gespeichert werden müssen.
- Sie können das Kopieren von Dateien und Verzeichnissen für die Langzeitspeicherung auf Datenträgern anfordern. Beispielsweise können Sie diese Daten auf einer Bänderinheit speichern, wodurch die Speicherkosten gesenkt werden können.
- Sie können angeben, dass die ursprünglichen Dateien nach der Archivierung vom Client gelöscht werden.

Vom Abrufservice werden die folgenden Funktionen bereitgestellt:

- Beim Abrufen von Daten werden die Daten aus einem Speicherpool auf einen Clientknoten kopiert.
- Die Abrufoperation hat keine Auswirkungen auf die Archivierungskopie im Speicherpool.

### Umlagerungs- und Rückrufservices

Umlagerungs- und Rückrufservices dienen zur Verwaltung von Speicherbereich auf Clientsystemen. Ziel der Speicherbereichsverwaltung ist es, die verfügbare Datenträgerkapazität für neue Daten zu maximieren und die Zeit für den Zugriff auf Daten zu minimieren. Sie können Daten in Serverspeicher umlagern, damit immer genügend freier Speicherbereich in einem lokalen Dateisystem vorhanden ist. Zum Speichern umgelagerter Daten bestehen die folgenden Möglichkeiten:

- In Plattenspeicher für die Langzeitspeicherung
- In einem *virtuellen Bandarchiv* (VTL = Virtual Tape Library) für den schnellen Rückruf von Dateien

Sie können Dateien bei Bedarf automatisch oder selektiv auf den Clientknoten zurückrufen.

## Typen von Clientdaten, die geschützt werden können

Sie können Daten für die folgenden Clienttypen mit IBM Spectrum Protect schützen:

### Anwendungsclients

IBM Spectrum Protect kann Daten für bestimmte Produkte oder Anwendungen schützen. Diese Clients werden als *Anwendungsclients* bezeichnet. Um die *strukturierten Daten* für diese Clients, das heißt die Daten in Datenbankfeldern, zu schützen, müssen Sie Komponenten sichern, die für die Anwendung spezifisch sind. Mit IBM Spectrum Protect können die folgenden Anwendungen geschützt werden:

- IBM Spectrum Protect for Enterprise Resource Planning-Clients:
  - Data Protection for SAP HANA
  - Data Protection for SAP for DB2
  - Data Protection for SAP for Oracle
- IBM Spectrum Protect for Databases-Clients:
  - Data Protection for Microsoft SQL Server
  - Data Protection for Oracle
- IBM Spectrum Protect for Mail-Clients:
  - Data Protection for IBM® Domino
  - Data Protection for Microsoft Exchange Server

### Virtuelle Maschinen

Virtuelle Maschinen, die unter Verwendung von Anwendungsclient-Software gesichert werden, die auf der virtuellen Maschine installiert ist. In der IBM Spectrum Protect-Umgebung kann eine virtuelle Maschine mithilfe von IBM Spectrum Protect for Virtual Environments geschützt werden.

### Systemclients

Die folgenden IBM Spectrum Protect-Clients werden als *Systemclients* bezeichnet:

- Alle Clients, die Daten in Dateien und Verzeichnissen sichern, das heißt *unstrukturierte Daten*, wie Clients für Sichern/Archivieren und API-Clients, die auf Workstations installiert sind.
- Ein Server in einer Konfiguration für virtuelle Datenträger für die Kommunikation zwischen Servern.
- Eine virtuelle Maschine, die unter Verwendung der Software von Clients für Sichern/Archivieren gesichert wird, die auf der virtuellen Maschine installiert ist.

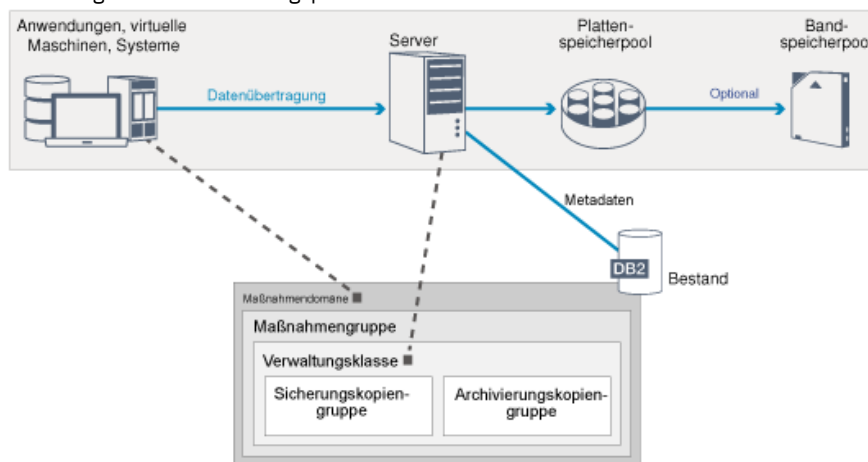
## Prozesse zur Verwaltung des Datenschutzes mit IBM Spectrum Protect

Der IBM Spectrum Protect-Serverbestand übernimmt eine wichtige Rolle in den Prozessen für den Datenschutz. Sie definieren Maßnahmen, die der Server zum Verwalten des Datenspeichers verwendet.

### Datenverwaltungsprozess

Abbildung 1 zeigt den IBM Spectrum Protect-Datenverwaltungsprozess.

Abbildung 1. Datenverwaltungsprozess



IBM Spectrum Protect verwendet Maßnahmen, um zu steuern, wie der Server Datenobjekte auf verschiedenen Typen von Speichereinheiten und -medien speichert und verwaltet. Sie ordnen einen Client einer Maßnahmendomäne zu, die eine einzelne aktive Maßnahmengruppe enthält. Wenn ein Client eine Datei sichert, archiviert oder umlagert, wird die Datei an eine Verwaltungsklasse in der aktiven Maßnahmengruppe der Maßnahmendomäne gebunden. Die Verwaltungsklasse und die Sicherungs- und

Archivierungskopiengruppen geben an, wo Dateien gespeichert werden und wie sie verwaltet werden. Wenn Sie Serverspeicher in einer Hierarchie konfigurieren, können Sie Dateien in andere Speicherpools umlagern.

## Bestandskomponenten

---

Die folgenden Bestandskomponenten sind Schlüsselkomponenten für den Betrieb des Servers:

### Serverdatenbank

Die Serverdatenbank enthält Informationen zu Clientdaten und Serveroperationen. In der Datenbank werden Informationen zu Clientdaten gespeichert, die als *Metadaten* bezeichnet werden. Informationen zu Clientdaten umfassen den Dateinamen, die Dateigröße, den Dateieigner, die Verwaltungsklasse, die Kopiengruppe sowie die Position der Datei im Serverspeicher. Die Datenbank umfasst die folgenden Informationen, die für den Betrieb des Servers erforderlich sind:

- Definitionen von Clientknoten und Administratoren
- Maßnahmen und Zeitpläne
- Servereinstellungen
- Aufzeichnungen von Serveroperationen wie Aktivitätenprotokolle und Ereignissätze
- Zwischenergebnisse für Verwaltungsabfragen

### Wiederherstellungsprotokoll

Der Server zeichnet Datenbanktransaktionen im Wiederherstellungsprotokoll auf. Mithilfe des Wiederherstellungsprotokolls kann sichergestellt werden, dass ein Fehler nicht zu einem inkonsistenten Zustand der Datenbank führt. Das Wiederherstellungsprotokoll wird außerdem dazu verwendet, die Konsistenz über Startoperationen des Servers hinweg zu gewährleisten. Das Wiederherstellungsprotokoll umfasst die folgenden Protokolle:

#### Aktive Protokolldatei

Mit diesem Protokoll werden aktuelle Transaktionen auf dem Server aufgezeichnet. Diese Informationen sind erforderlich, um den Server und die Datenbank nach einem Katastrophenfall zu starten.

#### Protokollspiegel (optional)

Der Spiegel der aktiven Protokolldatei ist eine Kopie der aktiven Protokolldatei, die verwendet werden kann, wenn die aktiven Protokolldateien nicht gelesen werden können. Alle Änderungen, die an der aktiven Protokolldatei vorgenommen werden, werden auch in einen Protokollspiegel geschrieben. Sie können nur einen einzigen Spiegel der aktiven Protokolldatei konfigurieren.

#### Archivprotokoll

Das Archivprotokoll enthält Kopien von geschlossenen Protokolldateien, die in der aktiven Protokolldatei enthalten waren. Das Archivprotokoll wird in Datenbanksicherungen eingeschlossen und für die Wiederherstellung der Serverdatenbank verwendet. Archivprotokolldateien, die in eine Datenbanksicherung eingeschlossen werden, werden automatisch bereinigt, nachdem ein vollständiger Datenbankzyklus abgeschlossen ist. Im Archivprotokoll muss genügend Speicherbereich verfügbar sein, um die Protokolldateien für Datenbanksicherungen speichern zu können.

#### Archivübernahmeprotokoll (optional)

Das Archivübernahmeprotokoll, das auch als sekundäres Archivprotokoll bezeichnet wird, ist das Verzeichnis, in dem der Server Archivprotokolldateien speichert, wenn das Archivprotokollverzeichnis voll ist.

## Auf Maßnahmen basierende Datenverwaltung

---

In der IBM Spectrum Protect-Umgebung enthält eine *Maßnahme* für die Verwaltung des Datenschutzes Regeln, die festlegen, wie Clientdaten gespeichert und verwaltet werden. Der Hauptzweck einer Maßnahme ist die Implementierung der folgenden Datenverwaltungsziele:

- Steuerung, in welchem Speicherpool Clientdaten anfänglich gespeichert werden
- Definition von Aufbewahrungskriterien, die steuern, wie viele Kopien von Objekten gespeichert werden
- Definition der Aufbewahrungsdauer der Objektkopien

Die auf Maßnahmen basierende Datenverwaltung ermöglicht es Ihnen, den Fokus statt auf die Verwaltung von Speichereinheiten und -medien auf Geschäftsanforderungen für den Schutz von Daten zu richten. Administratoren definieren Maßnahmen und ordnen Clientknoten einer *Maßnahmendomäne* zu.

Abhängig von Ihren Geschäftsanforderungen können eine oder mehrere Maßnahmen vorhanden sein. Beispielsweise können in einem Unternehmen verschiedene Abteilungen mit unterschiedlichen Typen von Daten angepasste Speicherverwaltungspläne haben. Maßnahmen können aktualisiert werden und die Aktualisierungen können auf bereits verwaltete Daten angewendet werden.

Wenn Sie IBM Spectrum Protect installieren, ist bereits eine Standardmaßnahme mit dem Namen STANDARD definiert. Die Maßnahme STANDARD stellt grundlegenden Sicherungsschutz für Benutzerworkstations bereit. Um unterschiedliche Service-Levels für unterschiedliche Clients bereitzustellen, können Sie die Standardmaßnahme ergänzen oder eine neue Maßnahme erstellen.

Sie erstellen Maßnahmen, indem Sie die folgenden Maßnahmenkomponenten definieren:

#### Maßnahmendomäne

Die Maßnahmendomäne ist die primäre Organisationsmethode zur Gruppierung von Clientknoten, die allgemeine Regeln für die Datenverwaltung gemeinsam nutzen. Obwohl ein Clientknoten für mehr als einen Server definiert werden kann, kann der Clientknoten nur für eine einzige Maßnahmendomäne auf jedem Server definiert werden.

#### Maßnahmengruppe

Eine *Maßnahmengruppe* umfasst eine Reihe von Maßnahmen, die in einer Gruppe zusammengefasst sind, sodass die Maßnahme für die Clientknoten in der Domäne nach Bedarf aktiviert oder inaktiviert werden kann. Ein Administrator verwendet eine Maßnahmengruppe, um unterschiedliche Verwaltungsklassen auf der Basis von Geschäfts- und Benutzeranforderungen zu implementieren. Eine Maßnahmendomäne kann mehrere Maßnahmengruppen enthalten, in der Domäne kann jedoch jeweils nur eine einzige Maßnahmengruppe aktiv sein. Jede Maßnahmengruppe enthält eine Standardverwaltungs-klasse und eine beliebige Anzahl weiterer Verwaltungsklassen.

#### Verwaltungs-klasse

Eine *Verwaltungs-klasse* ist ein Maßnahmenobjekt, das Sie an eine beliebige Kategorie von Daten binden können, um anzugeben, wie der Server die Daten verwaltet. Es können eine oder mehrere Verwaltungsklassen vorhanden sein. Eine der Verwaltungsklassen wird als Standardverwaltungs-klasse festgelegt, die von Clients verwendet wird, es sei denn, für den Client ist eine bestimmte Verwaltungsklasse festgelegt, die den Standardwert überschreibt.

Die Verwaltungsklasse kann eine Sicherungskopiengruppe, eine Archivierungskopiengruppe und Speicherverwaltungsattribute enthalten. Eine Kopiengruppe legt fest, wie der Server Sicherungs-versionen oder archivierte Kopien der Datei verwaltet. Die Speicherverwaltungsattribute legen fest, ob die Datei für die Umlagerung in Serverspeicher vom Client für das Speicherplatzmanagement auswählbar ist, und unter welchen Bedingungen die Datei umgelagert wird.

#### Kopiengruppe

Eine *Kopiengruppe* ist eine Gruppe von Attributen in einer Verwaltungsklasse, die die Folgendes steuert:

- Wo der Server Versionen von gesicherten Dateien oder Archivierungskopien speichert
- Wie lange der Server Versionen von gesicherten Dateien oder Archivierungskopien aufbewahrt
- Wie viele Versionen von Sicherungskopien aufbewahrt werden
- Welche Methode zum Generieren der Versionen von gesicherten Dateien oder Archivierungskopien verwendet werden soll

## Sicherheitsmanagement

---

IBM Spectrum Protect umfasst Sicherheitsfunktionen für die Registrierung von Administratoren und Benutzern. Nachdem Administratoren registriert wurden, muss ihnen Berechtigung erteilt werden, indem ihnen eine oder mehrere Berechtigungsklassen für Verwaltungsaufgaben zugeordnet werden. Ein Administrator mit Systemberechtigung kann jede Serverfunktion ausführen. Administratoren mit Maßnahmen-, Speicher-, Bediener- oder Knotenberechtigung können Untergruppen von Serverfunktionen ausführen. Der Zugriff auf den Server kann mithilfe jeder der folgenden Methoden, die jeweils über ein Kennwort gesteuert werden, erfolgen:

- Administratorzugriff zum Verwalten des Servers
- Clientzugriff auf Knoten zum Speichern und Abrufen von Daten

Außerdem stehen Funktionen zur Verfügung, die dazu beitragen können, die Sicherheit zu gewährleisten, wenn Clients eine Verbindung zum Server herstellen. Abhängig von Geschäftsanforderungen können Sie als Administrator eine der folgenden Clientregistrierungsmethoden auswählen:

#### Offene Registrierung

Wenn der Client zum ersten Mal die Verbindung zum Server herstellt, wird der Benutzer zur Eingabe eines Knotennamens, eines Kennworts und der Kontaktinformationen aufgefordert. Bei der offenen Registrierung werden dem Benutzer die folgenden Standardeinstellungen zur Verfügung gestellt:

- Der Clientknoten ist der Maßnahmendomäne STANDARD zugeordnet.
- Der Benutzer kann definieren, ob Dateien komprimiert werden, um das über Netze gesendete Datenvolumen und den von den Daten im Speicher belegten Speicherbereich zu reduzieren.
- Der Benutzer kann archivierte Kopien von Dateien aus Serverspeicher löschen, aber keine Sicherungs-versionen von Dateien.

#### Geschlossene Registrierung

Die geschlossene Registrierung ist die Standardmethode für die Registrierung des Clients beim Server. Bei diesem Typ von Registrierung werden alle Clients von einem Administrator registriert. Der Administrator kann die folgenden Einstellungen implementieren:

- Zuordnung des Knotens zu einer beliebigen Maßnahmendomäne
- Festlegung, ob der Benutzer die Komprimierung verwenden kann oder nicht oder ob der Benutzer die Wahl hat
- Steuerung, ob der Benutzer gesicherte Dateien oder archivierte Dateien löschen kann

Sie können weiteren Schutz für Ihre Daten und Kennwörter hinzufügen, indem Sie Secure Sockets Layer (SSL) verwenden. SSL ist die Standardtechnologie, mit der verschlüsselte Sitzungen für Server und Clients erstellt werden; SSL stellt einen sicheren Kanal für die Kommunikation über offene Kommunikationspfade zur Verfügung. Bei SSL wird die Identität des Servers mithilfe digitaler Zertifikate geprüft. Wenn die Authentifizierung mit einem Lightweight Directory Access Protocol-Server (LDAP-Server) erfolgt, werden Kennwörter zwischen dem Server und dem LDAP-Server durch TLS (Transport Layer Security) geschützt. Das TLS-Protokoll ist der Nachfolger des SSL-Protokolls. Bei der Kommunikation zwischen einem Server und einem Client wird mithilfe von TLS sichergestellt, dass Nachrichten nicht von Dritten abgefangen werden können.

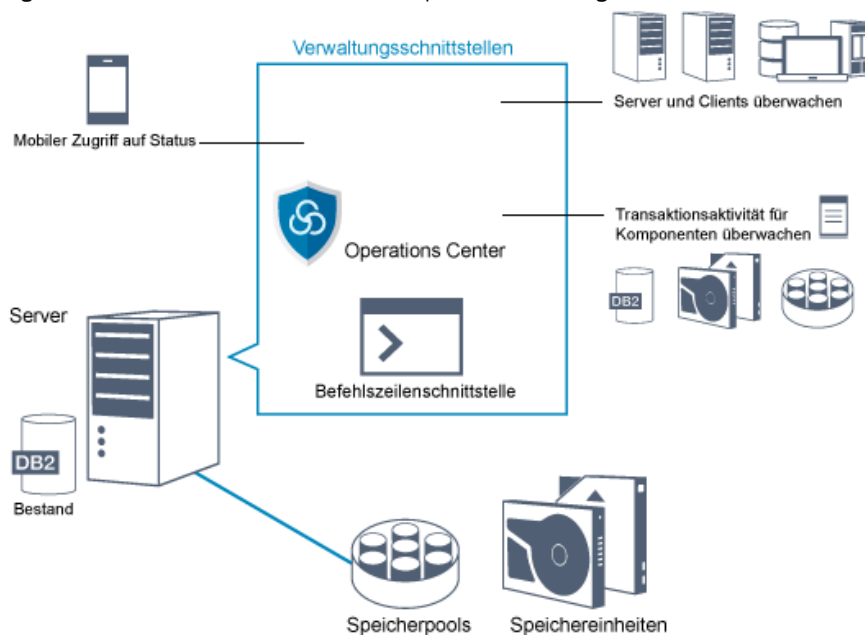
## Benutzerschnittstellen für die IBM Spectrum Protect-Umgebung

Für Überwachungs- und Konfigurationstasks stellt IBM Spectrum Protect verschiedene Schnittstellen, einschließlich des Operations Center, einer Befehlszeilenschnittstelle und einer SQL-Verwaltungsschnittstelle, bereit.

### Schnittstellen für die Datenspeicherverwaltung

Das Operations Center ist die primäre Schnittstelle für Administratoren zur Überwachung und Verwaltung von Servern. Ein Hauptvorteil des Operations Center ist die Möglichkeit, mehrere Server überwachen zu können (siehe Abbildung 1). Sie können IBM Spectrum Protect auch über eine Befehlszeilenverwaltungsschnittstelle überwachen und verwalten.

Abbildung 1. Benutzerschnittstellen für die Datenspeicherverwaltung



Für die Interaktion mit IBM Spectrum Protect können Sie die folgenden Schnittstellen verwenden:

#### Operations Center

Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. Mithilfe des Operations Center können Sie Überwachungstasks und bestimmte Verwaltungstasks ausführen, wie beispielsweise:

- Überwachung mehrerer Server und Clients
- Überwachung der Transaktionsaktivität für bestimmte Komponenten im Datenpfad, wie beispielsweise die Serverdatenbank, das Wiederherstellungsprotokoll, Speichereinheiten und Speicherpools

#### Befehlszeilenschnittstelle

Mithilfe einer Befehlszeilenschnittstelle können Sie Verwaltungstasks für Server ausführen. Der Zugriff auf die Befehlszeilenschnittstelle kann entweder über den IBM Spectrum Protect-Verwaltungsclient oder das Operations Center erfolgen.

#### Zugriff auf Informationen in der Serverdatenbank mithilfe von SQL-Anweisungen

Mithilfe von SQL-Anweisungen SELECT können Sie die Serverdatenbank abfragen und die Ergebnisse anzeigen. SQL-Tools anderer Anbieter sind verfügbar, um Administratoren bei der Datenbankverwaltung zu unterstützen.

### Schnittstellen für die Verwaltung der Clientaktivität

IBM Spectrum Protect stellt die folgenden Typen von Schnittstellen zur Verwaltung der Clientaktivität bereit:

- Anwendungsprogrammierschnittstelle (API)
- Grafische Benutzerschnittstellen für Clients

- Browserschnittstelle für den Client für Sichern/Archivieren
- Befehlszeilenschnittstellen für Clients

## Konzepte der Datenspeicherung in IBM Spectrum Protect

IBM Spectrum Protect stellt Funktionen zum Speichern von Daten in Einheitenspeicher und externem Speicher bereit.

Um dem Server Speichereinheiten zur Verfügung zu stellen, müssen Sie die Speichereinheiten anschließen und Speicherpools Einheitenklassen, Speicherarchiven und Laufwerken zuordnen.

- Typen von Speichereinheiten  
Zur Erreichung bestimmter Datenschutzziele können verschiedene Speichereinheiten in IBM Spectrum Protect verwendet werden.
- Datenspeicherung in Speicherpools  
Logische Speicherpools sind die Hauptkomponenten im IBM Spectrum Protect-Modell der Datenspeicherung. Die Verwendung von Speichereinheiten kann optimiert werden, indem die Merkmale von Speicherpools und Datenträgern bearbeitet werden.
- Datenübertragung über Netze in Speicher  
Die IBM Spectrum Protect-Umgebung bietet verschiedene Möglichkeiten, um Daten über verschiedene Typen von Netzen und Konfigurationen sicher in Speicher zu versetzen.

## Typen von Speichereinheiten

Zur Erreichung bestimmter Datenschutzziele können verschiedene Speichereinheiten in IBM Spectrum Protect verwendet werden.

## Speichereinheiten und Speicherobjekte

Der IBM Spectrum Protect-Server kann mit einer Kombination aus manuellen und automatisierten Speichereinheiten verbunden werden. IBM Spectrum Protect kann mit den folgenden Typen von Speichereinheiten verbunden werden:

- Platteneinheiten, die direkt angeschlossen, an ein SAN angeschlossen oder an ein Netz angeschlossen sind
- Physische Bandeinheiten, die manuell oder automatisch betrieben werden
- Virtuelle Bandeinheiten
- Cloudobjektspeicher

IBM Spectrum Protect stellt physische Speichereinheiten und Datenträger durch Speicherobjekte dar, die Sie in der Serverdatenbank definieren. Speicherobjekte klassifizieren verfügbare Speicherressourcen und handhaben die Umlagerung von einem Speicherpool in einen anderen. In Tabelle 1 sind die Speicherobjekte in der Serverspeicherumgebung beschrieben.

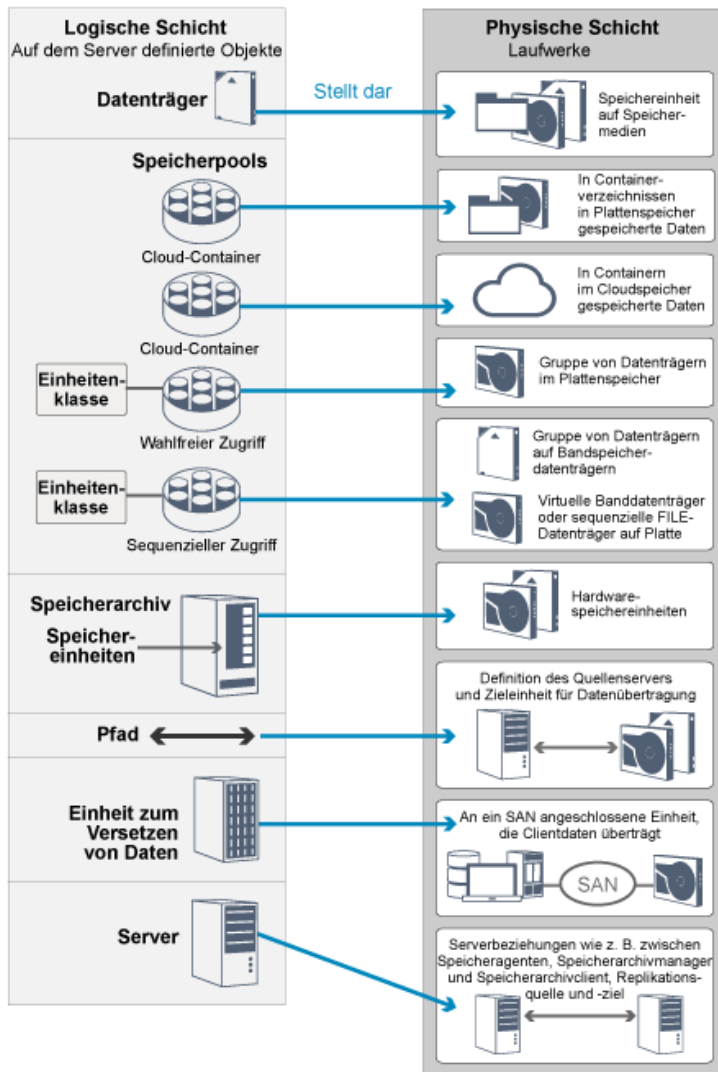
Tabelle 1. Speicherobjekte und Darstellungen

| Speicherobjekt        | Durch das Objekt dargestellte Ressource  |
|-----------------------|--|
| Datenträger           | Eine diskrete Speichereinheit auf Platte, Band oder anderen Speichermedien. Jeder Datenträger ist einem einzelnen Speicherpool zugeordnet.   |
| Speicherpool          | Eine Gruppe von Speicherdatenträgern oder Containern, die als Ziel zum Speichern von Clientdaten dient. IBM Spectrum Protect verwendet die folgenden Typen von Speicherpools: <ul style="list-style-type: none"> <li>• Verzeichniscontainerspeicherpools</li> <li>• Cloud-Containerspeicherpools</li> <li>• Speicherpools mit sequenziellem Zugriff, die einer Einheitenklasse zugeordnet sind</li> <li>• Speicherpools mit wahlfreiem Zugriff, die einer Einheitenklasse zugeordnet sind</li> </ul> |
| Container             | Eine Datenspeicherposition, beispielsweise eine Datei, ein Verzeichnis oder eine Einheit.  |
| Containerspeicherpool | Ein primärer Speicherpool, der von einem Server zum Speichern von Daten verwendet wird. Daten werden in Containern in Dateisystemverzeichnissen oder in Cloudspeicher gespeichert. Daten werden, falls erforderlich, dedupliziert, während der Server Daten in den Speicherpool schreibt.  |

| <b>Speicherobjekt</b>           | <b>Durch das Objekt dargestellte Ressource</b>  |
|---------------------------------|---|
| Einheitenklasse                 | Der Typ der Speichereinheit, der die Datenträger verwenden kann, die in einem Speicherpool mit sequenziellem Zugriff oder einem Speicherpool mit wahlfreiem Zugriff definiert sind. Jede Einheitenklasse für Typen austauschbarer Datenträger ist einem einzelnen Speicherarchiv zugeordnet.  |
| Speicherarchiv                  | Eine Speichereinheit. Beispielsweise kann ein Speicherarchiv ein Standalone-Laufwerk, eine Gruppe von Standalone-Laufwerken, eine automatisierte Einheit mit mehreren Laufwerken oder eine Gruppe von Laufwerken darstellen, die durch einen Datenträgermanager gesteuert wird.   |
| Laufwerk                        | Ein Objekt einer Bandarchivereinheit, die die Funktionalität zum Lesen und Schreiben von Daten von bzw. auf Bandarchivdatenträger bereitstellt. Jedes Laufwerk ist einem einzelnen Speicherarchiv zugeordnet.   |
| Pfad                            | Die Angabe der Datenquelle und der Zielposition der Einheit. Bevor eine Speichereinheit verwendet werden kann, muss ein Pfad zwischen der Einheit und dem Quellenserver, der Daten versetzt, definiert werden.  |
| Einheit zum Versetzen von Daten | Eine an ein SAN angeschlossene Einheit, die zur Übertragung von Clientdaten verwendet wird. Eine Einheit zum Versetzen von Daten wird nur bei einer Datenübertragung verwendet, bei der der Server nicht vorhanden ist, wie beispielsweise in einer NDMP-Umgebung. Einheiten zum Versetzen von Daten übertragen Daten zwischen Speichereinheiten, ohne viele Server-, Client- oder Netzressourcen zu verwenden. |
| Server                          | Ein Server, der von einem anderen IBM Spectrum Protect-Server verwaltet wird.   |

Der Administrator definiert die Speicherobjekte in der logischen Schicht des Servers (siehe Abbildung 1).

Abbildung 1. Speicherobjekte



## Platteneinheiten

Sie können Clientdaten auf Platteneinheiten mit den folgenden Datenträgertypen speichern:

- Verzeichnisse in Verzeichniscontainerspeicherpools
- Datenträger mit wahlfreiem Zugriff des Einheitentyps DISK
- Datenträger mit sequenziellem Zugriff des Einheitentyps FILE

IBM Spectrum Protect stellt die folgenden Funktionen bereit, wenn Sie Verzeichniscontainerspeicherpools für die Datenspeicherung verwenden:

- Dateneduplizierungs- und Plattencachingverfahren können angewendet werden, um die Datenspeichernutzung zu maximieren.
- Daten können sehr viel schneller von Platte als aus Bandspeicher abgerufen werden.

## Physische Bänderinheiten

In einem physischen Bandarchiv wird die Speicherkapazität als Gesamtzahl Datenträger in dem Speicherarchiv definiert. Physische Bänderinheiten können für die folgenden Aktivitäten verwendet werden:

- Speichern von Clientdaten, die von Clientknoten gesichert, archiviert oder umgelagert werden.
- Speichern von Datenbanksicherungen
- Exportieren von Daten auf einen anderen Server oder in Speicher an einem anderen Standort

Das Versetzen von Daten auf Band bietet die folgenden Vorteile:

- Daten für Clients können auf einer Platteneinheit verbleiben, während die Daten gleichzeitig auf Band versetzt werden.
- Die Leistung von Bandlaufwerken kann verbessert werden, indem Daten mittels Streaming von Platte auf Band umgelagert werden.



- Die Nutzungszeiten für Bandlaufwerke können verlängert werden, um die Effizienz der Bandlaufwerke zu verbessern.
- Daten auf Band können in Vaults an anderen Standorten versetzt werden.
- Der Stromverbrauch kann eingeschränkt werden, da Bandeinheiten nach dem Schreiben von Daten auf Band keinen Strom mehr verbrauchen.
- Verschlüsselung, die von der Bandlaufwerkhardware bereitgestellt wird, kann angewendet werden, um die Daten auf Band zu schützen.

Verglichen mit entsprechendem Plattenspeicher und virtuellem Bandspeicher sind die Einheitenkosten zum Speichern von Daten bei physischen Bandeinheiten tendenziell sehr viel geringer.

## Virtuelle Bandarchive

---

Ein virtuelles Bandarchiv (VTL) verwendet keine physischen Banddatenträger. Wenn Sie VTL-Speicher verwenden, werden die Zugriffsmechanismen von Bandhardware emuliert. In einem virtuellen Bandarchiv können Datenträger und Laufwerke definiert werden, um größere Flexibilität für die Speicherumgebung bereitzustellen. Die Speicherkapazität eines virtuellen Bandarchivs wird als insgesamt verfügbarer Plattenspeicherplatz definiert. Sie können die Anzahl und Größe der Datenträger auf der Platte erhöhen oder reduzieren.

Das Definieren eines virtuellen Bandarchivs für den IBM Spectrum Protect-Server kann zu einer Leistungsverbesserung führen, da der Server die Mountpunktverarbeitung für virtuelle Bandarchive anders als für reale Bandarchive handhabt. Obwohl die logischen Einschränkungen für Bandeinheiten weiterhin bestehen, gelten die physischen Einschränkungen für Bandhardware nicht für ein virtuelles Bandarchiv, das somit bessere Skalierbarkeit bietet. Sie können das virtuelle IBM Spectrum Protect-Bandarchiv verwenden, wenn die folgenden Bedingungen erfüllt sind:

- In dem virtuellen Bandarchiv wird nur ein einziger Typ und eine einzige Generation von Laufwerk und Datenträger emuliert.
- Jeder Server und jeder Speicheragent mit Zugriff auf das VTL hat Pfade, die für alle Laufwerke in dem Bandarchiv definiert sind.

## Datenspeicherung in Speicherpools

---

Logische Speicherpools sind die Hauptkomponenten im IBM Spectrum Protect-Modell der Datenspeicherung. Die Verwendung von Speichereinheiten kann optimiert werden, indem die Merkmale von Speicherpools und Datenträgern bearbeitet werden.

### Speicherpooltypen

---

Die Gruppe von Speicherpools, die Sie für den Server konfigurieren, wird als *Serverspeicher* bezeichnet. Im Serverspeicher können die folgenden Typen von Speicherpools definiert werden:

#### Primäre Speicherpools

Eine benannte Gruppe von Datenträgern, die der Server zum Speichern von Sicherungsversionen von Dateien, Archivierungskopien von Dateien und Dateien, die aus Clientknoten umgelagert werden, verwendet.

#### Kopienspeicherpools

Eine benannte Gruppe von Datenträgern, die Kopien von Dateien enthalten, die in primären Speicherpools gespeichert sind. Kopienspeicherpools werden nur zum Sichern der Daten verwendet, die in primären Speicherpools gespeichert sind. Ein Kopienspeicherpool kann nicht als Ziel für eine Sicherungskopiengruppe, eine Archivierungskopiengruppe oder eine Verwaltungsklasse für speicher verwaltete Dateien verwendet werden.

#### Containerkopienspeicherpools

Eine benannte Gruppe von Datenträgern, die eine Kopie der Datenbereiche enthalten, die in Verzeichniscontainerspeicherpools gespeichert sind. Containerkopienspeicherpools werden nur zum Schützen der Daten verwendet, die in Verzeichniscontainerspeicherpools gespeichert sind.

#### Speicherpools für aktive Daten

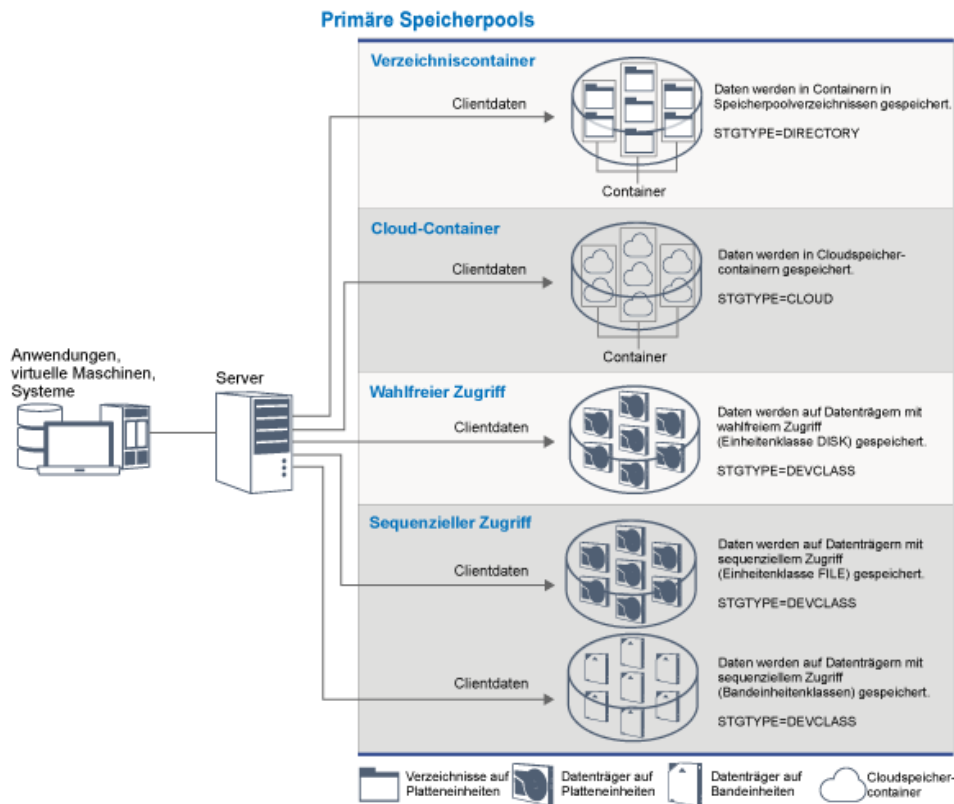
Eine benannte Gruppe von Speicherpooldatenträgern, die nur aktive Versionen von Clientsicherungsdaten enthalten.

### Primäre Speicherpools

---

Wenn Sie Dateidaten zurückschreiben, abrufen, zurückrufen oder exportieren, wird die angeforderte Datei aus einem primären Speicherpool abgerufen. Abhängig vom Typ des primären Speicherpools können sich die Speicherpools vor Ort oder an einen anderen Standort befinden. Primäre Speicherpools können in einer Speicherhierarchie angeordnet werden, sodass Daten aus Plattenspeicher in kostengünstigeren Speicher, wie beispielsweise Bandeinheiten, übertragen werden können. Abbildung 1 zeigt das Konzept primärer Speicherpools.

Abbildung 1. Primäre Speicherpools



Sie können die folgenden Typen primärer Speicherpools definieren:

#### Verzeichniscontainerspeicherpools

Ein Speicherpool, den der Server zum Speichern von Daten in Containern in Speicherpoolverzeichnissen verwendet. Daten, die in einem Verzeichniscontainerspeicherpool gespeichert sind, können entweder die Inline-Datendeduplizierung, die clientseitige Datendeduplizierung, die Inline-Komprimierung oder die clientseitige Komprimierung verwenden. Bei der Inline-Datendeduplizierung und der Inline-Komprimierung erfolgt die Reduktion der Daten zu dem Zeitpunkt, zu dem sie gespeichert werden.

Tipp: Daten, die zunächst komprimiert werden, können nicht dedupliziert werden; deduplizierte Daten können jedoch komprimiert werden.

Durch die Verwendung von Verzeichniscontainerspeicherpools entfällt die Notwendigkeit zur Datenträgerkonsolidierung, wodurch die Serverleistung verbessert und die Kosten der Speicherhardware reduziert werden. Daten in Verzeichniscontainerspeicherpools können auf der Ebene des Speicherpools geschützt und repariert werden. Sie können Daten, die in einem Cloud-Containerspeicherpool gespeichert sind, mit Tiering in einen Cloud-Containerspeicherpool versetzen.

Einschränkung: Folgende Funktionen können bei Verzeichniscontainerspeicherpools nicht verwendet werden:

- Umlagerung
- Konsolidierung
- Zusammenfassung
- Kollokation
- Gleichzeitiges Schreiben
- Speicherpoolsicherung
- Virtuelle Datenträger

#### Cloud-Containerspeicherpools

Ein Speicherpool, den ein Server zum Speichern von Daten in Cloudspeicher verwendet. Der Cloudspeicher kann sich vor Ort (on premises) oder außerhalb des Unternehmens (off premises) befinden. Bei Cloud-Containerspeicherpools, die von IBM Spectrum Protect bereitgestellt werden, können Daten in objektbasiertem Cloudspeicher gespeichert werden. Das Speichern von Daten in Cloud-Containerspeicherpools ermöglicht es Ihnen, die von Clouds gebotenen Vorteile der Kosten pro Einheit zusammen mit der vom Cloudspeicher bereitgestellten Skalierungsfunktionalität zu nutzen. Sie können Cloud-Tiering verwenden, um die Kosten zu senken, indem Sie Daten aus Plattenspeicher in einen Cloud-Containerspeicherpool versetzen. IBM Spectrum Protect verwaltet die Berechtigungsnachweise, Sicherheit, Lese- und Schreib-E/As sowie den Lebenszyklus für Daten, die in der Cloud gespeichert werden. Wenn Cloud-Containerspeicherpools auf dem Server implementiert werden, können Daten direkt in die Cloud geschrieben werden, indem ein Cloud-Containerspeicherpool mit den Clouberechtigungen konfiguriert wird. Daten, die in einem Cloud-Containerspeicherpool gespeichert sind, verwenden sowohl die Inline-Datendeduplizierung als auch die Inline-Komprimierung. Der Server schreibt deduplizierte, komprimierte und verschlüsselte Daten direkt in die Cloud. Sie können

Daten direkt im Cloud-Containerspeicherpool sichern und aus ihm zurückschreiben oder direkt im Cloud-Containerspeicherpool archivieren und aus ihm abrufen.

Sie können die folgenden Typen von Cloud-Containerspeicherpools definieren:

#### On premises

Sie können den On-Premises-Typ für Cloud-Containerspeicherpools verwenden, um Daten in einer privaten Cloud zu speichern, um mehr Sicherheit und maximale Kontrolle über Ihre Daten zu gewährleisten. Die Nachteile einer privaten Cloud sind höhere Kosten aufgrund der Hardwarevoraussetzungen und der Wartung vor Ort.

#### Off premises

Sie können den Off-Premises-Typ für Cloud-Containerspeicherpools verwenden, um Daten in einer öffentlichen Cloud zu speichern. Die Verwendung einer öffentlichen Cloud hat den Vorteil, dass die Kosten geringer sind als bei einer privaten Cloud, da beispielsweise die Wartung entfällt. Sie müssen jedoch diesen Vorteil und mögliche Leistungsprobleme aufgrund von Verbindungsgeschwindigkeiten und eingeschränkter Kontrolle über Ihre Daten gegeneinander abwägen.

Speicherpools, die Einheitenklassen zugeordnet sind

Sie können einen primären Speicherpool für die Verwendung der folgenden Typen von Speichereinheiten definieren:

#### Einheitenklasse DISK

In einem Speicherpool des Einheitentyps DISK werden Daten in Plattenblöcken mit wahlfreiem Zugriff gespeichert. Sie können Caching in DISK-Speicherpools verwenden, um die Clientzurückschreibungsleistung - mit einigen Einschränkungen bei der Serververarbeitung - zu verbessern. Die Speicherbereichszuordnung und -überwachung nach Blöcken verwendet mehr Datenbankspeicherbereich und erfordert eine höhere Verarbeitungsleistung als die Zuordnung und Überwachung nach Datenträger.

#### Einheitenklasse FILE

In einem Speicherpool des Einheitentyps FILE werden Dateien auf sequenziellen Datenträgern gespeichert, da hierbei die sequenzielle Leistung besser als bei der Speicherung in Plattenblöcken ist. Für den Server haben diese Dateien die Merkmale eines Banddatenträgers, sodass dieser Typ von Speicherpool für die Umlagerung auf Band besser geeignet ist. FILE-Datenträger sind für das *elektronische Vaulting* geeignet, bei dem ein Band nicht physisch an einen fernen Standort transportiert wird, sondern Daten elektronisch an einen fernen Standort übertragen werden. Im Allgemeinen wird dieser Typ von Speicherpool gegenüber DISK-Speicherpools bevorzugt.

Der Server verwendet die folgenden primären Standardspeicherpools mit wahlfreiem Zugriff:

#### ARCHIVEPOOL

In der Maßnahme STANDARD ist dieser Speicherpool das Ziel für Dateien, die von Clientknoten archiviert werden.

#### BACKUPPOOL

In der Maßnahme STANDARD ist dieser Speicherpool das Ziel für Dateien, die von Clientknoten gesichert werden.

#### SPACEMGPOOL

Dieser Speicherpool ist für speicher verwaltete Dateien, die von IBM Spectrum Protect for Space Management-Clientknoten umgelagert werden.

## Kopierspeicherpools

Kopierspeicherpools enthalten aktive und inaktive Versionen von Daten, die aus primären Speicherpools gesichert werden. Ein Verzeichniscontainerspeicherpool kann nicht als Kopierspeicherpool verwendet werden. Außerdem können Daten aus einem Verzeichniscontainerspeicherpool nicht in einen Kopierspeicherpool kopiert werden. Um Verzeichniscontainerspeicherpools zu schützen, kopieren Sie die Daten in einen Containerkopierspeicherpool. Abbildung 2 zeigt das Konzept von Kopierspeicherpools.



Kopierspeicherpools dienen der Wiederherstellung nach einem Katastrophenfall oder nach Datenträgerfehlern. Wenn beispielsweise ein Client versucht, eine beschädigte Datei aus dem primären Speicherpool abzurufen, wenn der Speicherpool nicht verfügbar oder die Datei in dem Speicherpool beschädigt ist, kann der Client die Daten aus dem Kopierspeicherpool zurückschreiben.

Die Datenträger in Kopierspeicherpools können ausgelagert und dennoch weiterhin vom Server verfolgt werden. Die Auslagerung dieser Datenträger ermöglicht die Wiederherstellung nach einem Katastrophenfall vor Ort. Ein Kopierspeicherpool kann nur Speicher mit sequenziellem Zugriff, wie beispielsweise eine Bandeinheitenklasse oder eine Einheitenklasse FILE, verwenden.

## Containerkopierspeicherpools

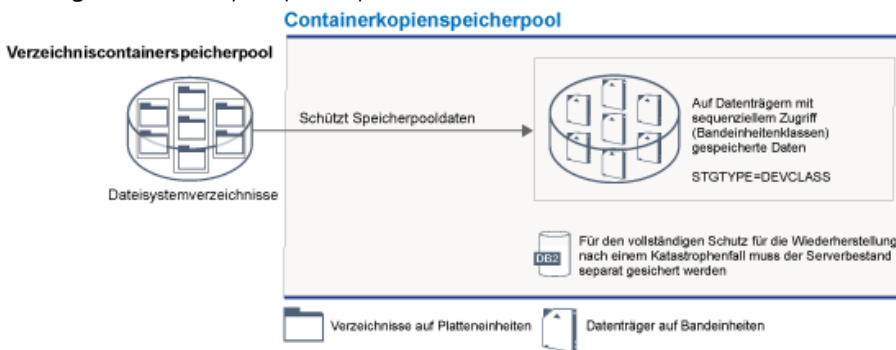
Ein Server kann einen Verzeichniscontainerspeicherpool schützen, indem er Kopien der Daten in einem Containerkopierspeicherpool speichert. Daten in Containerkopierspeicherpools werden auf Banddatenträgern gespeichert, die vor Ort oder an einem anderen Standort aufbewahrt werden können. Beschädigte Daten in Verzeichniscontainerspeicherpools können mithilfe deduplizierter Speicherbereiche in Containerkopierspeicherpools repariert werden. Containerkopierspeicherpools stellen eine Alternative zur Verwendung eines Replikationsservers zum Schützen von Daten in einem Verzeichniscontainerspeicherpool dar.

Einschränkung: Wenn alle Serverdaten verloren gehen, stellen Containerkopierspeicherpools alleine nicht dieselbe Schutzstufe wie die Replikation bereit:

- Bei der Replikation können Sie Clientdaten direkt vom Zielsystem zurückschreiben, wenn der Quellenserver nicht verfügbar ist.
- Bei Containerkopierspeicherpools müssen Sie zunächst den Server aus einer Datenbanksicherung zurückschreiben und dann die Verzeichniscontainerspeicherpools mithilfe von Banddatenträgern reparieren.

Abbildung 3 zeigt das Konzept von Containerkopierspeicherpools.

Abbildung 3. Containerkopierspeicherpools



Abhängig von Ihrer Systemkonfiguration können Sie Zeitpläne für den Schutz erstellen, um gemäß Ihren Anforderungen die Daten im Verzeichniscontainerspeicherpool gleichzeitig in Containerkopierspeicherpools vor Ort oder an einem anderen Standort zu kopieren:

- Wenn die Replikation aktiviert ist, können Sie einen einzelnen Containerkopierspeicherpool an einem anderen Standort erstellen. Mithilfe der Kopie an dem anderen Standort kann zusätzlicher Schutz in einer replizierten Umgebung bereitgestellt werden.
- Wenn die Replikation nicht aktiviert ist, können Sie einen einzelnen Containerkopierspeicherpool vor Ort und einen einzelnen Containerkopierspeicherpool an einem anderen Standort erstellen.

Abhängig von den Ressourcen und Anforderungen Ihres Standorts bietet die Möglichkeit, Verzeichniscontainerspeicherpools auf Band zu kopieren, die folgenden Vorteile:

- Die Notwendigkeit, einen weiteren Server und weiteren Plattenspeicherplatz zu verwalten, entfällt.
- Daten werden in Speicherpools kopiert, die auf dem Server definiert sind. Die Leistung ist nicht von der Netzverbindung zwischen Servern abhängig oder von ihr betroffen.
- Sie können gesetzliche Bestimmungen und Geschäftsanforderungen für Bandkopien an einem anderen Standort erfüllen.

## Speicherpools für aktive Daten

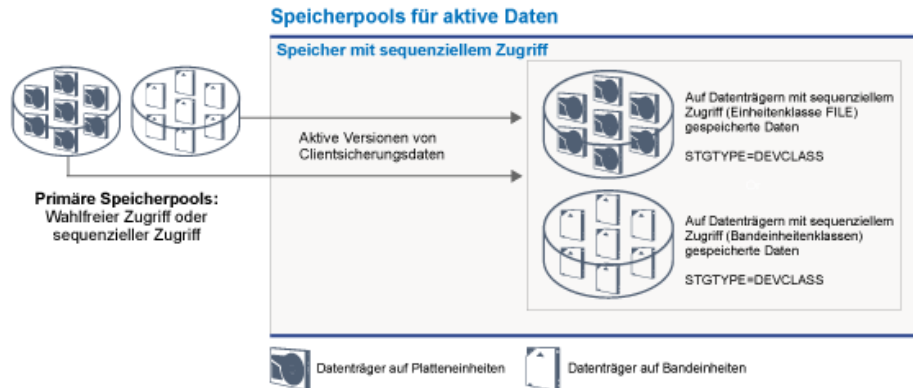
Ein Pool für aktive Daten enthält nur aktive Versionen von Clientsicherungsdaten. In diesem Fall muss der Server keine Positionierung hinter inaktive Dateien ausführen, die nicht zurückgeschrieben werden müssen. Ein Verzeichniscontainerspeicherpool kann nicht als Speicherpool für aktive Daten verwendet werden. Pools für aktive Daten werden verwendet, um die Effizienz von Datenspeicher- und Zurückschreibungsoperationen zu verbessern. Beispielsweise kann Sie dieser Typ von Speicherpool beim Erreichen der folgenden Ziele unterstützen:

- Erhöhen der Geschwindigkeit von Zurückschreibungsoperationen für Clientdaten
- Reduzieren der Anzahl Speicherdatenträger vor Ort oder an einem anderen Standort
- Reduzieren des Datenvolumens, das beim Kopieren oder Zurückschreiben von Dateien übertragen wird, die durch elektronisches Vaulting an einem fernen Standort geschützt werden.

Daten, die von Clients für die hierarchische Speicherverwaltung (HSM-Clients) umgelagert werden, und Archivierungsdaten sind in Pools für aktive Daten nicht zulässig. Während aktualisierte Versionen von Sicherungsdaten in Pools für aktive Daten gespeichert werden, werden ältere Versionen entfernt, da die verbleibenden Daten von einer großen Anzahl Datenträger mit sequenziellem Zugriff auf einer

geringeren Anzahl neuer Datenträger mit sequenziellem Zugriff konsolidiert werden. Abbildung 4 zeigt das Konzept von Speicherpools für aktive Daten.

Abbildung 4. Speicherpools für aktive Daten



Pools für aktive Daten können jeden Typ von Speicher mit sequenziellem Zugriff verwenden. Die Vorteile eines Pools für aktive Daten sind jedoch von dem Einheitentyp abhängig, der dem Pool zugeordnet ist. Beispielsweise sind Pools für aktive Daten, die einer Einheitenklasse FILE zugeordnet sind, aus den folgenden Gründen bestens für Clientschnellzurückschreibungsoperationen geeignet:

- FILE-Datenträger müssen nicht physisch bereitgestellt werden.
- Clientsitzungen, die Daten von FILE-Datenträgern in einen Pool für aktive Daten zurückschreiben, können gleichzeitig auf die Datenträger zugreifen, wodurch die Zurückschreibungsleistung verbessert wird.

**Zugehörige Informationen:**

- ➔ Häufig gestellte Fragen (FAQs) zu Verzeichniscontainerspeicherpools
- ➔ Häufig gestellte Fragen (FAQs) zu Cloud-Containerspeicherpools

## Datenübertragung über Netze in Speicher

Die IBM Spectrum Protect-Umgebung bietet verschiedene Möglichkeiten, um Daten über verschiedene Typen von Netzen und Konfigurationen sicher in Speicher zu versetzen.

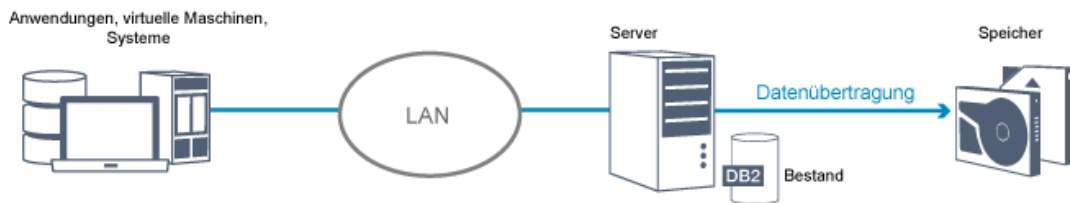
### Netzkonfigurationen für Speichereinheiten

IBM Spectrum Protect stellt Methoden zur Konfiguration von Clients und Servern in einem lokalen Netz (LAN = Local Area Network), in einem Speicherbereichsnetz (SAN = Storage Area Network), für die LAN-unabhängige Datenversetzung und als Network-attached Storage (NAS) bereit.

**Datensicherungsoperationen über ein LAN**

Abbildung 1 zeigt den Datenpfad für IBM Spectrum Protect-Sicherungsoperationen über ein LAN.

Abbildung 1. IBM Spectrum Protect-Sicherungsoperationen über ein LAN

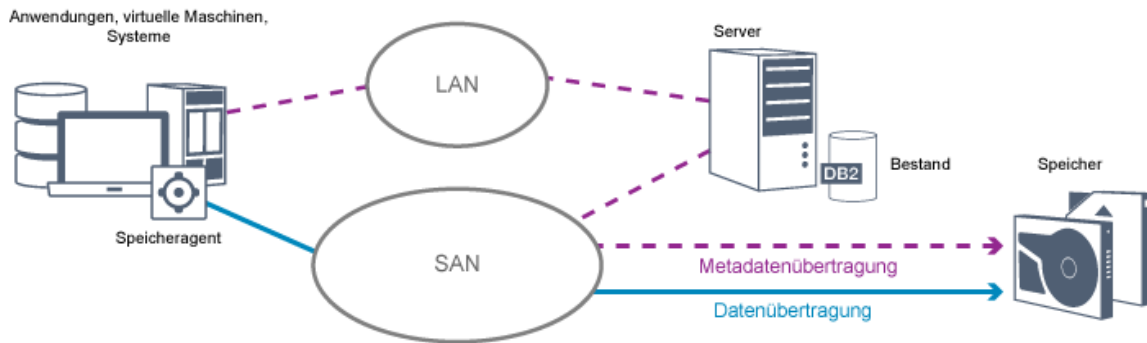


In einer LAN-Konfiguration sind einem einzelnen IBM Spectrum Protect-Server ein oder mehrere Bandarchive zugeordnet. Bei diesem Typ von Konfiguration müssen Clientdaten, E-Mails, Terminalverbindung, Anwendungsprogramm und Einheitensteuerinformationen alle von demselben Netz gehandhabt werden. Einheitensteuerinformationen und Clientsicherungs- und -zurückschreibungsdaten fließen über das LAN.

**Datensicherungsoperationen über ein SAN**

Abbildung 2 zeigt den Datenpfad für IBM Spectrum Protect-Sicherungsoperationen über ein SAN.

Abbildung 2. IBM Spectrum Protect-Sicherungsoperationen über ein SAN



Ein Speicherbereichsnetz (SAN) ist ein dediziertes Speichernetz, das die Systemleistung verbessern kann. In einem SAN können Sie Speicher konsolidieren und die bei lokalen Netzen (LANs) und Weitverkehrsnetzen (WANs) bestehenden Einschränkungen in Bezug auf Entfernung, Skalierbarkeit und Bandbreite verringern. Die Verwendung von IBM Spectrum Protect in einem SAN ermöglicht Ihnen die Nutzung der Vorteile der folgenden Funktionen:

- Gemeinsame Nutzung von Speichereinheiten durch mehrere IBM Spectrum Protect-Server. Dies schließt keine Einheiten ein, die den Einheitentyp GENERICTAPE verwenden.
- Versetzen von Daten von einem Clientsystem direkt in Speichereinheiten ohne Verwendung des LAN. Die LAN-unabhängige Datenversetzung erfordert die Installation eines Speicheragenten auf dem Clientsystem. Der Speicheragent ist zusammen mit dem Produkt IBM Spectrum Protect for SAN verfügbar.

Über den Speicheragenten kann der Client Daten direkt in einem Bandarchiv oder einem gemeinsam genutzten Dateisystem, wie beispielsweise GPFS, sichern und aus ihm zurückzuschreiben. Der IBM Spectrum Protect-Server verwaltet die Serverdatenbank und das Wiederherstellungsprotokoll und fungiert als Speicherarchivmanager, um Einheitenoperationen zu steuern. Der Speicheragent auf dem Client handhabt die Datenübertragung zu der Einheit auf dem SAN. Diese Implementierung gibt Bandbreite im LAN frei, die andernfalls für das Versetzen von Clientdaten verwendet würde.

- Gemeinsame Nutzung von Bandlaufwerken und Speicherarchiven, die vom IBM Spectrum Protect-Server unterstützt werden.
- Konsolidierung mehrerer Clients unter einem einzelnen Clientknotenname in einem GPFS-Cluster (GPFS = General Parallel File System).

#### Network-attached Storage (NAS)

Bei NAS-Dateiservern handelt es sich um Server mit dediziertem Speicher, deren Betriebssysteme für Dateiservicefunktionen optimiert sind. NAS-Dateiserver interagieren in der Regel mit IBM Spectrum Protect über standardisierte Netzprotokolle, wie beispielsweise Network Data Management Protocol (NDMP), oder als primärer Speicher für Speicherpools mit wahlfreiem oder sequenziellem Zugriff. IBM Spectrum Protect stellt die folgenden Basistypen von Konfigurationen bereit, die NDMP zum Sichern und Verwalten von NAS-Dateiservern verwenden:

- IBM Spectrum Protect sichert einen NAS-Dateiserver auf einer Speicherarchiveinheit, die direkt an den NAS-Dateiserver angeschlossen ist. Der NAS-Dateiserver, der remote an den IBM Spectrum Protect-Server angeschlossen sein kann, überträgt Sicherungsdaten direkt an ein Laufwerk in einem Bandarchiv, das über SCSI angeschlossen ist. Daten werden in NDMP-formatierten Speicherpools gespeichert; diese können auf Speichermedien gesichert werden, die zum Schutz vor einem Katastrophenfall vor Ort ausgelagert werden können.
- IBM Spectrum Protect sichert einen NAS-Dateiserver über das LAN in einer Speicherpoolhierarchie. Bei diesem Typ von Konfiguration können Sie NAS-Daten direkt auf Platte mit wahlfreiem Zugriff oder sequenziellem Zugriff speichern und die Daten dann auf Band umlagern. Sie können diesen Typ von Konfiguration auch für die Systemreplikation verwenden. Daten können auch auf Speichermedien gesichert werden, die ausgelagert werden können. Der Vorteil dieses Konfigurationstyps besteht darin, dass Ihnen alle Datenverwaltungsfunktionen, die für eine Speicherpoolhierarchie gelten, zur Verfügung stehen.
- Der IBM Spectrum Protect-Client liest die Daten mithilfe des NFS- oder CIFS-Protokolls aus dem NAS-System und sendet die Daten zum Speichern an den Server.

## Speicherverwaltung

Die Verwaltung der Einheiten und Datenträger, die zum Speichern von Clientdaten verwendet werden, erfolgt über den IBM Spectrum Protect-Server. Der Server integriert die Speicherverwaltung in die Maßnahmen, die Sie für die Verwaltung von Clientdaten in den folgenden Bereichen definieren:

#### Typen von Einheiten für Serverspeicher

IBM Spectrum Protect ermöglicht Ihnen die Verwendung von direkt angeschlossenen Einheiten und NAS-Einheiten für Serverspeicher. IBM Spectrum Protect stellt physische Speichereinheiten und Datenträger durch vom Administrator definierte Speicherobjekte dar.

#### Datenumlagerung über die Speicherhierarchie

Bei primären Speicherpools, die keine Verzeichniscontainerspeicherpools sind, können Sie die Speicherpools in einer oder mehreren hierarchischen Strukturen zusammenfassen. Diese Speicherhierarchie bietet Flexibilität in vielerlei Hinsicht. Sie können beispielsweise eine Maßnahme definieren, um Daten für schnellere Sicherungsoperationen auf Platten zu sichern. Der IBM Spectrum Protect-Server kann dann automatisch Daten von Platte auf Band umlagern.

#### Entfernen verfallener Daten

Die von Ihnen definierte Maßnahme steuert, wann Clientdaten auf dem IBM Spectrum Protect-Server automatisch verfallen. Zum Entfernen von Daten, die für den Verfall auswählbar sind, markiert ein Serververfallsprozess die Daten als verfallen und löscht die Metadaten für die verfallenen Daten aus der Datenbank. Der von den verfallenen Daten belegte Speicherbereich ist dann wieder für neue Daten verfügbar. Sie können die Häufigkeit des Verfallsprozesses über eine Serveroption steuern.

#### Datenträgerwiederverwendung durch Konsolidierung

Da Daten aufgrund von Servermaßnahmen automatisch verfallen, nimmt der freie Speicherbereich auf den Datenträgern, auf denen die Daten gespeichert sind, ständig zu. Bei allen Speichermedien mit Ausnahme von Verzeichniscontainerspeicherpools und Plattenspeicherpools mit wahlfreiem Zugriff implementiert der IBM Spectrum Protect-Server die *Konsolidierung*, ein Prozess, bei dem Datenträger für die Wiederverwendung freigegeben werden, ohne dass die traditionelle Bandrotation angewendet wird. Bei der Konsolidierung wird ein Datenträger automatisch defragmentiert, indem nicht verfallene Daten auf anderen Datenträgern konsolidiert werden, wenn der freie Speicherbereich auf einem Datenträger einen definierten Stand erreicht. Der konsolidierte Datenträger kann dann vom Server erneut verwendet werden. Die Konsolidierung ermöglicht den automatischen Umlauf von Datenträgern im Speicherwaltungsprozess und die Minimierung der Anzahl erforderlicher Datenträger.

## Gesicherte Clientdaten konsolidieren

---

Durch das Gruppieren der Clientdaten, die gesichert werden, kann die Anzahl Datenträgermounts für eine Clientwiederherstellung auf ein Minimum reduziert werden. Der IBM Spectrum Protect-Server stellt die folgenden Methoden zum Gruppieren von Clientdateien in anderen Speichermedien als Verzeichniscontainerspeicherpools zur Verfügung:

#### Clientdaten kollokieren

Der IBM Spectrum Protect-Server kann Clientdaten *kollokieren*, das heißt, er kann Clientdaten auf einigen wenigen Datenträgern speichern, anstatt sie über viele Datenträger zu verteilen. Bei der Kollokation nach Client wird die Anzahl Datenträger, die zum Sichern und Zurückschreiben von Clientdaten erforderlich ist, auf ein Minimum reduziert. Bei der Datenkollokation kann sich die Anzahl Datenträgermounts erhöhen, da die Speicherung von Daten mehrerer Clients nicht auf demselben Datenträger erfolgt, sondern jeder Client möglicherweise über einen dedizierten Datenträger verfügt.

Sie können festlegen, dass der Server Clientdaten kollokiert, wenn die Daten anfänglich in Serverspeicher gestellt werden. In einer Speicherhierarchie können Sie die Daten kollokieren, wenn der Server die Daten aus dem ursprünglichen Speicherpool in den nächsten Speicherpool in der Speicherhierarchie umlagert. Sie können Daten nach Client, nach Dateibereich pro Client oder nach Clientgruppe kollokieren. Ihre Auswahl ist von der Größe der Dateibereiche, die gespeichert werden, und von Zurückschreibungsanforderungen abhängig.

#### Pools für aktive Daten verschiedenen Einheiten zuordnen

Pools für aktive Daten sind für die Schnellwiederherstellung von Clientdaten geeignet. Vorteile umfassen eine Reduzierung der Anzahl Speicherdatenträger vor Ort oder an einem anderen Standort oder eine Verringerung der Bandbreite, wenn Sie Dateien kopieren oder zurückschreiben, die durch elektronisches Vaulting an einem fernen Standort geschützt werden. Pools für aktive Daten, die austauschbare Datenträger verwenden, wie beispielsweise Bänder, bieten ähnliche Vorteile. Obwohl Bandeinheiten bereitgestellt werden müssen, muss der Server keine Positionierung hinter inaktive Dateien ausführen. Der Hauptvorteil bei der Verwendung austauschbarer Datenträger in Pools für aktive Daten liegt jedoch in der Reduzierung der Anzahl Datenträger, die für die Aufbewahrung vor Ort und an einem anderen Standort verwendet werden. Wenn Daten an einem fernen Standort gespeichert werden, können Sie das Datenvolumen, das übertragen werden muss, auf ein Minimum reduzieren, indem nur aktive Daten kopiert und zurückgeschrieben werden.

#### Sicherungsgruppe erstellen

Eine Sicherungsgruppe enthält alle aktiven gesicherten Dateien, die für den betreffenden Client im Serverspeicher vorhanden sind. Die Sicherungsgruppe ist portierbar und wird für den von Ihnen angegebenen Zeitraum aufbewahrt. Eine Sicherungsgruppe ist zusätzlich zu den Sicherungen vorhanden, die bereits gespeichert sind, und erfordert weitere Datenträger.

#### Daten für einen Clientknoten versetzen

Sie können Daten für einen Clientknoten konsolidieren, indem Sie die Daten innerhalb des Serverspeichers versetzen. Sie können eine Sicherungsgruppe auf verschiedene Datenträger versetzen, auf denen die Sicherungsgruppe für den von Ihnen angegebenen Zeitraum aufbewahrt wird. Durch die Konsolidierung von Daten kann die Effizienz während Clientzurückschreibungs- oder -abrufoperationen verbessert werden.

## Datenschutzstrategien bei IBM Spectrum Protect

---

IBM Spectrum Protect stellt Möglichkeiten zur Implementierung verschiedener Datenschutzstrategien bereit.

In der Konfiguration von IBM Spectrum Protect können Sie angeben, ob Daten an Speichereinheiten am lokalen Standort oder an einem fernen Standort gesendet werden sollen. Um den Datenschutz zu maximieren, können Sie die Replikation auf einen fernen Server konfigurieren.

- Strategien zum Minimieren der Verwendung von Speicherbereich für Sicherungen  
Um die Größe des erforderlichen Speicherbereichs zu minimieren, sichert IBM Spectrum Protect Daten unter Verwendung der Datendeduplizierung und der progressiven Teilsicherung.
- Strategien zum Schutz vor Katastrophen  
IBM Spectrum Protect stellt Strategien bereit, um Daten in einem Katastrophenfall zu schützen. Diese Strategien umfassen Knotenreplikation an einen fernen Standort, Speicherpoolschutz, Datenbanksicherungen, Auslagerung von Sicherungsbändern und Einheitenreplikation auf einen Standby-Server.
- Strategien für die Wiederherstellung nach einem Katastrophenfall mithilfe von IBM Spectrum Protect  
IBM Spectrum Protect stellt verschiedene Möglichkeiten zur Wiederherstellung des Servers für den Fall bereit, dass die Datenbank oder Speicherpools fehlschlagen.

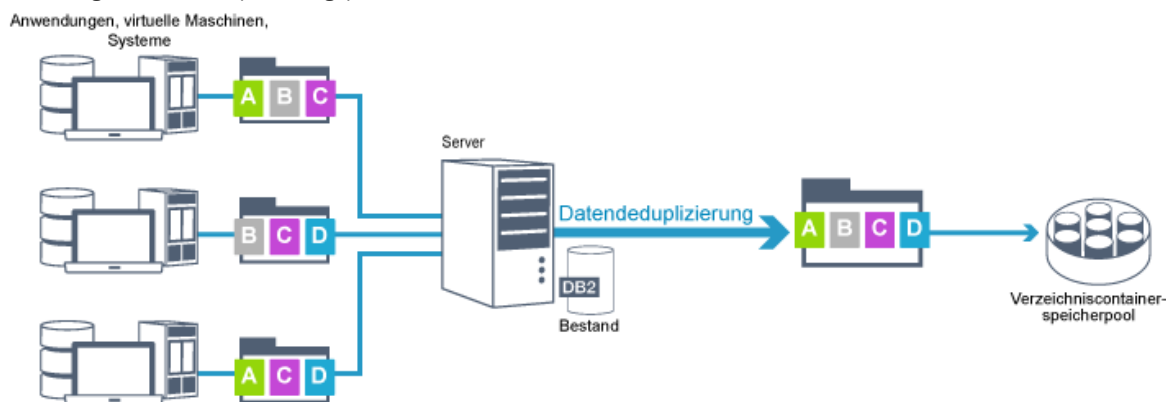
## Strategien zum Minimieren der Verwendung von Speicherbereich für Sicherungen

Um die Größe des erforderlichen Speicherbereichs zu minimieren, sichert IBM Spectrum Protect Daten unter Verwendung der Datendeduplizierung und der progressiven Teilsicherung.

### Datendeduplizierung

Wenn der IBM Spectrum Protect-Server Daten von einem Client empfängt, identifiziert der Server doppelte Datenbereiche und speichert eindeutige Instanzen der Datenbereiche in einem Verzeichniscontainerspeicherpool. Durch das Datendeduplizierungsverfahren wird die Speichernutzung verbessert und es ist keine dedizierte Datendeduplizierungsappliance erforderlich.

Abbildung 1. Datendeduplizierungsprozess



Wenn dasselbe Bytemuster mehrmals vorkommt, wird das Datenvolumen, das gespeichert oder übertragen werden muss, durch die Datendeduplizierung erheblich reduziert. Zusätzlich zu vollständigen Dateien kann IBM Spectrum Protect auch Teile von Dateien deduplizieren, die mit Teilen anderer Dateien identisch sind.

IBM Spectrum Protect stellt die folgenden Datendeduplizierungstypen bereit:

#### Serverseitige Datendeduplizierung

Der Server identifiziert doppelte Datenbereiche und versetzt die Daten in einen Verzeichniscontainerspeicherpool. Der serverseitige Prozess verwendet die *Inline-Datendeduplizierung*, bei der Daten zu demselben Zeitpunkt dedupliziert werden, zu dem sie in einen Verzeichniscontainerspeicherpool geschrieben werden. Deduplizierte Daten können auch in anderen Typen von Speicherpools gespeichert werden. Die Inline-Datendeduplizierung auf dem Server bietet die folgenden Vorteile:

- Die Notwendigkeit einer Konsolidierung entfällt.
- Der Speicherbereich, der von den gespeicherten Daten belegt wird, wird reduziert.

#### Clientseitige Datendeduplizierung

Mit dieser Methode wird die Verarbeitung während eines Sicherungsprozesses auf den Server und den Client verteilt. Der Client und der Server identifizieren und entfernen doppelte Daten, um Speicherbereich auf dem Server einzusparen. Bei der clientseitigen Datendeduplizierung werden nur komprimierte, deduplizierte Daten an den Server gesendet. Der Server speichert



die Daten in dem vom Client zur Verfügung gestellten komprimierten Format. Die clientseitige Dateneduplizierung bietet die folgenden Vorteile:

- Das Datenvolumen, das über das lokale Netz (LAN) gesendet wird, wird reduziert.
- Die zusätzliche Verarbeitungsleistung und -zeit, die zum Entfernen doppelter Daten auf dem Server erforderlich sind, entfallen.
- Die Datenbankleistung wird verbessert, da die clientseitige Dateneduplizierung ebenfalls inline erfolgt.

Sie können die clientseitige und serverseitige Dateneduplizierung in derselben Produktionsumgebung kombinieren. Die Möglichkeit, Daten entweder auf dem Client oder auf dem Server zu deduplizieren, bietet Flexibilität in Bezug auf Ressourcennutzung, Maßnahmenverwaltung und Datenschutz.

#### Komprimierung

Verwenden Sie die Inline-Komprimierung, um die Größe des Speicherbereichs in Containerspeicherpools zu reduzieren. Daten werden beim Schreiben in den Containerspeicherpool komprimiert.

Einschränkung: Verschlüsselte Daten können vom IBM Spectrum Protect-Server nicht komprimiert werden.

## Progressive Teilsicherung

---

Bei einer progressiven Teilsicherung überwacht der Server die Clientaktivität und sichert alle Dateien, die sich seit der ersten Gesamtsicherung geändert haben. Es werden vollständige Dateien gesichert, sodass der Server keine Basisversionen der Dateien referenzieren muss. Bei dieser Sicherungsmethode entfällt die Notwendigkeit, mehrere Gesamtsicherungen von Clientdaten erstellen zu müssen, wodurch Netzressourcen und Speicherbereich eingespart werden.

## Strategien zum Schutz vor Katastrophen

---

IBM Spectrum Protect stellt Strategien bereit, um Daten in einem Katastrophenfall zu schützen. Diese Strategien umfassen Knotenreplikation an einen fernen Standort, Speicherpoolschutz, Datenbanksicherungen, Auslagerung von Sicherungsbändern und Einheitenreplikation auf einen Standby-Server.

### Replikation an einen fernen Standort

---

*Knotenreplikation* ist der Prozess, bei dem Daten inkrementell von einem Server auf einen anderen Server kopiert werden. Der Server, von dem Clientdaten repliziert werden, wird als *Quellenreplikationsserver* bezeichnet. Der Server, auf den Clientdaten repliziert werden, wird als *Zielreplikationsserver* bezeichnet. Zum Schutz vor Katastrophen befindet sich der Zielreplikationsserver an einem fernen Standort. Ein Replikationsserver kann als Quellenserver und/oder Zielservers fungieren. Die Replikationsverarbeitung wird verwendet, um denselben Stand von Dateien auf dem Quellen- und dem Zielservers beizubehalten.

Die Knotenreplikation ermöglicht die sofortige Verfügbarkeit von Daten durch Übernahme. Auch wenn mithilfe der Knotenreplikation der größte Teil der Metadaten geschützt wird, bietet diese Methode keinen adäquaten Schutz vor einer Beschädigung der Datenbank. Sie können umfassenderen Schutz bereitstellen, indem Sie Speicherpools zum Speichern von Datensicherungen verwenden.

#### Vorteile

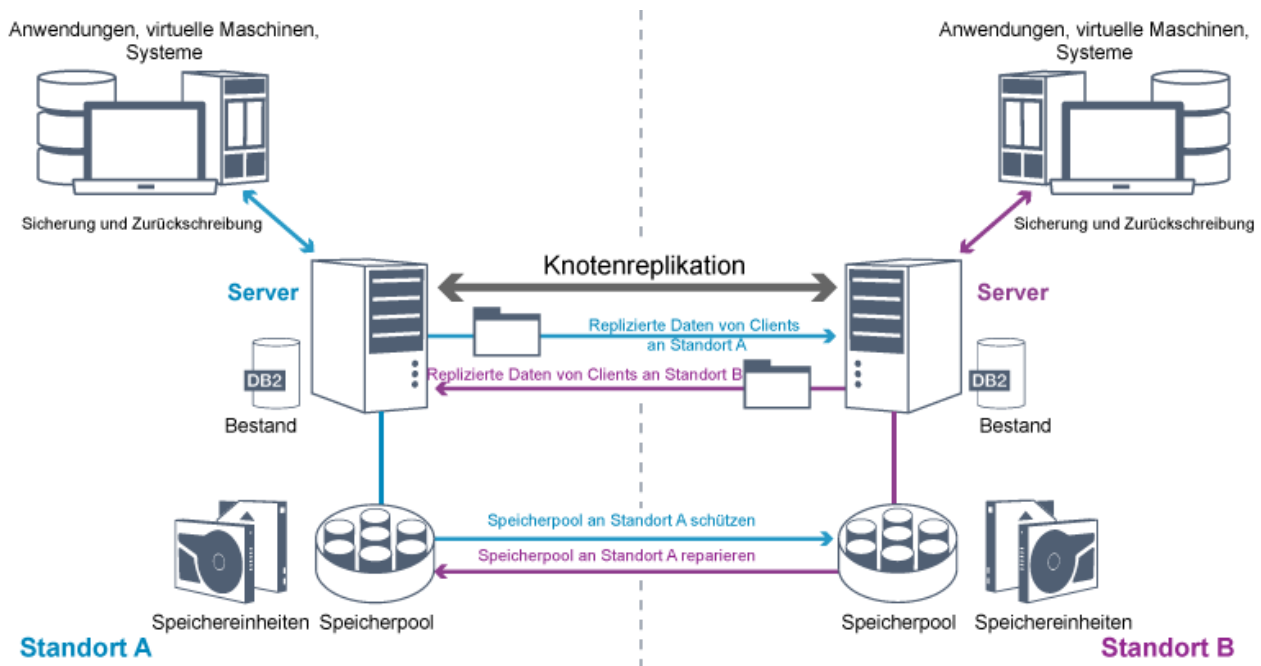
- Übernahme, sodass Daten sofort verfügbar sind, wenn ein Katastrophenfall eintritt
- Inkrementelle Replikation, die eine schnelle Datenübertragung zur Folge hat
- Elektronische Übertragung
- Schutz sowohl von Daten als auch von Metadaten

#### Nachteile

- Sowohl Daten als auch Metadaten müssen wiederhergestellt werden.
- Daten auf dem Quellenserver müssen erneut vom fernen Standort repliziert werden.

Abbildung 1 zeigt den Replikationsprozess an einen fernen Standort.

Abbildung 1. Knotenreplikationsprozess



Wenn Clientdaten repliziert werden, werden Daten, die nicht auf dem Zielsystem vorhanden sind, auf den Zielsystem kopiert. Wenn replizierte Daten den Aufbewahrungszeitraum überschreiten, entfernt der Zielsystem die Daten automatisch vom Quellsystem. Um den Datenschutz zu maximieren, synchronisieren Sie den lokalen Server und den fernen Server; beispielsweise repliziert Standort B Daten von Standort A und Standort A repliziert Daten von Standort B. Im Rahmen der Replikationsverarbeitung werden Clientdaten, die vom Quellsystem gelöscht wurden, auch vom Zielsystem gelöscht.

IBM Spectrum Protect stellt die folgenden Replikationsfunktionen bereit:

- Sie können Maßnahmen für den Zielsystem auf folgende Art und Weise definieren:
  - Identische Maßnahmen auf dem Quellsystem und dem Zielsystem
  - Unterschiedliche Maßnahmen auf dem Quellsystem und dem Zielsystem, um unterschiedliche Geschäftsanforderungen zu erfüllen

Wenn ein Katastrophenfall eintritt und der Quellsystem nicht verfügbar ist, können Clients Daten vom Zielsystem wiederherstellen. Wenn eine Wiederherstellung des Quellsystems nicht möglich ist, können Sie Clients anweisen, Daten auf dem Zielsystem zu speichern. Bei einem Ausfall kann für die Clients, die auf dem Quellsystem gesichert werden, automatisch eine Übernahme erfolgen, damit ihre Daten vom Zielsystem zurückgeschrieben werden können.

- Mithilfe der Replikationsverarbeitung können Sie beschädigte Dateien aus Speicherpools wiederherstellen. Sie müssen die Clientdaten auf den Zielsystem replizieren, bevor die Datei beschädigt wird. Nachfolgende Replikationsprozesse erkennen beschädigte Dateien auf dem Quellsystem und ersetzen sie durch unbeschädigte Dateien vom Zielsystem.

## Rolle der Replikation beim Schutz vor Katastrophen

Wenn ein Katastrophenfall eintritt, können Sie replizierte Daten vom fernen Standort wiederherstellen und denselben Stand von Dateien auf dem Quellsystem und dem Zielsystem beibehalten. Die Replikation wird zum Erreichen der folgenden Ziele verwendet:

- Steuern des Netzdurchsatzes durch die Planung der Knotenreplikation für bestimmte Zeiten
- Wiederherstellen von Daten nach einem Verlust aller Daten am Standort
- Wiederherstellen beschädigter Dateien auf dem Quellsystem

## Speicherpoolschutz

Stellen Sie im Rahmen einer Strategie zur Wiederherstellung nach einem Katastrophenfall sicher, dass eine Sicherungskopie der Daten in Speicherpools an einem fernen Standort verfügbar ist.

Vorteile

- Schnelle Wiederherstellung und Neuerstellung des Quellsystems

Nachteile

- Es werden nur Daten geschützt; Metadaten werden nicht geschützt.
- Für jeden Speicherpool müssen Sie das Speichermedium definieren.

Verschiedene Methoden können zum Schutz vor dem permanenten Verlust von Daten verwendet werden, die in Containerspeicherpools und in FILE- und DISK-Speicherpools gespeichert sind.

#### Verzeichniscontainerspeicherpools

Wenn nicht alle Daten in einem Clientknoten repliziert werden müssen, verwenden Sie Containerkopierspeicherpools, um einige Verzeichniscontainerspeicherpools zu schützen. Indem ein Verzeichniscontainerspeicherpool geschützt wird, werden keine Ressourcen verwendet, die vorhandene Daten und Metadaten replizieren, wodurch die Serverleistung verbessert wird.

Die bevorzugte Methode ist, den Verzeichniscontainerspeicherpool vor dem Replizieren des Clientknotens zu schützen. Wenn die Knotenreplikation gestartet wird, werden die Datenbereiche, die bereits durch Speicherpoolschutz repliziert werden, übersprungen und die Replikationsverarbeitungszeit wird somit reduziert. Wenn die Daten in einem Verzeichniscontainerspeicherpool beschädigt werden, können Sie die Daten mithilfe einer Kopie in einem Containerkopierspeicherpool reparieren.

#### Containerkopierspeicherpools

Sie schützen Verzeichniscontainerspeicherpools, indem Sie die Daten im Verzeichniscontainerspeicherpool in Containerkopierspeicherpools kopieren. Verwenden Sie Containerkopierspeicherpools, um bis zu zwei Bandkopien eines Verzeichniscontainerspeicherpools zu erstellen. Die Bandkopien können vor Ort oder an einem anderen Standort aufbewahrt werden. Beschädigte Daten in Verzeichniscontainerspeicherpools können mithilfe von Containerkopierspeicherpools repariert werden. Containerkopierspeicherpools stellen eine Alternative zur Verwendung eines Replikationsservers zum Schützen von Daten in einem Verzeichniscontainerspeicherpool dar.

#### Speicherpools, die Einheitenklassen FILE und DISK zugeordnet sind

Für Speicherpools, die Einheitenklassen FILE und DISK zugeordnet sind, verwenden Sie die Knotenreplikation, um eine knotenkonsistente Kopie der Daten auf dem Zielsystem beizubehalten. Die Datenkopie kann direkt vom Zielsystem in die Speicherpools zurückgeschrieben werden.

## Datenbanksicherungen

---

Sie verwenden Datenbanksicherungen, um Ihr System nach einer Beschädigung der Datenbank wiederherzustellen. Datenbanksicherungen müssen außerdem verwendet werden, um zu verhindern, dass bei DB2 der Speicherbereich für das Archivprotokoll knapp wird. Datenbanksicherungsoperationen sind nicht Teil der Knotenreplikation. Bei einer Datenbanksicherung kann es sich um eine Gesamt-, Teil- oder Momentaufnahmesicherung handeln. Um eine schnelle Wiederherstellung nach einem Katastrophenfall zu ermöglichen, muss eine Kopie der Datenbanksicherungen an einen anderen Standort gespeichert werden. Um die Datenbank zurückschreiben zu können, müssen Sie über die Sicherungsdatenträger für die Datenbank verfügen. Sie können die Datenbank mithilfe einer Operation für die Zurückschreibung nach Zeitpunkt oder einer Operation für die Zurückschreibung mit dem neuesten Stand aus Sicherungsdatenträgern zurückschreiben.

#### Zurückschreibung nach Zeitpunkt

Verwenden Sie Operationen für die Zurückschreibung nach Zeitpunkt bei der Wiederherstellung nach einem Katastrophenfall oder zum Entfernen der Auswirkungen von Fehlern, die Inkonsistenzen in der Datenbank zur Folge haben können. Zurückschreibungsoperationen für die Datenbank, bei denen Momentaufnahmesicherungen verwendet werden, sind eine Form der Operation für die Zurückschreibung nach Zeitpunkt. Die Operation für die Zurückschreibung nach Zeitpunkt umfasst die folgenden Aktionen:

- Das Verzeichnis für aktive Protokolldateien und das Archivprotokollverzeichnis, die in der Datei dmserv.opt angegeben sind, werden entfernt und erneut erstellt.
- Das Datenbankimage wird von den Sicherungsdatenträgern in die Datenbankverzeichnisse, die in einer Datenbanksicherung aufgezeichnet wurden, oder in neue Verzeichnisse zurückgeschrieben.
- Archivprotokolle werden von den Sicherungsdatenträgern in das Überlaufverzeichnis zurückgeschrieben.
- Protokolldateien aus dem Überlaufverzeichnis werden bis zu einem angegebenen Zeitpunkt verwendet.

#### Zurückschreibung mit dem neuesten Stand

Wenn die Datenbank mit dem Stand wiederhergestellt werden soll, den sie zu dem Zeitpunkt hatte, zu dem sie verloren ging, stellen Sie die Datenbank mit dem neuesten Stand wieder her. Die Operation für die Zurückschreibung mit dem neuesten Stand umfasst die folgenden Aktionen:

- Ein Datenbankimage wird von den Sicherungsdatenträgern in die Datenbankverzeichnisse, die in einer Datenbanksicherung aufgezeichnet wurden, oder in neue Verzeichnisse zurückgeschrieben.
- Archivprotokolle werden von den Sicherungsdatenträgern in das Überlaufverzeichnis zurückgeschrieben.
- Protokolldateien aus dem Überlaufverzeichnis und Archivprotokolle aus dem Archivprotokollverzeichnis werden verwendet.

Im Rahmen der letzten Zurückschreibung werden das Verzeichnis für aktive Protokolldateien und das Archivprotokollverzeichnis nicht entfernt und erneut erstellt.

## Alternativmethoden zum Schutz vor Katastrophen

---

Zusätzlich zu Replikation, Speicherpoolschutz und Datenbanksicherungen können Sie auch die folgenden Methoden zum Schutz von Daten und zur Implementierung der Wiederherstellung nach einem Katastrophenfall mit IBM Spectrum Protect verwenden:

Transport von Sicherungsbändern an einen fernen Standort

Daten werden zu geplanten Zeiten vom Quellenserver auf Band gesichert. Die Bänder werden an einen fernen Standort transportiert. Wenn ein Katastrophenfall eintritt, werden die Bänder an den Standort des Quellenservers zurücktransportiert und die Daten werden auf die Quellclients zurückgeschrieben. Ausgelagerte Kopien der Daten auf Sicherungsband können Sie auch bei der Wiederherstellung nach Ransomware-Attacken unterstützen.

Replikation mit Appliances an mehreren Standorten auf einen Standby-Server

Bei der Konfiguration mit Appliances an mehreren Standorten wird die Quellen-Appliance auf einen fernen Server in einer SAN-Architektur repliziert. Wenn die Client-Hardware am ursprünglichen Standort beschädigt wird, kann bei dieser Konfiguration die Quelleneinheit vom Standby-Server am fernen Standort repliziert werden. Mit dieser Konfiguration werden plattenbasierte Sicherungs- und Zurückschreibungsoperationen bereitgestellt.

## Vergleich der Konfigurationsstrategien für den Schutz

---

Beachten Sie die folgenden potenziellen Datenverlustszenarios:

- Datenbankdaten werden beschädigt: Schützen Sie sich mithilfe der Datenbanksicherung vor Ort vor dem Verlust von Daten in der Datenbank.
- Speicherpooldaten werden beschädigt: Schützen Sie sich mithilfe von Kopierspeicherpools vor Ort oder mithilfe der Knotenreplikation vor dem Verlust von Daten in Speicherpools.
- Störungsszenario, bei dem sowohl die Datenbank vor Ort als auch die Speicherpools vor Ort verloren gehen: Schützen Sie sich vor einer großen Katastrophe, indem Sie die Knotenreplikation und sowohl die Datenbanksicherung an einem anderen Standort als auch Speicherpoolsicherungskopien an einem anderen Standort verwenden.

Die folgenden potenziellen Konfigurationen betreffen die gängigsten Datenschutzszenarios:

Konfigurationen ausschließlich für den Schutz vor einer Beschädigung

- Implementieren Sie Datenbanksicherungsoperationen vor Ort mit einem optionalen Containerkopierspeicherpool vor Ort, um Daten in Verzeichniscontainerspeicherpools zu schützen.
- Implementieren Sie Datenbanksicherungsoperationen vor Ort und die Knotenreplikation vor Ort.

Konfigurationen für die Wiederherstellung nach einem Katastrophenfall und den Schutz vor einer Beschädigung

- Implementieren Sie Datenbanksicherungsoperationen an einen anderen Standort mit Containerkopierspeicherpools an einen anderen Standort, um Daten in Verzeichniscontainerspeicherpools zu schützen.
- Implementieren Sie Datenbanksicherungsoperationen vor Ort und die Knotenreplikation an einem anderen Standort mit einem optionalen Containerkopierspeicherpool vor Ort für die schnellere Wiederherstellung beschädigter Daten.

## Strategien für die Wiederherstellung nach einem Katastrophenfall mithilfe von IBM Spectrum Protect

---

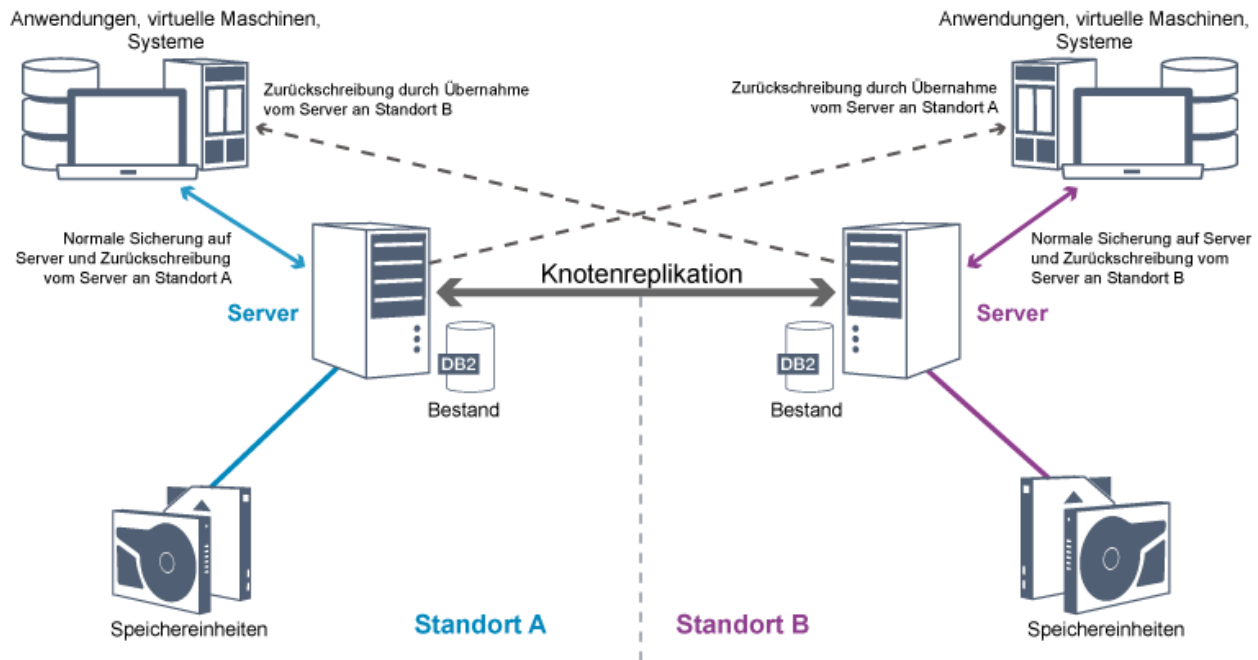
IBM Spectrum Protect stellt verschiedene Möglichkeiten zur Wiederherstellung des Servers für den Fall bereit, dass die Datenbank oder Speicherpools fehlschlagen.

### Automatische Übernahme für die Wiederherstellung nach einem Katastrophenfall

---

Die *automatische Übernahme* ist eine Operation, mit zu einem Standby-System gewechselt wird, wenn eine Software-, Hardware- oder Netzunterbrechung auftritt. Die automatische Übernahme wird zusammen mit der Knotenreplikation zur Wiederherstellung von Daten nach einem Systemfehler verwendet. Abbildung 1 zeigt den automatischen Übernahmeprozess in IBM Spectrum Protect.

Abbildung 1. Automatischer Übernahmeprozess



Die automatische Übernahme für die Datenwiederherstellung erfolgt, wenn der Quellenreplikationsserver aufgrund einer Katastrophe oder eines Systemausfalls nicht verfügbar ist. Wenn der Client während des normalen Betriebs auf einen Quellenreplikationsserver zugreift, empfängt der Client Verbindungsinformationen für den Zielreplikationsserver. Der Clientknoten speichert die Übernahmeverbindungsinformationen in der Clientoptionsdatei.

Während Clientzurückschreibungsoperationen wechseln Clients automatisch vom Quellenreplikationsserver zum Zielreplikationsserver und wieder zurück; dieser Wechsel wird durch den Server ausgeführt. Für den Schutz durch Übernahme kann jeweils nur ein einziger Server pro Knoten verwendet werden. Wenn eine neue Clientoperation gestartet wird, versucht der Client, die Verbindung zum Quellenreplikationsserver herzustellen. Der Client nimmt die Operationen auf dem Quellenserver wieder auf, wenn der Quellenreplikationsserver verfügbar ist.

Um die automatische Übernahme für replizierte Clientknoten verwenden zu können, müssen der Quellenreplikationsserver, der Zielreplikationsserver und der Client Version 7.1 oder höher haben. Wenn einer der Server eine frühere Version hat, wird die automatische Übernahme inaktiviert und Sie müssen den Übernahmeprozess manuell ausführen.

## Wiederherstellung von IBM Spectrum Protect-Komponenten

Die Serverdatenbank, das Wiederherstellungsprotokoll und die Speicherpools sind für den Betrieb von IBM Spectrum Protect kritisch und müssen geschützt werden. Wenn die Datenbank nicht verwendbar ist, ist der gesamte Server nicht verfügbar und die Wiederherstellung von Daten, die vom Server verwaltet werden, kann sich schwierig gestalten oder als unmöglich erweisen.

Sogar ohne die Datenbank könnten Datenfragmente oder vollständige Dateien von Speicherpooldatenträgern gelesen werden, die nicht verschlüsselt sind, und die Sicherheit kann beeinträchtigt werden. Aus diesem Grund müssen Sie die Datenbank immer sichern. Verschlüsseln Sie außerdem immer sensible Daten mithilfe des Clients oder der Speichereinheit, es sei denn, die Speichermedien sind physisch geschützt.

IBM Spectrum Protect stellt eine Reihe von Datenschutzmethoden bereit, die das Sichern von Speicherpools und der Datenbank umfassen. Sie können beispielsweise für die Ausführung der folgenden Operationen Zeitpläne definieren:

- Nach der ersten Gesamtsicherung Ihrer Speicherpools werden jede Nacht Speicherpoolteilsicherungen ausgeführt.
- Datenbankteilsicherungen werden jede Nacht ausgeführt.
- Datenbankgesamtsicherungen werden einmal pro Woche ausgeführt.

Bei bandbasierten Umgebungen können Sie Disaster Recovery Manager (DRM) zur Unterstützung bei der Ausführung vieler Tasks verwenden, die den Schutz und die Wiederherstellung von Daten betreffen. DRM ist in IBM Spectrum Protect Extended Edition verfügbar.

## Vorbeugende Maßnahmen für die Wiederherstellung

Die Wiederherstellung basiert auf folgenden vorbeugenden Maßnahmen:

- Spiegeln, wodurch der Server eine Kopie der aktiven Protokolldatei beibehält
- Sichern der Datenbank
- Sichern der Speicherpools

- Prüfen der Speicherpools auf beschädigte Dateien und Wiederherstellen der beschädigten Dateien, falls erforderlich
- Sichern der Einheitenkonfigurationsdateien und Protokolldateien für Datenträger
- Prüfen der Daten in Speicherpools mithilfe der zyklischen Blockprüfung
- Speichern der Datei cert.kdb an einer sicheren Position, um zu gewährleisten, dass Secure Sockets Layer (SSL) sicher ist

Wenn Sie Bänder zum Speichern verwenden, können Sie auch einen Plan zur Wiederherstellung nach einem Katastrophenfall (der auch als Wiederherstellungsplan bezeichnet wird) erstellen, der Sie durch den Wiederherstellungsprozess mit DRM führt. Sie können den Wiederherstellungsplan zu Prüfzwecken verwenden, um die Wiederherstellbarkeit des Servers zu bestätigen. Die Methoden von DRM zur Wiederherstellung nach einem Katastrophenfall basieren auf den folgenden Maßnahmen:

- Erstellen einer Wiederherstellungsplandatei für den Server
- Sichern von Serverdaten auf Band
- Senden der Serversicherungsdaten an einen fernen Standort oder einen anderen Server
- Speichern von Clientsysteminformationen
- Definieren und Verfolgen der Speichermedien, die zum Speichern und Wiederherstellen von Clientdaten verwendet werden

## IBM Spectrum Protect-Datenschutzlösungen

---

IBM Spectrum Protect-Server und -Clients stellen Datenschutzlösungen für die meisten allgemeinen Geschäfts- und Konformitätsanforderungen bereit.

- **Datenschutzlösung für Ihre Umgebung auswählen**  
Lesen Sie zur Unterstützung bei der Implementierung einer Datenschutzumgebung die Informationen zu Best-Practice-Konfigurationen von IBM Spectrum Protect und wählen Sie die beste Lösung für Ihre Geschäftsanforderungen aus.
- **Plattenspeicherlösung für einen einzelnen Standort**  
Diese Datenschutzlösung stellt kosteneffizienten Datenspeicher an einem einzelnen Standort mit minimaler Hardwarekonfiguration bereit.
- **Plattenspeicherlösung für mehrere Standorte**  
Diese Datenschutzlösung stellt Replikation an mehreren Standorten bereit, sodass jeder Server Daten für den jeweils anderen Standort schützt.
- **Bandspeicherlösung**  
Diese Datenschutzlösung stellt Speicher für Banddatenträger bereit, eine flexible und kosteneffiziente Option für die langfristige Aufbewahrung von Daten.
- **Serverlösungsdokumentation in PDF-Dateien**  
Vordefinierte PDF-Dateien für die IBM Spectrum Protect-Dokumentation sind zum Download verfügbar.

## Datenschutzlösung für Ihre Umgebung auswählen

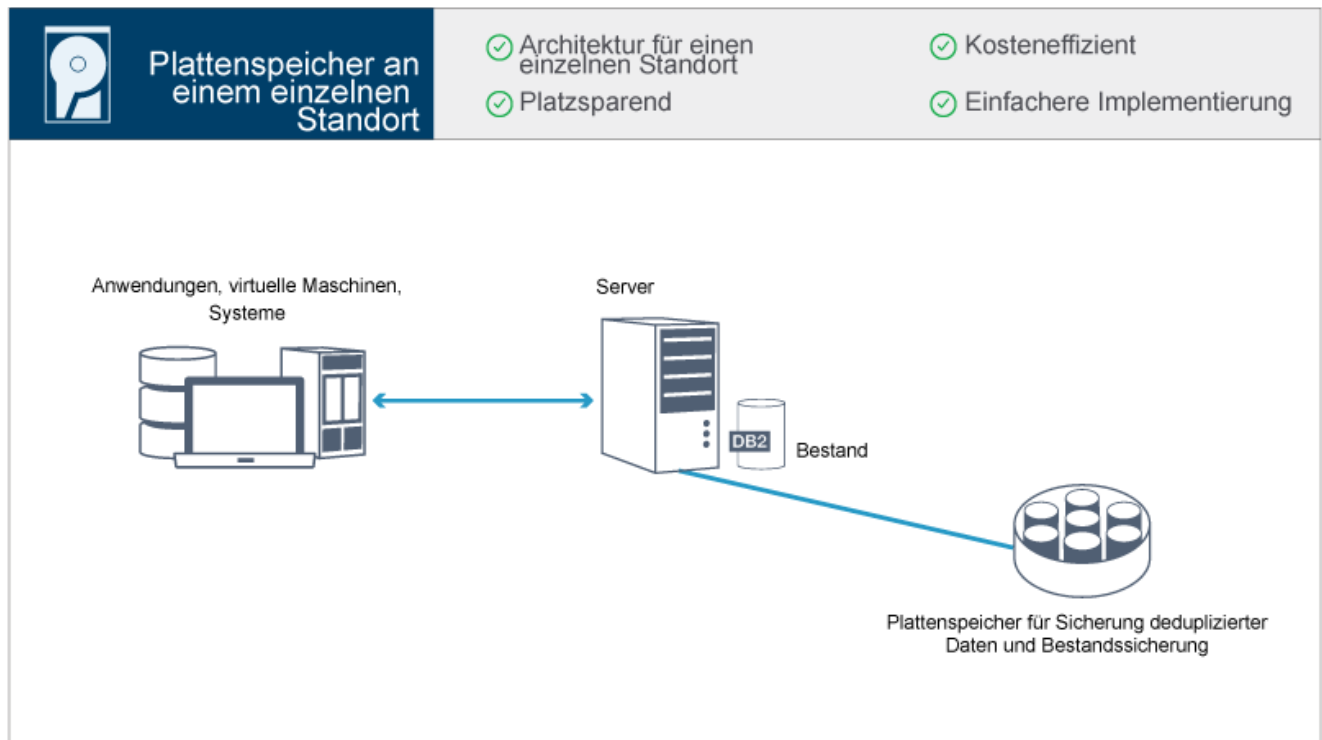
---

Lesen Sie zur Unterstützung bei der Implementierung einer Datenschutzumgebung die Informationen zu Best-Practice-Konfigurationen von IBM Spectrum Protect und wählen Sie die beste Lösung für Ihre Geschäftsanforderungen aus.

- **Plattenbasierte Implementierung einer Datenschutzlösung für einen einzelnen Standort**  
Diese plattenbasierte Implementierung einer Datenschutzlösung mit IBM Spectrum Protect verwendet Inline-Dateneduplizierung und stellt Schutz für Daten an einem einzelnen Standort bereit.
- **Plattenbasierte Implementierung einer Datenschutzlösung für mehrere Standorte**  
Diese plattenbasierte Implementierung einer Datenschutzlösung mit IBM Spectrum Protect verwendet Inline-Dateneduplizierung und Replikation an zwei Standorten.
- **Appliance-basierte Implementierung einer Datenschutzlösung für mehrere Standorte**  
Diese Implementierung einer IBM Spectrum Protect-Datenschutzlösung für mehrere Standorte verwendet appliance-basierte Dateneduplizierung und Replikation. Ein Standby-Server ist an einem zweiten Standort für die Wiederherstellung von Daten für den Fall konfiguriert, dass der primäre Server nicht verfügbar ist.
- **Bandbasierte Implementierung einer Datenschutzlösung**  
Diese Implementierung einer Datenschutzlösung mit IBM Spectrum Protect verwendet eine oder mehrere Bandspeichereinheiten zum Sichern von Daten. Die Bandsicherung stellt kostengünstige Skalierbarkeit bereit, die für die langfristige Aufbewahrung optimiert ist.
- **Vergleich der Datenschutzlösungen**  
Vergleichen Sie die Schlüsselfunktionen der einzelnen IBM Spectrum Protect-Lösungen, um die Konfiguration zu bestimmen, die Ihre Datenschutzerfordernungen am besten erfüllt. Lesen Sie dann die verfügbare Dokumentation, um die Lösung zu implementieren.
- **Roadmap für die Implementierung einer Datenschutzlösung**  
Planen und implementieren Sie die geeignetste Datenschutzlösung für Ihre Geschäftsumgebung mit IBM Spectrum Protect.

## Plattenbasierte Implementierung einer Datenschutzlösung für einen einzelnen Standort

Diese plattenbasierte Implementierung einer Datenschutzlösung mit IBM Spectrum Protect verwendet Inline-Dateneduplizierung und stellt Schutz für Daten an einem einzelnen Standort bereit.



Diese Datenschutzlösung bietet die folgenden Vorteile:

- Serversystem und Speicherhardware an einem einzigen Standort
- Kosteneffizient Nutzung des Speichers über die Dateneduplizierungsfunktion
- Platzsparende Lösung mit minimaler Hardwarekonfiguration
- Minimale Implementierung, die nur die Installation und Konfiguration für einen einzigen Server und unterstützende Speicherhardware erfordert

Bei dieser Lösung sendet der Client Daten an den IBM Spectrum Protect-Server, auf dem die Daten dedupliziert und in einem Verzeichniscontainerspeicherpool gespeichert werden, der in Plattenspeicher implementiert ist. Daten aus dem Bestand werden ebenfalls in Plattenspeicher gesichert. Diese Lösung ist für Einstiegsumgebungen geeignet, bei denen keine zweite Kopie der Daten erforderlich ist.

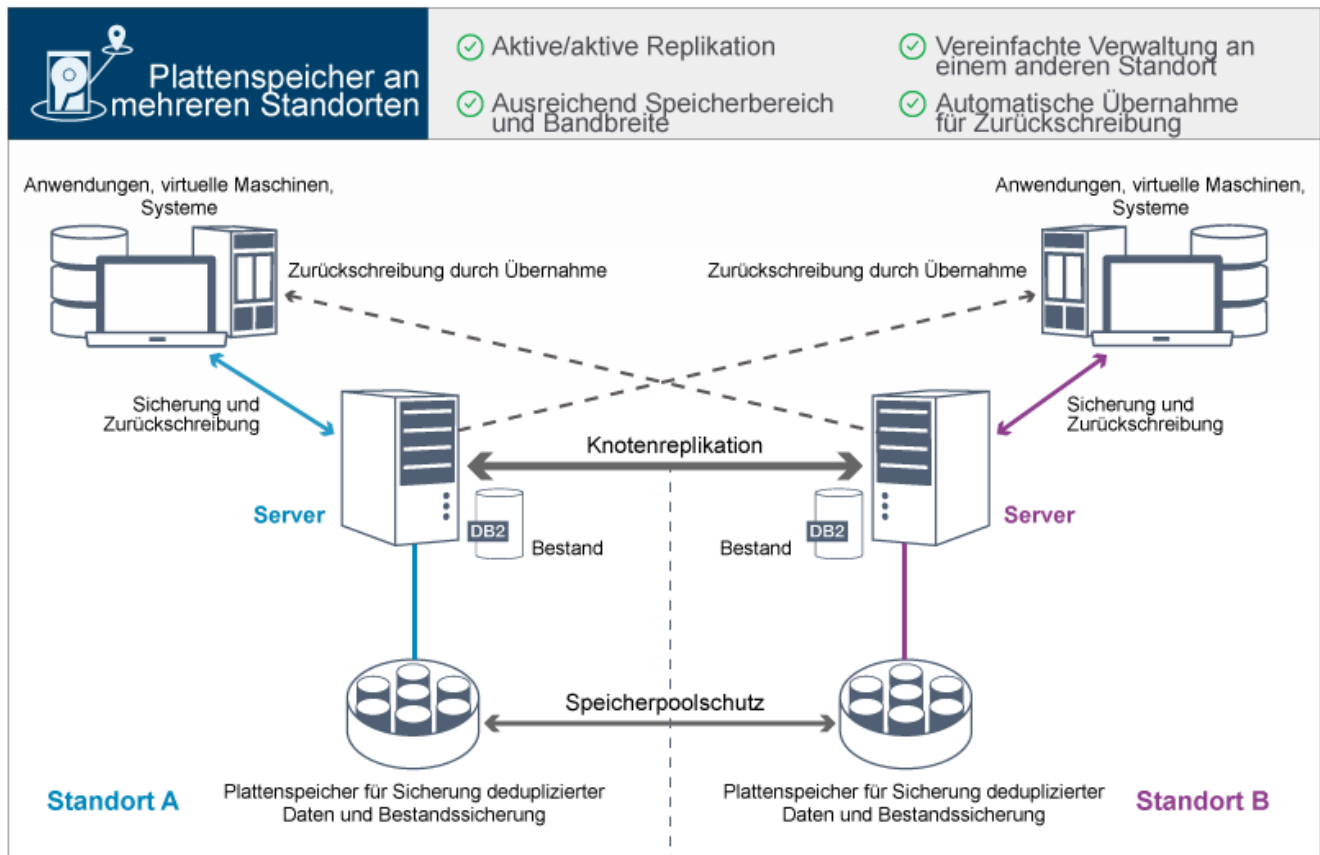
### Zugehörige Verweise:

Vergleich der Datenschutzlösungen

Roadmap für die Implementierung einer Datenschutzlösung

## Plattenbasierte Implementierung einer Datenschutzlösung für mehrere Standorte

Diese plattenbasierte Implementierung einer Datenschutzlösung mit IBM Spectrum Protect verwendet Inline-Dateneduplizierung und Replikation an zwei Standorten.



Diese Datenschutzlösung bietet die folgenden Vorteile:

- Replikation kann an beiden Standorten konfiguriert werden, sodass jeder Server Daten für den jeweils anderen Standort schützt.
- Die Auslagerung von Daten für jeden Standort wird vereinfacht.
- Bandbreite wird effizient genutzt, da nur deduplizierte Daten zwischen den Standorten repliziert werden.
- Für Clients kann eine automatische Übernahme durch einen Zielreplikationsserver erfolgen, wenn der Quellenreplikationsserver nicht verfügbar ist.

Bei dieser Lösung senden Clients Daten an den Quellenserver, auf dem die Daten dedupliziert und in einem Verzeichniscontainerspeicherpool gespeichert werden, der in Plattenspeicher implementiert ist. Die Daten werden für jeden Standort in den Speicherpool auf dem Zielsystem repliziert. Diese Lösung ist für Umgebungen geeignet, die Schutz vor Katastrophen erfordern. Wenn die gegenseitige Replikation konfiguriert ist, können Clients an beiden Standorten die Wiederherstellung durch Übernahme für unterbrechungsfreie Sicherungen und Datenwiederherstellung von dem am anderen Standort verfügbaren Server nutzen.

#### Zugehörige Verweise:

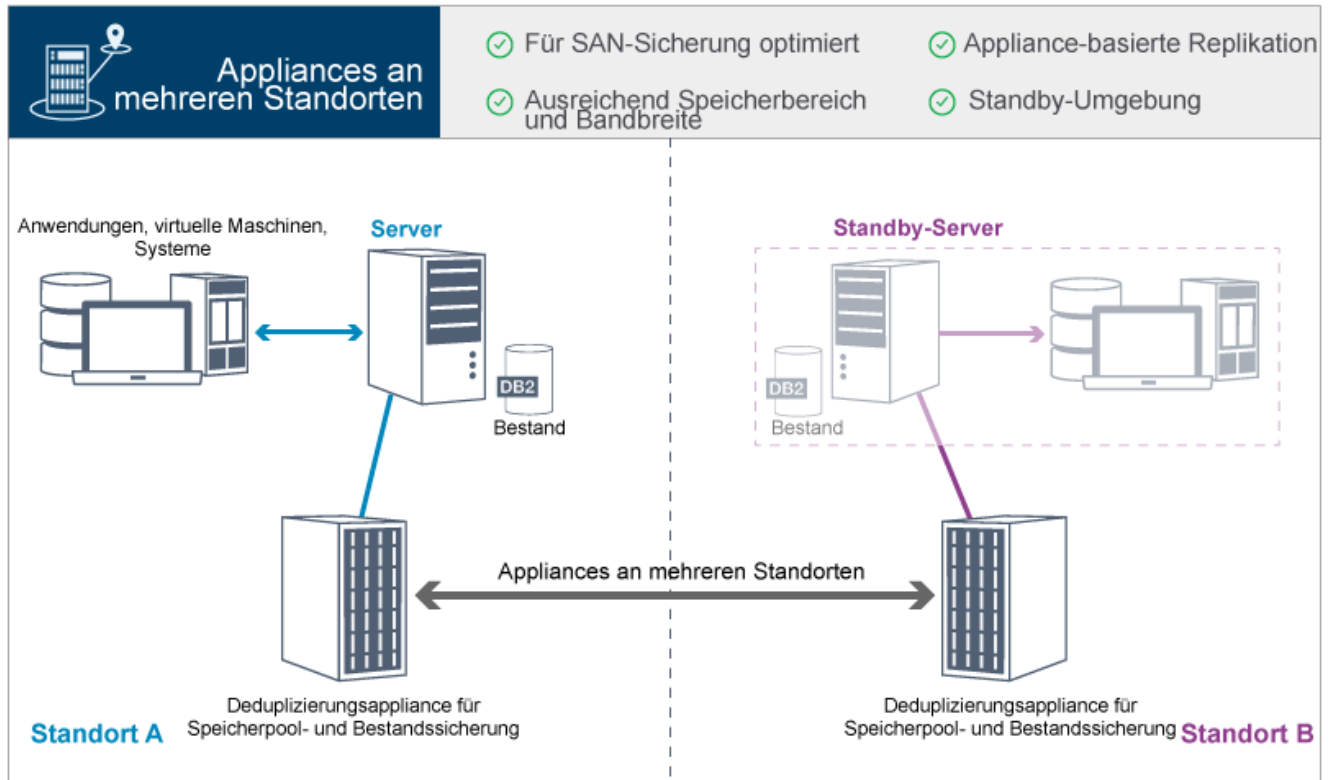
Vergleich der Datenschutzlösungen

Roadmap für die Implementierung einer Datenschutzlösung

## Appliance-basierte Implementierung einer Datenschutzlösung für mehrere Standorte

Diese Implementierung einer IBM Spectrum Protect-Datenschutzlösung für mehrere Standorte verwendet appliance-basierte Datendeduplizierung und Replikation. Ein Standby-Server ist an einem zweiten Standort für die Wiederherstellung von Daten für den Fall konfiguriert, dass der primäre Server nicht verfügbar ist.





Diese Datenschutzlösung bietet die folgenden Vorteile:

- Die Leistung ist für Sicherungen in Hochgeschwindigkeits-SANs und für die Verwendung mit IBM Spectrum Protect for SAN optimiert, wenn Clients Daten direkt auf virtuelle Bandeinheiten sichern, die an ein Speicherbereichsnetz (SAN) angeschlossen sind.
- Durch die schnelle, appliance-basierte Replikation wird der Server von der Notwendigkeit befreit, Replikationsmetadaten in der Serverdatenbank verfolgen zu müssen.
- Bandbreite und Speicherbereich werden effizient genutzt, da nur deduplizierte Daten zwischen den Standorten repliziert werden.
- Eine Standby-Umgebung ist für die Wiederherstellung nach einem Katastrophenfall verfügbar, erfordert aber nicht so viele Ressourcen, wie für einen vollständig aktiven Standort benötigt werden.

Bei dieser Datenschutzkonfiguration verwendet der Server Hardware-Appliances zum Deduplizieren und Replizieren von Daten. Die Appliance an Standort A dedupliziert Daten und repliziert die Daten anschließend zum Schutz vor Katastrophen auf die Appliance an Standort B. Bei einem Ausfall an Standort A können Sie den Standby-Server aktivieren, indem Sie die neueste Datenbanksicherung zurückschreiben und die replizierte Kopie der Daten aktivieren.

Weitere Informationen zum Konfigurieren virtueller Bandarchive finden Sie in [Virtuelle Bandarchive konfigurieren](#).

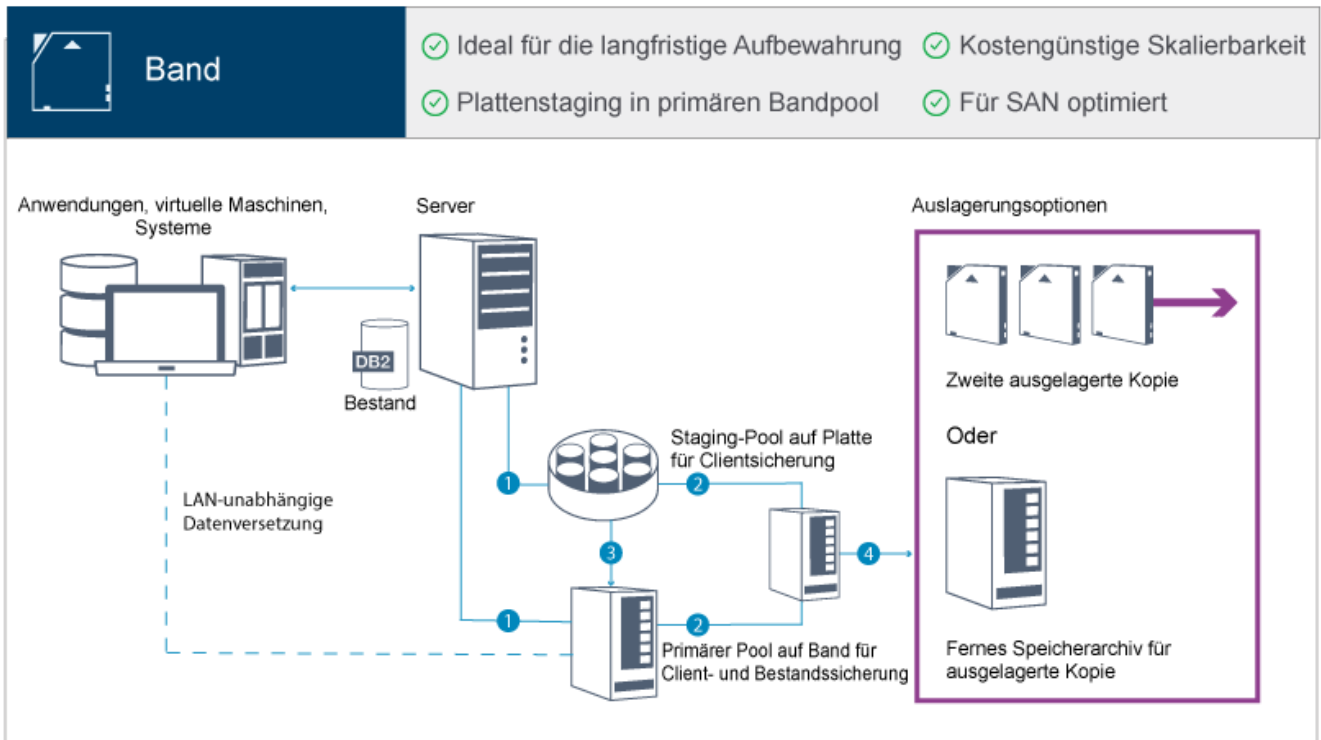
#### Zugehörige Verweise:

[Vergleich der Datenschutzlösungen](#)

[Roadmap für die Implementierung einer Datenschutzlösung](#)

## Bandbasierte Implementierung einer Datenschutzlösung

Diese Implementierung einer Datenschutzlösung mit IBM Spectrum Protect verwendet eine oder mehrere Bandspeichereinheiten zum Sichern von Daten. Die Bandsicherung stellt kostengünstige Skalierbarkeit bereit, die für die langfristige Aufbewahrung optimiert ist.



Diese Datenschutzlösung bietet die folgenden Vorteile:

- Die Leistung wird für Sicherungsoperationen in Hochgeschwindigkeits-SANs, die direkt auf Band erfolgen, für große Datentypen und für die langfristige Aufbewahrung von Daten optimiert.
- Die Datenverfügbarkeit wird optimiert, indem Kopien von Daten für die Wiederherstellung nach einem Katastrophenfall an anderen Standorten aufbewahrt werden. Wenn Sie die Funktion 'Disaster Recovery Management' (DRM) aktivieren und eine Katastrophe eintritt, unterstützt Sie DRM bei der Optimierung des Wiederherstellungsprozesses für Ihre Server.
- Die Datensicherheit wird optimiert, da Kopien von Daten an einem anderen Standort auf Bänderinheiten gespeichert werden die *nicht* mit dem Internet verbunden sind. Ransomware-Angriffe sind auf Internetverbindungen angewiesen; demzufolge kann die Speicherung an einem anderen Standort zum Schutz gegen derartige Angriffe beitragen.
- Kostengünstige Skalierbarkeit wird erzielt, indem die Notwendigkeit zusätzlicher Plattenhardware reduziert und Energiekosten gesenkt werden.

**Zugehörige Konzepte:**

Bandeinheitentreiber auswählen

**Zugehörige Tasks:**

Datensicherungsstrategien erstellen

Datenträgerbestand verwalten

**Zugehörige Verweise:**

Vergleich der Datenschutzlösungen





Bandeinheitentreiber installieren und konfigurieren

## Vergleich der Datenschutzlösungen

Vergleichen Sie die Schlüsselfunktionen der einzelnen IBM Spectrum Protect-Lösungen, um die Konfiguration zu bestimmen, die Ihre Datenanforderungen am besten erfüllt. Lesen Sie dann die verfügbare Dokumentation, um die Lösung zu implementieren.

|                     | Plattenspeicher an einem einzelnen Standort | Plattenspeicher an mehreren Standorten | Appliances an mehreren Standorten | Band |
|---------------------|---|--|-----------------------------------|------|
|                     |   |  |                                   |      |
| <b>Schwerpunkte</b> |   |  |                                   |      |
| Kosten              | \$  | \$\$\$                                 | \$\$\$\$                          | \$\$ |

|   | Plattenspeicher an einem einzelnen Standort                                       | Plattenspeicher an mehreren Standorten   | Appliances an mehreren Standorten   | Band  |
|---|---|--|---|---|
|   |  |  |  |  |
| Schutzstufe   | 1 Datenkopie  | 2 oder mehr Datenkopien  | 2 oder mehr Datenkopien   | 2 oder mehr Datenkopien   |
| Wiederherstellung nach einem Katastrophenfall   | Keine   | Aktiver Server   | Standby-Server  | Kopien an einem anderen Standort  |
| <b>Hauptvorteile</b>  |   |  |   |   |
| Erstklassige Datenreduktion   | ✓   | ✓  | ✓   | ✓   |
| Schnelle und effiziente plattenbasierte Sicherungs- und Zurückschreibungsoperationen  | ✓   |  | ✓   |   |
| Vereinfachte Verwaltung an einem anderen Standort   |   | ✓  |   |   |
| Datendeduplizierungsfunktion ohne Zusatzkosten  | ✓   | ✓  |   |   |
| Inklusive Replikationsverarbeitung ohne Zusatzkosten  |   | ✓  |   |   |
| Datendeduplizierung sowohl auf dem Quellenserver als auch auf dem Zielserver  |   | ✓  |   |   |
| Kostengünstige Skalierbarkeit, für die langfristige Aufbewahrung optimiert  |   |  |   | ✓   |
| <b>Effizienz und Kosten</b>   |   |  |   |   |
| Für Hochgeschwindigkeitssicherungsoperationen im Speicherbereichsnetz optimiert   |   |  | ✓   | ✓   |
| Für Hochgeschwindigkeitsoperationen im lokalen Netz (LAN) optimiert   | ✓   | ✓  | ✓   |   |
| Globale Datendeduplizierung für alle Datentypen und Quellen   | ✓   | ✓  | ✓   |   |
| Bandbreiteneffiziente Replikation   |   | ✓  | ✓   |   |
| Niedrigere Energiekosten  |   |  |   | ✓   |
| Option einer zweiten Kopie ohne weitere Plattenhardware   |   |  |   | ✓   |
| <b>Verfügbarkeit</b>  |   |  |   |   |
| Möglichkeit von Kopien an einem anderen Standort  |   | ✓  | ✓   | ✓   |
| Appliance-basierte Replikation  |   |  | ✓   |   |
| Clientwiederherstellung von einem Hochverfügbarkeitsserver  |   | ✓  |   |   |
| Replikationsziel in der Cloud   |   | ✓  |   |   |
| Unabhängige Verwaltung von Aufbewahrungsmaßnahmen für Replikationsdaten; Möglichkeit, am Wiederherstellungsstandort mehr oder weniger Daten aufzubewahren |   | ✓  |   |   |
| Replikation auf Anwendungsebene; Möglichkeit, die Systeme und Anwendungen auszuwählen, die repliziert werden  |   | ✓  |   |   |
| <b>Skalierbarkeit</b>   |   |  |   |   |

|  | Plattenspeicher an einem einzelnen Standort                                       | Plattenspeicher an mehreren Standorten   | Appliances an mehreren Standorten   | Band  |
|--|---|--|---|---|
|  |  |  |  |  |
| Globale Dateneduplizierung für alle Server                     |   |  | ✓   |   |
| Direkte SAN-optimierte Sicherung auf Band für große Datentypen |   |  |   | ✓   |
| Skalierbarkeit von Einzelinstanzen im Petabytebereich          |   |  |   | ✓   |

## Nächste Schritte

Lesen Sie die für die Lösungen verfügbare Dokumentation (siehe Roadmap für die Implementierung einer Datenschutzlösung).

### Zugehörige Verweise:

Plattenbasierte Implementierung einer Datenschutzlösung für einen einzelnen Standort

Plattenbasierte Implementierung einer Datenschutzlösung für mehrere Standorte

Appliance-basierte Implementierung einer Datenschutzlösung für mehrere Standorte

Bandbasierte Implementierung einer Datenschutzlösung

## Roadmap für die Implementierung einer Datenschutzlösung

Planen und implementieren Sie die geeignetste Datenschutzlösung für Ihre Geschäftsumgebung mit IBM Spectrum Protect.

### Plattenspeicherlösung für einen einzelnen Standort

Die Schritte, die die Planung, Implementierung, Überwachung und Ausführung einer Plattenspeicherlösung für einen einzelnen Standort beschreiben, finden Sie in Plattenspeicherlösung für einen einzelnen Standort.

### Plattenspeicherlösung für mehrere Standorte

Die Schritte, die die Planung, Implementierung, Überwachung und Ausführung einer Plattenspeicherlösung für mehrere Standorte beschreiben, finden Sie in Plattenspeicherlösung für mehrere Standorte.

### Bandspeicherlösung

Die Schritte, die die Planung, Implementierung, Überwachung und Ausführung einer Bandeinheitenlösung beschreiben, finden Sie in Bandspeicherlösung.

### Appliance-Lösung für mehrere Standorte

Eine Übersicht über die Tasks, die zur Implementierung einer Appliance-Lösung für mehrere Standorte erforderlich sind, liefern die folgenden Schritte:

1. Starten Sie die Planung für die Lösung, indem Sie die Informationen unter den folgenden Links lesen:
  - o AIX: Kapazitätsplanung
  - o Linux: Kapazitätsplanung
  - o Windows: Kapazitätsplanung
2. Installieren Sie den Server und wahlweise das Operations Center. Lesen Sie die Informationen unter den folgenden Links:
  - o Server installieren
  - o Installation und Upgrade für das Operations Center durchführen
3. Konfigurieren Sie den Server für Speicher in einem virtuellen Bandarchiv.
  - o Virtuelle Bandarchive verwalten
  - o Bandeinheiten für den Server anschließen

Eine Anleitung zur Verbesserung der Systemleistung finden Sie in Bewährte Verfahren bei der Konfiguration.

4. Konfigurieren Sie Maßnahmen zum Schützen Ihrer Daten. Lesen Sie die Informationen in Maßnahmen anpassen.
5. Definieren Sie Clientzeitpläne. Lesen Sie die Informationen in Sicherungs- und Archivierungsoperationen planen.

6. Installieren und konfigurieren Sie Clients. Ausführliche Informationen zur Bestimmung des Typs der erforderlichen Client-Software finden Sie in Clients hinzufügen.
7. Konfigurieren Sie die Überwachung für Ihr System. Lesen Sie die Informationen in Speicherlösungen überwachen.

**Zugehörige Verweise:**

Vergleich der Datenschutzlösungen  
Plattenbasierte Implementierung einer Datenschutzlösung für einen einzelnen Standort  
Plattenbasierte Implementierung einer Datenschutzlösung für mehrere Standorte  
Appliance-basierte Implementierung einer Datenschutzlösung für mehrere Standorte  
Bandbasierte Implementierung einer Datenschutzlösung

## Plattenspeicherlösung für einen einzelnen Standort

---

Diese Datenschutzlösung stellt kosteneffizienten Datenspeicher an einem einzelnen Standort mit minimaler Hardwarekonfiguration bereit.

- Planung für eine Plattenspeicherdatenschutzlösung für einen einzelnen Standort  
Führen Sie die Planung für eine Datenschutzimplementierung durch, die einen Server an einem einzelnen Standort umfasst, der Datendeduplizierung verwendet.
- Implementierung einer Plattenspeicherdatenschutzlösung für einen einzelnen Standort  
Die Plattenspeicherlösung für einen einzelnen Standort wird an einem einzelnen Standort konfiguriert und verwendet Datendeduplizierung und Replikation.
- Plattenspeicherlösung für einen einzelnen Standort überwachen  
Überwachen Sie nach der Implementierung einer Plattenspeicherlösung für einen einzelnen Standort mit IBM Spectrum Protect die Lösung auf ihre korrekte Funktionsweise. Indem die Lösung täglich und regelmäßig überwacht wird, können Sie bestehende und potenzielle Probleme erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden.
- Operationen für eine Plattenspeicherlösung für einen einzelnen Standort verwalten  
Verwenden Sie diese Informationen, um Operationen für eine Plattenspeicherlösung für einen einzelnen Standort mit IBM Spectrum Protect zu verwalten, die einen Server umfasst und Datendeduplizierung für einen einzelnen Standort verwendet.

## Planung für eine Plattenspeicherdatenschutzlösung für einen einzelnen Standort

---

Führen Sie die Planung für eine Datenschutzimplementierung durch, die einen Server an einem einzelnen Standort umfasst, der Datendeduplizierung verwendet.

### Implementierungsoptionen

---

Sie können den Server für eine Plattenspeicherlösung für einen einzelnen Standort wie folgt konfigurieren:

Server unter Verwendung des Operations Center und von Verwaltungsbefehlen konfigurieren

In dieser Dokumentation werden Schritte zum Konfigurieren einer Reihe von Speichersystemen und der Server-Software für Ihre Lösung bereitgestellt. Konfigurationstasks werden mithilfe von Assistenten und Optionen im Operations Center und mithilfe von IBM Spectrum Protect-Befehlen ausgeführt. Informationen zu ersten Schritten finden Sie in Planungsroadmap.

Server mithilfe automatisierter Scripts konfigurieren

Eine ausführliche Anleitung zur Implementierung einer Plattenspeicherlösung für einen einzelnen Standort mit bestimmten IBM® Storwize-Speichersystemen sowie zur Verwendung automatisierter Scripts zur Konfiguration des Servers finden Sie in den IBM Spectrum Protect-Blueprints. Die Dokumentation und Scripts sind unter IBM developerWorks verfügbar: IBM Spectrum Protect Blueprints.

Die Blueprint-Dokumentation umfasst keine Schritte zum Installieren und Konfigurieren des Operations Center oder zum Konfigurieren der sicheren Kommunikation mithilfe von Transport Security Layer (TLS). Eine Option zur Verwendung von Elastic Storage Server-Speicher auf der Basis der Technologie von IBM Spectrum Scale ist eingeschlossen.

### Planungsroadmap

---

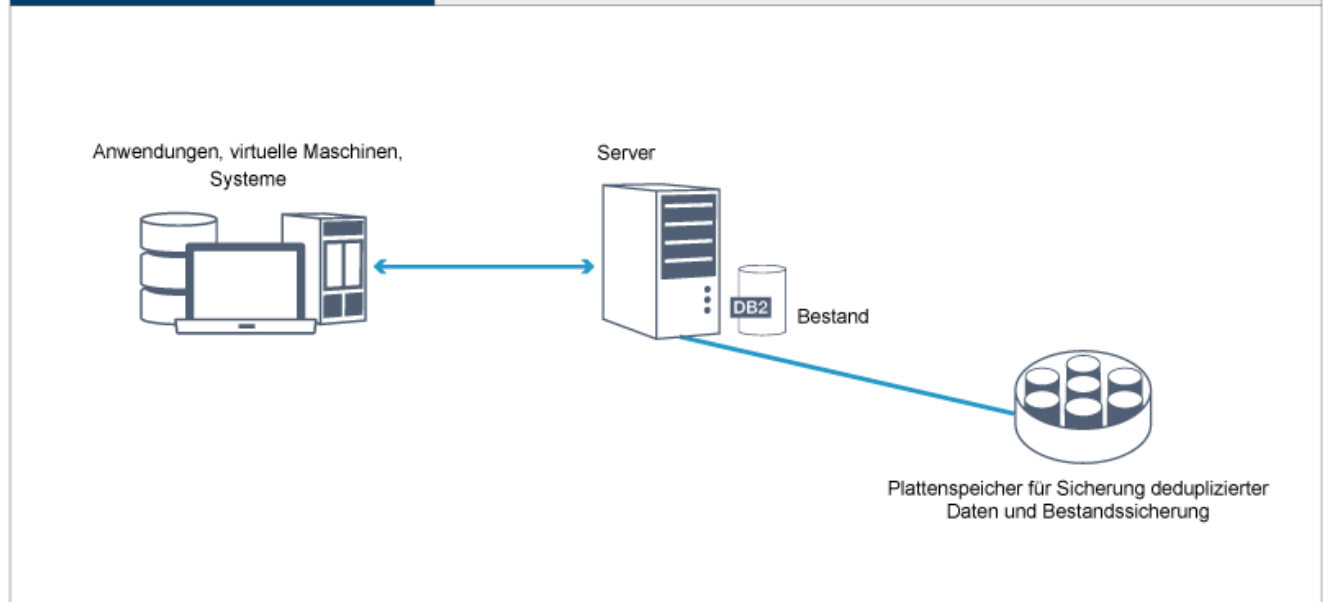
Planen Sie eine Plattenspeicherlösung für einen einzelnen Standort, indem Sie das Architekturlayout in der folgenden Abbildung überprüfen und dann die Roadmap-Tasks ausführen, die auf die Abbildung folgen.



## Plattenspeicher an einem einzelnen Standort

- ✓ Architektur für einen einzelnen Standort
- ✓ Platzsparend

- ✓ Kosteneffizient
- ✓ Einfachere Implementierung



Die folgenden Schritte sind für die Planung für eine Plattenspeicherumgebung an einem einzelnen Standort erforderlich.

1. Wählen Sie Ihre Systemgröße aus.
2. Erfüllen Sie die Systemvoraussetzungen für Hardware und Software.
3. Notieren Sie die Werte für Ihre Systemkonfiguration in den Arbeitsblättern zur Planung.
4. Führen Sie die Planung für den Speicher durch.
5. Führen Sie die Planung für die Sicherheit durch.
  - a. Führen Sie die Planung für Administratorrollen durch.
  - b. Führen Sie die Planung für die sichere Kommunikation durch.
  - c. Führen Sie die Planung für verschlüsselte Daten durch.
  - d. Führen Sie die Planung für den Firewallzugriff durch.

## Systemgröße auswählen

Wählen Sie die Größe des IBM Spectrum Protect-Servers auf der Basis des verwalteten Datenvolumens und der Systeme, die geschützt werden müssen, aus.

## Informationen zu diesem Vorgang

Mithilfe der Informationen in der Tabelle können Sie auf der Basis des verwalteten Datenvolumens die erforderliche Größe des Servers bestimmen.

In der folgenden Tabelle ist das Datenvolumen aufgeführt, das von einem Server verwaltet wird. Dieses Volumen umfasst alle Versionen. Das tägliche Datenvolumen gibt an, wie viele neue Daten täglich gesichert werden. Sowohl das Gesamtvolumen der verwalteten Daten als auch das tägliche Volumen an neuen Daten wird als Größe vor jeglicher Datenreduktion gemessen.

Tabelle 1. Größe des Servers bestimmen

| Gesamtvolumen der verwalteten Daten | Volumen an täglich zu sichernden neuen Daten | Erforderliche Servergröße |
|-------------------------------------|--|---------------------------|
| 60 TB bis 240 TB                    | Bis zu 10 TB pro Tag                         | Klein                     |
| 196 TB bis 784 TB                   | 10 bis 20 TB pro Tag                         | Mittelgroß                |
| 1000 TB bis 4000 TB                 | 20 bis 100 TB pro Tag                        | Groß                      |

Die Werte für die tägliche Sicherung in der Tabelle basieren auf Testergebnissen für Objekte mit einer Größe von 128 MB, die von IBM Spectrum Protect for Virtual Environments verwendet werden. Bei Workloads, die aus Objekten bestehen, die kleiner als 128 KB sind, werden diese Grenzwerte für tägliche Sicherungen möglicherweise nicht erreicht.

# Systemvoraussetzungen für eine Plattenspeicherlösung für einen einzelnen Standort

Überprüfen Sie nach der Auswahl der besten IBM Spectrum Protect-Lösung für Ihre Datenschutzanforderungen die Systemvoraussetzungen, um die Planung für die Implementierung der Datenschutzlösung auszuführen.

Stellen Sie sicher, dass Ihr System die Hardware- und Softwarevoraussetzungen für die geplante Größe des Servers erfüllt.

- **Hardwarevoraussetzungen**  
Hardwarevoraussetzungen für Ihre IBM Spectrum Protect-Lösung basieren auf der Systemgröße. Wählen Sie funktional entsprechende oder bessere Komponenten als die aufgelisteten aus, um optimale Leistung für Ihre Umgebung zu gewährleisten.
- **Softwarevoraussetzungen**  
Die Dokumentation für die IBM Spectrum Protect-Plattenspeicherlösung für einen einzelnen Standort umfasst Installations- und Konfigurationstasks für die folgenden Betriebssysteme. Die aufgelisteten Softwaremindestvoraussetzungen müssen erfüllt sein.

## Zugehörige Informationen:










[IBM Spectrum Protect Supported Operating Systems](#)

## Hardwarevoraussetzungen

Hardwarevoraussetzungen für Ihre IBM Spectrum Protect-Lösung basieren auf der Systemgröße. Wählen Sie funktional entsprechende oder bessere Komponenten als die aufgelisteten aus, um optimale Leistung für Ihre Umgebung zu gewährleisten.

Eine Definition der Systemgrößen finden Sie in Systemgröße auswählen.

In der folgenden Tabelle sind die Hardwaremindestvoraussetzungen für den Server und Speicher auf der Basis der Größe Servers aufgelistet, der erstellt werden soll. Wenn Sie logische Partitionen (LPARs) oder Arbeitspartitionen (WPARs) verwenden, passen Sie die Netzvoraussetzungen an, um den Partitionsgrößen Rechnung zu tragen.

| Hardwarekomponente | Kleines System  | Mittelgroßes System   | Großes System   |
|--------------------|---|---|---|
| Serverprozessor    |  AIX-Betriebssysteme6<br>Prozessorkerne, 3,42 GHz oder schneller<br><br> Linux-Betriebssysteme<br> Windows-Betriebssysteme12<br>Prozessorkerne, 1,9 GHz oder schneller |  AIX-Betriebssysteme8<br>Prozessorkerne, 3,42 GHz oder schneller<br><br> Linux-Betriebssysteme<br> Windows-Betriebssysteme16<br>Prozessorkerne, 2,0 GHz oder schneller |  AIX-Betriebssysteme20<br>Prozessorkerne, 3,42 GHz<br><br> Linux-Betriebssysteme<br> Windows-Betriebssysteme32<br>Prozessorkerne, 2,0 GHz oder schneller |
| Serverspeicher     | 64 GB RAM   | 128 GB RAM  | 192 GB RAM  |
| Netz               | <ul style="list-style-type: none"> <li>• 10 GB Ethernet (1 Port)</li> <li>• 8 GB Fibre Channel-Adapter (2 Ports)</li> </ul>   | <ul style="list-style-type: none"> <li>• 10 GB Ethernet (2 Ports)</li> <li>• 8 GB Fibre Channel-Adapter (2 Ports)</li> </ul>  | <ul style="list-style-type: none"> <li>• 10 GB Ethernet (4 Ports)</li> <li>• 8 GB Fibre Channel-Adapter (4 Ports)</li> </ul>  |
| Speicher           | <ul style="list-style-type: none"> <li>• 1,3 TB Bestand plus Speicherbereich für Operations Center-Datensätze</li> <li>• 46 TB deduplizierter Verzeichniscontainerspeicherpool</li> </ul>   | <ul style="list-style-type: none"> <li>• 2 TB Bestand plus Speicherbereich für Operations Center-Datensätze</li> <li>• 200 TB deduplizierter Verzeichniscontainerspeicherpool</li> </ul>  | <ul style="list-style-type: none"> <li>• 6 TB Bestand plus Speicherbereich für Operations Center-Datensätze</li> <li>• 1000 TB deduplizierter Verzeichniscontainerspeicherpool</li> </ul>   |

## Speicherbedarf für die Datenbank für das Operations Center schätzen

Hardwarevoraussetzungen für das Operations Center sind mit Ausnahme des Speicherbereichs für die Datenbank und das Archivprotokoll (Bestand), den das Operations Center zum Aufnehmen von Datensätzen für verwaltete Clients verwendet, in die vorherige Tabelle eingeschlossen.

Wenn Sie nicht planen, das Operations Center auf demselben System wie den Server zu installieren, können Sie die Systemanforderungen separat schätzen. Informationen zum Berechnen der Systemanforderungen für das Operations Center enthält die Technote 1641684 für die Berechnungsfunktion der Systemanforderungen.

Die Verwaltung des Operations Center auf dem Server stellt eine Workload dar, die zusätzlichen Speicherbereich für Datenbankoperationen erfordert. Wie viel Speicherbereich erforderlich ist, ist von der Anzahl Clients abhängig, die auf einem Server überwacht werden. Lesen Sie die folgenden Richtlinien, um schätzen zu können, wie viel Speicherbereich Ihr Server erfordert.

#### Speicherbereich in der Datenbank

Das Operations Center benötigt ungefähr 1,2 GB Speicherbereich in der Datenbank pro 1000 Clients, die auf einem Server überwacht werden. Angenommen, ein Hub-Server überwacht 2000 Clients und verwaltet außerdem drei Peripherieserver mit jeweils 1500 Clients. Bei dieser Konfiguration sind insgesamt 6500 Clients auf den vier Servern vorhanden und ungefähr 8,4 GB Speicherbereich in der Datenbank erforderlich. Bei der Berechnung dieses Werts werden die 6500 Clients auf den nächsthöheren Tausenderwert aufgerundet, d. h. auf 7000:

$$7 \times 1,2 \text{ GB} = 8,4 \text{ GB}$$

#### Speicherbereich für das Archivprotokoll

Das Operations Center verwendet alle 24 Stunden ungefähr 8 GB Speicherbereich für das Archivprotokoll pro 1000 Clients. In dem Beispiel mit den 6500 Clients auf dem Hub-Server und den Peripherieservern werden in einem Zeitraum von 24 Stunden für den Hub-Server 56 GB Speicherbereich für das Archivprotokoll verwendet.

Für jeden Peripherieserver in dem Beispiel werden im Verlauf von 24 Stunden etwa 16 GB Speicherbereich für das Archivprotokoll verwendet. Diese Schätzungen basieren auf dem Standardintervall von 5 Minuten zur Erfassung von Statusdaten. Wenn Sie das Erfassungsintervall von einmal alle 5 Minuten auf einmal alle 3 Minuten reduzieren, erhöht sich der Speicherbedarf. Das folgende Beispiel zeigt die ungefähre Erhöhung des Protokollspeicherbedarfs bei einem Erfassungsintervall von einmal alle 3 Minuten:

- Hub-Server: von 56 GB auf ungefähr 94 GB
- Jeder Peripherieserver: von 16 GB auf ungefähr 28 GB

Vergrößern Sie den Speicherbereich für das Archivprotokoll, sodass genügend Speicherbereich zur Unterstützung des Operations Center ohne Auswirkungen auf die vorhandenen Serveroperationen verfügbar ist.

## Softwarevoraussetzungen

Die Dokumentation für die IBM Spectrum Protect-Plattenspeicherlösung für einen einzelnen Standort umfasst Installations- und Konfigurationstasks für die folgenden Betriebssysteme. Die aufgelisteten Softwaremindestvoraussetzungen müssen erfüllt sein.

Informationen zu den Softwarevoraussetzungen für IBM® lin\_tape-Einheitentreiber finden Sie in der Veröffentlichung IBM Tape Device Drivers Installation and User's Guide.

## AIX-Systeme

| Softwaretyp           | Softwaremindestvoraussetzungen   |
|-----------------------|--|
| Betriebssystem        | IBM AIX 7.1<br><br>Weitere Informationen zu Betriebssystemvoraussetzungen finden Sie in AIX: Systemmindestvoraussetzungen für AIX-Systeme.   |
| Dienstprogramm gunzip | Das Dienstprogramm gunzip muss auf Ihrem System verfügbar sein, bevor Sie die Installation oder das Upgrade für den IBM Spectrum Protect-Server ausführen. Stellen Sie sicher, dass das Dienstprogramm gunzip installiert ist und der Pfad zu diesem Dienstprogramm in der Umgebungsvariablen PATH definiert ist.  |
| Dateisystemtyp        | JFS2-Dateisysteme<br><br>AIX-Systeme können ein großes Volumen an Dateisystemdaten zwischenspeichern, wodurch der Speicherplatz, der für Server- und IBM DB2-Prozesse erforderlich ist, reduziert werden kann. Um beim AIX-Server eine Auslagerung zu verhindern, verwenden Sie die Mountoption rbrw für das JFS2-Dateisystem. Für den Dateisystemcache wird weniger Speicher verwendet und für IBM Spectrum Protect ist mehr Speicher verfügbar.<br><br>Verwenden Sie nicht die Mountoptionen für Dateisysteme, gleichzeitige E/A (CIO = Concurrent I/O) und direkte E/A (DIO = Direct I/O) für Dateisysteme, die die IBM Spectrum Protect-Datenbank, Protokolle oder Speicherpooldatenträger enthalten. Diese Optionen können eine Leistungsverschlechterung vieler Serveroperationen zur Folge haben. IBM Spectrum Protect und DB2 können, wenn dies von Vorteil ist, weiterhin DIO verwenden, IBM Spectrum Protect erfordert die Mountoptionen jedoch nicht, um die Vorteile dieser Verfahren selektiv nutzen zu können. |
| Andere Software       | Korn-Shell (ksh)   |

## Linux-Systeme



| Softwaretyp     | Softwaremindestvoraussetzungen   |
|-----------------|--|
| Betriebssystem  | Red Hat Enterprise Linux 7 (x86_64)  |
| Bibliotheken    | GNU C-Bibliotheken, Version 2.3.3-98.38 oder höher, die auf dem IBM Spectrum Protect-System installiert sind.<br>Red Hat Enterprise Linux-Server: <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 (32-Bit- und 64-Bit-Pakete sind erforderlich)</li> <li>• numactl.x86_64</li> </ul> |
| Dateisystemtyp  | Formatieren Sie datenbankbezogene Dateisysteme mit ext3 oder ext4.<br>Verwenden Sie für speicherpoolbezogene Dateisysteme XFS.   |
| Andere Software | Korn-Shell (ksh)   |

## Windows-Systeme

| Softwaretyp     | Softwaremindestvoraussetzungen   |
|-----------------|--|
| Betriebssystem  | Microsoft Windows Server 2012 R2 (64-Bit) oder Windows Server 2016   |
| Dateisystemtyp  | NTFS   |
| Andere Software | Windows 2012 R2 oder Windows 2016 mit .NET Framework 3.5 ist installiert und aktiviert.<br>Die folgenden Benutzerkontensteuerungsrichtlinien müssen inaktiviert sein: <ul style="list-style-type: none"> <li>• Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto</li> <li>• Benutzerkontensteuerung: Alle Administratoren im Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen</li> </ul> |

### Zugehörige Tasks:

- ☛ AIX-Netzoptionen definieren

## Arbeitsblätter zur Planung

Verwenden Sie die Arbeitsblätter zur Planung für die Aufzeichnung von Werten, die Sie bei der Konfiguration Ihres Systems und bei der Konfiguration des IBM Spectrum Protect-Servers verwenden. Verwenden Sie die Best-Practice-Standardwerte, die in den Arbeitsblättern aufgeführt sind.

Jedes Arbeitsblatt unterstützt Sie bei den Vorbereitungen für unterschiedliche Teile der Systemkonfiguration mithilfe der Best-Practice-Werte:

### Vorkonfiguration des Serversystems

Führen Sie mithilfe der Arbeitsblätter zur Vorkonfiguration die Planung für die Dateisysteme und Verzeichnisse aus, die erstellt werden sollen, wenn Sie während der Systemkonfiguration Dateisysteme für IBM Spectrum Protect konfigurieren. Alle Verzeichnisse, die Sie für den Server erstellen, müssen leer sein.

### Serverkonfiguration

Verwenden Sie die Arbeitsblätter zur Konfiguration, wenn Sie den Server konfigurieren. Für die meisten Elemente werden Standardwerte vorgeschlagen; andernfalls ist ein entsprechender Hinweis vorhanden.

## AIX

Tabelle 1. Arbeitsblatt für die Vorkonfiguration eines AIX-Serversystems

| Element | Standardwert | Eigener Wert | Minimale Verzeichnisgröße | Anmerkungen |
|---------|--------------|--------------|---------------------------|-------------|
|         |              |              |                           |             |

| Element   | Standardwert            | Eigener Wert | Minimale Verzeichnisgröße   | Anmerkungen  |
|---|-------------------------|--------------|---|--|
| TCP/IP-Portadresse für die Kommunikation mit dem Server | 1500                    |              | Nicht zutreffend  | Stellen Sie sicher, dass dieser Port verfügbar ist, wenn Sie das Betriebssystem installieren und konfigurieren.<br><br>Die Portnummer kann eine Zahl zwischen 1024 und 32767 sein. |
| Verzeichnis für die Serverinstanz                       | /home/tsminst1/tsminst1 |              | 50 GB   | Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den DB2-Instanzeigner in Tabelle 2.                          |
| Verzeichnis für Serverinstallation                      | /                       |              | Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist:<br>5 GB                                |  |
| Verzeichnis für Serverinstallation                      | /usr                    |              | Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist:<br>5 GB                                |  |
| Verzeichnis für Serverinstallation                      | /var                    |              | Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist:<br>5 GB                                |  |
| Verzeichnis für Serverinstallation                      | /tmp                    |              | Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist:<br>5 GB                                |  |
| Verzeichnis für Serverinstallation                      | /opt                    |              | Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist:<br>10 GB                               |  |
| Verzeichnis für die aktive Protokolldatei               | /tsminst1/TSMalog       |              | <ul style="list-style-type: none"> <li>• Klein und mittel: 140 GB</li> <li>• Groß: 300 GB</li> </ul>          | Wenn Sie die aktive Protokolldatei während der Erstkonfiguration des Servers erstellen, setzen Sie die Größe auf 128 GB.   |
| Verzeichnis für das Archivprotokoll                     | /tsminst1/TSMarchlog    |              | <ul style="list-style-type: none"> <li>• Klein: 1 TB</li> <li>• Mittel: 2 TB</li> <li>• Groß: 4 TB</li> </ul> |  |

| Element                              | Standardwert  | Eigener Wert | Minimale Verzeichnisgröße   | Anmerkungen  |
|--------------------------------------|---|--------------|---|--|
| Verzeichnisse für die Datenbank      | /tsminst1/TSMdbspace00<br>/tsminst1/TSMdbspace01<br>/tsminst1/TSMdbspace02<br>/tsminst1/TSMdbspace03<br>... |              | Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: <ul style="list-style-type: none"> <li>• Klein: Mindestens 1 TB</li> <li>• Mittel: Mindestens 2 TB</li> <li>• Groß: Mindestens 4 TB</li> </ul>      | Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank: <ul style="list-style-type: none"> <li>• Klein: Mindestens 4 Dateisysteme</li> <li>• Mittel: Mindestens 4 Dateisysteme</li> <li>• Groß: Mindestens 8 Dateisysteme</li> </ul>   |
| Verzeichnisse für Speicher           | /tsminst1/TSMfile00<br>/tsminst1/TSMfile01<br>/tsminst1/TSMfile02<br>/tsminst1/TSMfile03<br>...             |              | Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: <ul style="list-style-type: none"> <li>• Klein: Mindestens 38 TB</li> <li>• Mittel: Mindestens 180 TB</li> <li>• Groß: Mindestens 500 TB</li> </ul> | Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher: <ul style="list-style-type: none"> <li>• Klein: Mindestens 10 Dateisysteme</li> <li>• Mittel: Mindestens 20 Dateisysteme</li> <li>• Groß: Mindestens 40 Dateisysteme</li> </ul>   |
| Verzeichnisse für Datenbanksicherung | /tsminst1/TSMbkup00<br>/tsminst1/TSMbkup01<br>/tsminst1/TSMbkup02<br>/tsminst1/TSMbkup03                    |              | Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: <ul style="list-style-type: none"> <li>• Klein: Mindestens 3 TB</li> <li>• Mittel: Mindestens 10 TB</li> <li>• Groß: Mindestens 16 TB</li> </ul>    | Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank: <ul style="list-style-type: none"> <li>• Klein: Mindestens 2 Dateisysteme</li> <li>• Mittel: Mindestens 4 Dateisysteme</li> <li>• Groß: Mindestens 4 Dateisysteme, vorzugsweise jedoch 6</li> </ul> <p>Das erste Datenbanksicherungsv erzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfiguration sdatei verwendet.</p> |

Tabelle 2. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

| Element  | Standardwert   | Eigener Wert | Anmerkungen   |
|--|--|--------------|---|
| DB2-Instanzeigner                                      | tsminst1   |              | Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 1 in einen anderen Wert geändert haben, ändern Sie auch den Wert für den DB2-Instanzeigner.   |
| Kennwort des DB2-Instanzeigners                        | passwd   |              | Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.   |
| Primärgruppe für den DB2-Instanzeigner                 | tsmsrvs  |              |   |
| Servername   | Der Standardwert für den Servernamen ist der Systemhostname. |              |   |
| Serverkennwort   | passwd   |              | Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.  |
| Administrator-ID:<br>Benutzer-ID für die Serverinstanz | admin  |              |   |
| Kennwort für die Administrator-ID                      | passwd   |              | Wählen Sie für das Administratorkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.   |
| Startzeit des Zeitplans                                | 22:00  |              | Die standardmäßige Startzeit des Zeitplans gibt den Anfang der Client-Workload-Phase an, die sich in erster Linie auf die Clientsicherungs- und -archivierungsaktivitäten bezieht. Während der Client-Workload-Phase werden Clientoperationen durch Serverressourcen unterstützt. Normalerweise werden diese Operationen während des nächtlichen Zeitplanfensters ausgeführt.<br><br>Zeitpläne für Serververwaltungsoperationen beginnen gemäß Definition 10 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen. |

## Linux

Tabelle 3. Arbeitsblatt für die Vorkonfiguration eines Linux-Serversystems

| Element | Standardwert | Eigener Wert | Minimale Verzeichnisgröße | Anmerkungen |
|---------|--------------|--------------|---------------------------|-------------|
|---------|--------------|--------------|---------------------------|-------------|

| Element   | Standardwert  | Eigener Wert | Minimale Verzeichnisgröße  | Anmerkungen   |
|---|---|--------------|--|---|
| TCP/IP-Portadresse für die Kommunikation mit dem Server | 1500  |              | Nicht zutreffend   | Stellen Sie sicher, dass dieser Port verfügbar ist, wenn Sie das Betriebssystem installieren und konfigurieren.<br><br>Die Portnummer kann eine Zahl zwischen 1024 und 32767 sein.  |
| Verzeichnis für die Serverinstanz                       | /home/tsminst1/tsminst1   |              | 25 GB  | Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den DB2-Instanzeigner in Tabelle 4.   |
| Verzeichnis für die aktive Protokolldatei               | /tsminst1/TSMalog   |              | <ul style="list-style-type: none"> <li>• Klein und mittel: 140 GB</li> <li>• Groß: 300 GB</li> </ul>   |   |
| Verzeichnis für das Archivprotokoll                     | /tsminst1/TSMarchlog  |              | <ul style="list-style-type: none"> <li>• Klein: 1 TB</li> <li>• Mittel: 2 TB</li> <li>• Groß: 4 TB</li> </ul>  |   |
| Verzeichnisse für die Datenbank                         | /tsminst1/TSMdbspace00<br>/tsminst1/TSMdbspace01<br>/tsminst1/TSMdbspace02<br>/tsminst1/TSMdbspace03<br>... |              | <p>Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 1 TB</li> <li>• Mittel: Mindestens 2 TB</li> <li>• Groß: Mindestens 4 TB</li> </ul>      | <p>Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 4 Dateisysteme</li> <li>• Mittel: Mindestens 4 Dateisysteme</li> <li>• Groß: Mindestens 8 Dateisysteme</li> </ul>   |
| Verzeichnisse für Speicher                              | /tsminst1/TSMfile00<br>/tsminst1/TSMfile01<br>/tsminst1/TSMfile02<br>/tsminst1/TSMfile03<br>...             |              | <p>Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 38 TB</li> <li>• Mittel: Mindestens 180 TB</li> <li>• Groß: Mindestens 500 TB</li> </ul> | <p>Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 10 Dateisysteme</li> <li>• Mittel: Mindestens 20 Dateisysteme</li> <li>• Groß: Mindestens 40 Dateisysteme</li> </ul> |

| Element                              | Standardwert   | Eigener Wert | Minimale Verzeichnisgröße   | Anmerkungen   |
|--------------------------------------|--|--------------|---|---|
| Verzeichnisse für Datenbanksicherung | /tsminst1/TSMbkup00<br>/tsminst1/TSMbkup01<br>/tsminst1/TSMbkup02<br>/tsminst1/TSMbkup03 |              | <p>Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 3 TB</li> <li>• Mittel: Mindestens 10 TB</li> <li>• Groß: Mindestens 16 TB</li> </ul> | <p>Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 2 Dateisysteme</li> <li>• Mittel: Mindestens 4 Dateisysteme</li> <li>• Groß: Mindestens 4 Dateisysteme, vorzugsweise jedoch 6</li> </ul> <p>Das erste Datenbanksicherungsv erzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfiguration sdatei verwendet.</p> |

Tabelle 4. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

| Element   | Standardwert   | Eigener Wert | Anmerkungen   |
|---|--|--------------|---|
| DB2-Instanzeigner                                   | tsminst1   |              | Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 3 in einen anderen Wert geändert haben, ändern Sie auch den Wert für den DB2-Instanzeigner. |
| Kennwort des DB2-Instanzeigners                     | passw0rd   |              | Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.             |
| Primärgruppe für den DB2-Instanzeigner              | tsmsrvrs   |              |   |
| Servername  | Der Standardwert für den Servernamen ist der Systemhostname. |              |   |
| Serverkennwort                                      | passw0rd   |              | Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.                          |
| Administrator-ID: Benutzer-ID für die Serverinstanz | admin  |              |   |

| Element                           | Standardwert | Eigener Wert | Anmerkungen   |
|-----------------------------------|--------------|--------------|---|
| Kennwort für die Administrator-ID | passw0rd     |              | Wählen Sie für das Administratorkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.   |
| Startzeit des Zeitplans           | 22:00        |              | Die standardmäßige Startzeit des Zeitplans gibt den Anfang der Client-Workload-Phase an, die sich in erster Linie auf die Clientsicherungs- und -archivierungsaktivitäten bezieht. Während der Client-Workload-Phase werden Clientoperationen durch Serverressourcen unterstützt. Normalerweise werden diese Operationen während des nächtlichen Zeitplanfensters ausgeführt.<br><br>Zeitpläne für Serververwaltungsoperationen beginnen gemäß Definition 10 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen. |

## Windows

Da für den Server viele Datenträger erstellt werden, konfigurieren Sie den Server mithilfe der Windows-Funktion zum Zuordnen von Plattendatenträgern zu Verzeichnissen (statt der Funktion zum Zuordnen von Plattendatenträgern zu Laufwerkbuchstaben).

Beispielsweise ist C:\tsminst1\TSMdbpsace00 ein Mountpunkt für einen Datenträger mit eigenem Speicherbereich. Der Datenträger wird einem Verzeichnis unter dem Laufwerk C: zugeordnet, nimmt aber keinen Speicherbereich auf Laufwerk C: in Anspruch. Einzige Ausnahme ist das Serverinstanzverzeichnis, C:\tsminst1, das ein Mountpunkt oder ein normales Verzeichnis sein kann.

Tabelle 5. Arbeitsblatt für die Vorkonfiguration eines Windows-Serversystems

| Element   | Standardwert        | Eigener Wert | Minimale Verzeichnisgröße  | Anmerkungen  |
|---|---------------------|--------------|--|--|
| TCP/IP-Portadresse für die Kommunikation mit dem Server | 1500                |              | Nicht zutreffend   | Stellen Sie sicher, dass dieser Port verfügbar ist, wenn Sie das Betriebssystem installieren und konfigurieren.<br><br>Die Portnummer kann eine Zahl zwischen 1024 und 32767 sein. |
| Verzeichnis für die Serverinstanz                       | C:\tsminst1         |              | 25 GB  | Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den DB2-Instanzeigner in Tabelle 6.                          |
| Verzeichnis für die aktive Protokolldatei               | C:\tsminst1\TSMalog |              | <ul style="list-style-type: none"> <li>• Klein und mittel: 140 GB</li> <li>• Groß: 300 GB</li> </ul> |  |

| Element                             | Standardwert  | Eigener Wert | Minimale Verzeichnisgröße  | Anmerkungen   |
|-------------------------------------|---|--------------|--|---|
| Verzeichnis für das Archivprotokoll | C:\tsminst1\TSMarchlog  |              | <ul style="list-style-type: none"> <li>• Klein: 1 TB</li> <li>• Mittel: 2 TB</li> <li>• Groß: 4 TB</li> </ul>  |   |
| Verzeichnisse für die Datenbank     | C:\tsminst1\TSMdbspace00<br>C:\tsminst1\TSMdbspace01<br>C:\tsminst1\TSMdbspace02<br>C:\tsminst1\TSMdbspace03<br>... |              | <p>Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 1 TB</li> <li>• Mittel: Mindestens 2 TB</li> <li>• Groß: Mindestens 4 TB</li> </ul>      | <p>Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 4 Dateisysteme</li> <li>• Mittel: Mindestens 4 Dateisysteme</li> <li>• Groß: Mindestens 8 Dateisysteme</li> </ul>   |
| Verzeichnisse für Speicher          | C:\tsminst1\TSMfile00<br>C:\tsminst1\TSMfile01<br>C:\tsminst1\TSMfile02<br>C:\tsminst1\TSMfile03<br>...             |              | <p>Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 38 TB</li> <li>• Mittel: Mindestens 180 TB</li> <li>• Groß: Mindestens 500 TB</li> </ul> | <p>Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 10 Dateisysteme</li> <li>• Mittel: Mindestens 20 Dateisysteme</li> <li>• Groß: Mindestens 40 Dateisysteme</li> </ul> |



| Element                              | Standardwert   | Eigener Wert | Minimale Verzeichnisgröße   | Anmerkungen   |
|--------------------------------------|--|--------------|---|---|
| Verzeichnisse für Datenbanksicherung | C:\tsminst1\TSMbkup00<br>C:\tsminst1\TSMbkup01<br>C:\tsminst1\TSMbkup02<br>C:\tsminst1\TSMbkup03 |              | <p>Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 3 TB</li> <li>• Mittel: Mindestens 10 TB</li> <li>• Groß: Mindestens 16 TB</li> </ul> | <p>Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 2 Dateisysteme</li> <li>• Mittel: Mindestens 4 Dateisysteme</li> <li>• Groß: Mindestens 4 Dateisysteme, vorzugsweise jedoch 6</li> </ul> <p>Das erste Datenbanksicherungsv erzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfiguration sdatei verwendet.</p> |

Tabelle 6. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

| Element   | Standardwert   | Eigener Wert | Anmerkungen   |
|---|--|--------------|---|
| DB2-Instanzeigner                                   | tsminst1   |              | Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 5 in einen anderen Wert geändert haben, ändern Sie auch den Wert für den DB2-Instanzeigner. |
| Kennwort des DB2-Instanzeigners                     | pAssW0rd   |              | Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.             |
| Servername  | Der Standardwert für den Servernamen ist der Systemhostname. |              |   |
| Serverkennwort                                      | passw0rd   |              | Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.                          |
| Administrator-ID: Benutzer-ID für die Serverinstanz | admin  |              |   |

| Element                           | Standardwert | Eigener Wert | Anmerkungen   |
|-----------------------------------|--------------|--------------|---|
| Kennwort für die Administrator-ID | passw0rd     |              | Wählen Sie für das Administratorkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.   |
| Startzeit des Zeitplans           | 22:00        |              | Die standardmäßige Startzeit des Zeitplans gibt den Anfang der Client-Workload-Phase an, die sich in erster Linie auf die Clientsicherungs- und -archivierungsaktivitäten bezieht. Während der Client-Workload-Phase werden Clientoperationen durch Serverressourcen unterstützt. Normalerweise werden diese Operationen während des nächtlichen Zeitplanfensters ausgeführt.<br><br>Zeitpläne für Serververwaltungsoperationen beginnen gemäß Definition 10 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen. |

## Planung für Speicher

Wählen Sie die effektivste Speichertechnologie für IBM Spectrum Protect-Komponenten aus, um effiziente Serverleistung und Serveroperationen zu gewährleisten.

Speicherhardwareeinheiten haben unterschiedliche Kapazitäts- und Leistungsmerkmale, die festlegen, wie die Einheiten effizient mit IBM Spectrum Protect verwendet werden können. Die folgenden Richtlinien stellen eine allgemeine Anleitung zur Auswahl der für Ihre Lösung geeigneten Speicherhardware und Konfiguration dar.

### Datenbank und aktive Protokolldatei

- Verwenden Sie eine schnelle Platte für die IBM Spectrum Protect-Datenbank und die aktive Protokolldatei, die beispielsweise die folgenden Merkmale hat:
  - Hochleistungsplatte mit 15.000 Umdrehungen pro Minute mit Fibre Channel- oder SAS-Schnittstelle
  - Solid-State-Platte (SSD)
- Trennen Sie die aktive Protokolldatei von der Datenbank, es sei denn, Sie verwenden SSD oder Flash-Hardware.
- Verwenden Sie beim Erstellen von Arrays für die Datenbank RAID-Stufe 5.

### Speicherpool

- Sie können kostengünstigere und langsamere Platten für den Speicherpool verwenden.
- Der Speicherpool kann Platten für den Speicher für das Archivprotokoll und die Datenbanksicherung gemeinsam nutzen.
- Verwenden Sie RAID-Stufe 6 für Speicherpoolarrays, um bei Verwendung von Typen großer Platten Schutz vor Laufwerkdoppelfehlern hinzuzufügen.
- Planung der Speicherarrays  
Bereiten Sie die Konfiguration des Plattenspeichers vor, indem Sie die Planung für RAID-Arrays und Datenträger gemäß der Größe Ihres IBM Spectrum Protect-Systems ausführen.

### Zugehörige Verweise:

[Speichersystemvoraussetzungen und Reduzierung des Risikos fehlerhafter Daten](#)

## Planung für Sicherheit

Planen Sie den Schutz der Sicherheit von Systemen in der IBM Spectrum Protect-Lösung mithilfe von Steuerelementen für Zugriff und Authentifizierung und ziehen Sie das Verschlüsseln von Daten und der Übertragung von Kennwörtern in Erwägung.

Richtlinien zum Schutz Ihrer Speicherumgebung vor Ransomware-Attacken und zur Wiederherstellung Ihrer Speicherumgebung nach einer Attacke finden Sie in Speicherumgebung vor Ransomware-Attacken schützen.

- **Planung für Administratorrollen**  
Definieren Sie die Berechtigungsstufen, die Administratoren zugeordnet werden sollen, die Zugriff auf die IBM Spectrum Protect-Lösung haben.
- **Planung für sichere Kommunikation**  
Planen Sie den Schutz der Kommunikation zwischen den IBM Spectrum Protect-Lösungskomponenten.
- **Planung für die Speicherung verschlüsselter Daten**  
Bestimmen Sie, ob Ihr Unternehmen die Verschlüsselung gespeicherter Daten erfordert, und wählen Sie für Ihre Anforderungen am besten geeignete Option aus.
- **Planung des Firewallzugriffs**  
Bestimmen Sie die definierten Firewalls und die Ports, die offen sein müssen, damit die IBM Spectrum Protect-Lösung funktionsfähig ist.

## Planung für Administratorrollen

Definieren Sie die Berechtigungsstufen, die Administratoren zugeordnet werden sollen, die Zugriff auf die IBM Spectrum Protect-Lösung haben.

Sie können Administratoren eine der folgenden Berechtigungsstufen zuordnen:

### Systemberechtigung

Administratoren mit Systemberechtigung verfügen über die höchste Berechtigungsstufe. Administratoren mit dieser Berechtigungsstufe können jede Task ausführen. Sie können alle Maßnahmendomänen und Speicherpools verwalten und anderen Administratoren Berechtigung erteilen.

### Maßnahmenberechtigung

Administratoren mit Maßnahmenberechtigung können alle Tasks verwalten, die sich auf die Maßnahmenverwaltung beziehen. Diese Berechtigung kann uneingeschränkt sein oder auf bestimmte Maßnahmendomänen eingeschränkt werden.

### Speicherberechtigung

Administratoren mit Speicherberechtigung können Speicherressourcen für den Server zuordnen und steuern.

### Bedienerberechtigung

Administratoren mit Bedienerberechtigung können den sofortigen Betrieb des Servers und die Verfügbarkeit von Speichermedien wie beispielsweise Bandarchiven und -laufwerken steuern.

Die Szenarios in Tabelle 1 enthalten Beispiele, die zeigen, warum es sinnvoll ist, Administratoren für die Ausführung von Tasks unterschiedliche Berechtigungsstufen zuzuordnen:

Tabelle 1. Szenarios für Administratorrollen

| Szenario  | Typ der zu konfigurierenden Administrator-ID  |
|---|---|
| Ein Administrator in einem kleinen Unternehmen verwaltet den Server und ist für alle Serveraktivitäten verantwortlich.  | <ul style="list-style-type: none"> <li>• Systemberechtigung: 1 Administrator-ID</li> </ul>  |
| Ein Administrator für mehrere Server verwaltet auch das gesamte System. Mehrere andere Administratoren verwalten ihre eigenen Speicherpools.  | <ul style="list-style-type: none"> <li>• Systemberechtigung auf allen Servern: 1 Administrator-ID für den Administrator des gesamten Systems</li> <li>• Speicherberechtigung für bestimmte Speicherpools: 1 Administrator-ID für jeden der anderen Administratoren</li> </ul> |
| Ein Administrator verwaltet 2 Server. Eine andere Person unterstützt ihn bei den Verwaltungstasks. Zwei Assistenten müssen sicherstellen, dass wichtige Systeme gesichert werden. Jeder Assistent ist für die Überwachung der geplanten Sicherungen auf einem der IBM Spectrum Protect-Server verantwortlich. | <ul style="list-style-type: none"> <li>• Systemberechtigung auf beiden Servern: 2 Administrator-IDs</li> <li>• Bedienerberechtigung: 2 Administrator-IDs für die Assistenten mit Zugriff auf den Server, für den die jeweilige Person verantwortlich ist.</li> </ul>          |

## Planung für sichere Kommunikation

Planen Sie den Schutz der Kommunikation zwischen den IBM Spectrum Protect-Lösungskomponenten.

Bestimmen Sie auf der Basis der Regelungen und Geschäftsanforderungen für Ihr Unternehmen, welche Stufe des Schutzes für Ihre Daten erforderlich ist.

Wenn Ihr Unternehmen ein hohes Maß an Sicherheit für Kennwörter und die Datenübertragung erfordert, planen Sie die Implementierung der sicheren Kommunikation mit dem Protokoll Transport Layer Security (TLS) oder Secure Sockets Layer (SSL).

TLS und SSL stellen sichere Kommunikation zwischen dem Server und dem Client bereit, können sich jedoch auf die Systemleistung auswirken. Um die Systemleistung zu verbessern, verwenden Sie TLS für die Authentifizierung, ohne Objektdaten zu verschlüsseln. Informationen zur Angabe, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, finden Sie in der Beschreibung der Clientoption SSL für die Client/Server-Kommunikation und der Beschreibung des Parameters UPDATE SERVER=SSL für die Kommunikation zwischen Servern. Ab Version 8.1.2 wird TLS standardmäßig für die Authentifizierung verwendet. Wenn Sie sich für die Verwendung von TLS entscheiden, um vollständige Sitzungen zu verschlüsseln, verwenden Sie das Protokoll nur für Sitzungen, für die es erforderlich ist; fügen Sie außerdem auf dem Server Prozessorressourcen hinzu, um den wachsenden Datenaustausch im Netz handhaben zu können. Sie können auch versuchsweise andere Optionen verwenden. Beispielsweise stellen einige Netzeinheiten wie Router und Switches die TLS- oder SSL-Funktion bereit.

Mithilfe von TLS und SSL können Sie einige oder alle der unterschiedlichen möglichen Kommunikationspfade schützen, beispielsweise:

- Operations Center: vom Browser zum Hub-Server; vom Hub-Server zum Peripherieserver
- Vom Client zum Server
- Vom Server zum Server: Knotenreplikation

**Zugehörige Tasks:**

 Kommunikation schützen


## Planung für die Speicherung verschlüsselter Daten

Bestimmen Sie, ob Ihr Unternehmen die Verschlüsselung gespeicherter Daten erfordert, und wählen Sie für Ihre Anforderungen am besten geeignete Option aus.

Wenn Ihr Unternehmen die Verschlüsselung der Daten in Speicherpools erfordert, können Sie entweder die IBM Spectrum Protect-Verschlüsselung oder eine externe Einheit wie beispielsweise ein Band für die Verschlüsselung verwenden.

Wenn Sie IBM Spectrum Protect zum Verschlüsseln der Daten auswählen, sind zusätzliche IT-Ressourcen auf dem Client erforderlich, die sich auf die Leistung von Sicherungs- und Zurückschreibungsprozessen auswirken können.

**Zugehörige Informationen:**

 [Technote 1963635](#)

## Planung des Firewallzugriffs

Bestimmen Sie die definierten Firewalls und die Ports, die offen sein müssen, damit die IBM Spectrum Protect-Lösung funktionsfähig ist.

In Tabelle 1 sind die Ports beschrieben, die vom Server, vom Client und vom Operations Center verwendet werden.

Tabelle 1. Vom Server, Client und Operations Center verwendete Ports

| Element                                   | Standardwert      | Richtung           | Beschreibung   |
|---|-------------------|--------------------|--|
| Basisport (TCPPOINT)                      | 1500              | Abgehend/Eingehend | Jede Serverinstanz erfordert einen eindeutigen Port. Sie können eine alternative Portnummer angeben, anstatt den Standardwert zu verwenden. Der mit der Option TCPPOINT angegebene Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen vom Client empfangsbereit. Für den Datenverkehr des Verwaltungsclients können Sie zum Festlegen von Portwerten die Optionen TCPADMINPORT und ADMINONCLIENTPORT verwenden. |
| Port ausschließlich für SSL (SSLTCPPOINT) | Kein Standardwert | Abgehend/Eingehend | Dieser Port wird verwendet, wenn die Kommunikation am Port auf ausschließlich SSL-fähige Sitzungen beschränkt werden soll. Um sowohl die SSL-Kommunikation als auch die Nicht-SSL-Kommunikation zu unterstützen, verwenden Sie die Option TCPPOINT oder TCPADMINPORT.  |
| SMB                                       | 45                | Eingehend/Abgehend | Dieser Port wird von Konfigurationsassistenten verwendet, die unter Verwendung nativer Protokolle mit mehreren Hosts kommunizieren.  |
| SSH                                       | 22                | Eingehend/Abgehend | Dieser Port wird von Konfigurationsassistenten verwendet, die unter Verwendung nativer Protokolle mit mehreren Hosts kommunizieren.  |
| SMTP                                      | 25                | Abgehend           | Dieser Port wird zum Senden von E-Mail-Alerts vom Server verwendet.  |

| Element                               | Standardwert                   | Richtung           | Beschreibung  |
|---------------------------------------|--------------------------------|--------------------|---|
| NDMP                                  | Kein Standardwert              | Eingehend/Abgehend | <p>Der Server muss eine abgehende NDMP-Steuerportverbindung zu der NAS-Einheit öffnen können. Der abgehende Steuerport ist die Adresse der unteren Ebene in der Definition der Einheit zum Versetzen von Daten für die NAS-Einheit.</p> <p>Während einer NDMP-Zurückschreibung vom Dateiserver auf den Server muss der Server eine abgehende NDMP-Datenverbindung zu der NAS-Einheit öffnen können. Der Datenverbindungsport, der während einer Zurückschreibung verwendet wird, kann auf der NAS-Einheit konfiguriert werden.</p> <p>Während NDMP-Sicherungen vom Dateiserver auf den Server muss die NAS-Einheit abgehende Datenverbindungen zum Server öffnen können und der Server muss eingehende NDMP-Datenverbindungen akzeptieren können. Mithilfe der Serveroption NDMPPORTRANGE können Sie die für die Verwendung als NDMP-Datenverbindungen verfügbare Gruppe von Ports einschränken. Sie können eine Firewall für Verbindungen zu diesen Ports konfigurieren.</p> |
| Replikation                           | Kein Standardwert              | Abgehend/Eingehend | <p>Der Port und das Protokoll für den Port für abgehende Daten für die Replikation werden mit dem Befehl DEFINE SERVER festgelegt, der zum Konfigurieren der Replikation verwendet wird.</p> <p>Bei den Ports für eingehende Daten für die Replikation handelt es sich um die TCP-Ports und SSL-Ports, die für den Quellenserver im Befehl DEFINE SERVER angegeben werden.</p>  |
| Port für Clientzeitplan               | Client-Port: 1501              | Abgehend           | Der Client ist an dem angegebenen Port empfangsbereit und teilt die Portnummer dem Server mit. Der Server kontaktiert den Client, wenn die servergesteuerte Zeitplanung verwendet wird. Sie können eine alternative Portnummer in der Clientoptionsdatei angeben.   |
| Lange laufende Sitzungen              | Einstellung für KEEPALIVE: YES | Abgehend           | Wenn die Option KEEPALIVE aktiviert ist, werden während Client/Server-Sitzungen Keepalive-Pakete gesendet, um zu verhindern, dass die Firewall-Software lange laufende inaktive Verbindungen schließt.  |
| Operations Center                     | HTTPS: 11090                   | Eingehend          | Diese Ports werden für den Web-Browser des Operations Center verwendet. Sie können eine alternative Portnummer angeben.   |
| Port für den Clientverwaltungsservice | Client-Port: 9028              | Eingehend          | Der Zugriff auf den Port für den Clientverwaltungsservice muss über das Operations Center möglich sein. Stellen Sie sicher, dass Verbindungen nicht durch Firewalls verhindert werden können. Der Clientverwaltungsservice verwendet den TCP-Port des Servers für den Clientknoten für die Authentifizierung unter Verwendung einer Verwaltungssitzung.   |

## Implementierung einer Plattenspeicherdatenschutzlösung für einen einzelnen Standort

Die Plattenspeicherlösung für einen einzelnen Standort wird an einem einzelnen Standort konfiguriert und verwendet Datenduplizierung und Replikation.

### Implementierungsroadmap

Die folgenden Schritte sind zum Konfigurieren der IBM Spectrum Protect-Plattenspeicherumgebung an einem einzelnen Standort erforderlich.

1. Konfigurieren Sie das System.
  - a. Konfigurieren Sie die Speicherhardware und Speicherarrays für Ihre Umgebungsgröße.
  - b. Installieren Sie das Serverbetriebssystem.
  - c. Konfigurieren Sie Multipath I/O.
  - d. Erstellen Sie die Benutzer-ID für die Serverinstanz.
  - e. Bereiten Sie Dateisysteme für IBM Spectrum Protect vor.

2. Installieren Sie den Server und das Operations Center.
3. Konfigurieren Sie den Server und das Operations Center.
  - a. Führen Sie die Erstkonfiguration des Servers aus.
  - b. Legen Sie Serveroptionen fest.
  - c. Konfigurieren Sie Secure Sockets Layer für den Server und den Client.
  - d. Konfigurieren Sie das Operations Center.
  - e. Registrieren Sie Ihre IBM Spectrum Protect-Lizenz.
  - f. Konfigurieren Sie die Dateneduplizierung.
  - g. Definieren Sie Datenaufbewahrungsregeln für Ihr Unternehmen.
  - h. Definieren Sie Zeitpläne für die Serververwaltung.
  - i. Definieren Sie Clientzeitpläne.
4. Installieren und konfigurieren Sie Clients.
  - a. Registrieren Sie Clients und ordnen Sie Clients Zeitplänen zu.
  - b. Installieren und überprüfen Sie den Clientverwaltungsservice.
  - c. Konfigurieren Sie das Operations Center für die Verwendung des Clientverwaltungsservice.
5. Schließen Sie die Implementierung ab.

## System konfigurieren

---

Um das System konfigurieren zu können, müssen Sie zunächst Ihre Plattenspeicherhardware und das Serversystem für IBM Spectrum Protect konfigurieren.

- Speicherhardware konfigurieren  
Um Ihre Speicherhardware zu konfigurieren, lesen Sie die allgemeine Anleitung für Plattensysteme und IBM Spectrum Protect.
- Serverbetriebssystem installieren  
Installieren Sie das Betriebssystem auf dem Serversystem und stellen Sie sicher, dass die Voraussetzungen für den IBM Spectrum Protect-Server erfüllt sind. Passen Sie Betriebssystemeinstellungen gemäß Anweisung an.
- Multipath I/O konfigurieren  
Sie können Multipathing für Plattenspeicher aktivieren und konfigurieren. Die mit Ihrer Hardware zur Verfügung gestellte Dokumentation enthält ausführliche Anweisungen.
- Benutzer-ID für den Server erstellen  
Erstellen Sie die Benutzer-ID, die Eigner der IBM Spectrum Protect-Serverinstanz ist. Sie geben diese Benutzer-ID an, wenn Sie die Serverinstanz im Rahmen der Erstkonfiguration des Servers erstellen.
- Dateisysteme für den Server vorbereiten  
Sie müssen die Dateisystemkonfiguration ausführen, damit der Plattenspeicher vom Server verwendet werden kann.

## Speicherhardware konfigurieren

---

Um Ihre Speicherhardware zu konfigurieren, lesen Sie die allgemeine Anleitung für Plattensysteme und IBM Spectrum Protect.

### Vorgehensweise

---

1. Stellen Sie unter Berücksichtigung der folgenden Richtlinien eine Verbindung zwischen dem Server und den Speichereinheiten her:
  - Verwenden Sie einen Switch oder eine Direktverbindung für Fibre Channel-Verbindungen.
  - Berücksichtigen Sie die Anzahl Ports, die verbunden sind, und die erforderliche Bandbreite.
  - Berücksichtigen Sie die Anzahl Ports auf dem Server und die Anzahl Host-Ports auf dem Plattensystem, die verbunden sind.
2. Stellen Sie sicher, dass die Einheitentreiber und die Firmware für das Serversystem, die Adapter und das Betriebssystem aktuell sind und die empfohlenen Versionen haben.
3. Konfigurieren Sie Speicherarrays. Stellen Sie sicher, dass Sie entsprechend geplant haben, um die optimale Leistung zu gewährleisten. Weitere Informationen finden Sie in Planung für Speicher.
4. Stellen Sie sicher, dass das Serversystem Zugriff auf Plattendatenträger hat, die erstellt werden. Führen Sie die folgenden Schritte aus:
  - a. Wenn das System mit einem Fibre Channel-Switch verbunden ist, verzonen Sie den Server, um die Platten anzuzeigen.
  - b. Ordnen Sie alle Datenträger zu, um dem Plattensystem mitzuteilen, dass diesem spezifischen Server die Anzeige jeder Platte ermöglicht werden soll.

## Serverbetriebssystem installieren

---

Installieren Sie das Betriebssystem auf dem Serversystem und stellen Sie sicher, dass die Voraussetzungen für den IBM Spectrum Protect-Server erfüllt sind. Passen Sie Betriebssystemeinstellungen gemäß Anweisung an.

- Installation auf AIX-Systemen  
Führen Sie die folgenden Schritte aus, um AIX auf dem Serversystem zu installieren.
- Installation auf Linux-Systemen  
Führen Sie die folgenden Schritte aus, um Linux x86\_64 auf dem Serversystem zu installieren.
- Installation auf Windows-Systemen  
Installieren Sie Microsoft Windows Server 2012 Standard Edition auf dem Serversystem und bereiten Sie das System für die Installation und Konfiguration des IBM Spectrum Protect-Servers vor.

## Installation auf AIX-Systemen

---

Führen Sie die folgenden Schritte aus, um AIX auf dem Serversystem zu installieren.

### Vorgehensweise

---

1. Installieren Sie AIX Version 7.1, TL4, SP2 oder höher gemäß den Anweisungen des Herstellers.
2. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Anweisungen zur Installation des Betriebssystems.
3. Öffnen Sie die Datei /etc/hosts und führen Sie die folgenden Aktionen aus:
  - Aktualisieren Sie die Datei, um die IP-Adresse und den Hostnamen des Servers einzuschließen. Beispiel:

```
192.0.2.7 server.yourdomain.com server
```

- Überprüfen Sie, ob die Datei einen Eintrag für localhost mit der Adresse 127.0.0.1 enthält. Beispiel:

```
127.0.0.1 localhost
```

4. Aktivieren Sie die AIX-I/O Completion Ports (IOCP), indem Sie den folgenden Befehl eingeben:

```
chdev -l iocp0 -P
```

Die Olson-Zeitzonendefinition kann sich auf die Serverleistung auswirken.

5. Um die Leistung zu optimieren, ändern Sie Ihr Systemzeitonenformat von Olson in POSIX. Verwenden Sie das folgende Befehlsformat zum Aktualisieren der Zeitzoneneinstellung:

```
chtz=Ortszeitzone,Datum/Uhrzeit,Datum/Uhrzeit
```

Beispielsweise würden Sie in Tucson, Arizona, wo die Mountain Standard Time gilt, den folgenden Befehl ausgeben, um das Format in das POSIX-Format zu ändern:

```
chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
```

6. Fügen Sie in .profile des Instanzbenutzers einen Eintrag hinzu, um die folgende Umgebung festzulegen:

```
export MALLOCOPTIONS=multiheap:16
```

7. Legen Sie fest, dass das System vollständige Anwendungskerndateien erstellen soll. Geben Sie den folgenden Befehl aus:

```
chdev -l sys0 -a fullcore=true -P
```

8. Stellen Sie für die Kommunikation mit dem Server und dem Operations Center sicher, dass die folgenden Ports für alle Firewalls, die gegebenenfalls vorhanden sind, offen sind:

- Öffnen Sie für die Kommunikation mit dem Server Port 1500.
- Öffnen Sie für die sichere Kommunikation mit dem Operations Center Port 11090 auf dem Hub-Server.

Wenn Sie nicht die Standardwerte für Ports verwenden, stellen Sie sicher, dass die verwendeten Ports offen sind.

9. Aktivieren Sie TCP-Hochleistungsverbesserungen. Geben Sie den folgenden Befehl aus:

```
no -p -o rfc1323=1
```

10. Um optimalen Durchsatz und optimale Zuverlässigkeit zu gewährleisten, kombinieren Sie vier 10-Gb-Ethernet-Ports durch Bonding miteinander. Verwenden Sie das System Management Interface Tool (SMIT), um die Ports durch Bonding unter Verwendung von Etherchannel zu kombinieren. Beim Testen wurden die folgenden Einstellungen verwendet:

|                |              |   |
|----------------|--------------|---|
| mode           | 8023ad       |   |
| auto_recovery  | yes          | Automatische Wiederherstellung nach Übernahme aktivieren          |
| backup_adapter | NONE         | Adapter, der beim Fehlschlagen des gesamten Kanals verwendet wird |
| hash_mode      | src_dst_port | Legt fest, wie der abgehende Adapter ausgewählt wird              |
| interval       | long         | Legt den Intervallwert für den IEEE-Modus 802.3ad fest            |

|                 |        |   |
|-----------------|--------|---|
| mode            | 8023ad | EtherChannel-Betriebsart  |
| netaddr         | 0      | Mit Ping zu überprüfende Adresse  |
| noloss_failover | yes    | Verlustfreie Übernahme nach dem Fehlschlagen des Pingbefehls aktivieren |
| num_retries     | 3      | Anzahl Wiederholungen für Pingbefehl vor dem Fehlschlagen               |
| retry_time      | 1      | Wartezeit (in Sekunden) zwischen Pingbefehlen                           |
| use_alt_addr    | no     | Alternative EtherChannel-Adresse aktivieren                             |
| use_jumbo_frame | no     | Jumbo-Frames für Gigabit Ethernet aktivieren                            |

11. Überprüfen Sie, ob Benutzerprozessressourcengrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, gemäß den Richtlinien in Tabelle 1 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

Tabelle 1. Benutzergrenzwerte (ulimit-Werte)

| Typ des Benutzergrenzwerts                           | Einstellung | Wert      | Befehl zum Abfragen des Werts |
|--|-------------|-----------|-------------------------------|
| Maximale Größe der erstellten Kerndateien            | core        | Unlimited | ulimit -Hc                    |
| Maximale Größe eines Datensegments für einen Prozess | data        | Unlimited | ulimit -Hd                    |
| Maximale Dateigröße                                  | fsize       | Unlimited | ulimit -Hf                    |
| Maximale Anzahl offener Dateien                      | nofile      | 65536     | ulimit -Hn                    |
| Maximale Prozessorzeit in Sekunden                   | cpu         | Unlimited | ulimit -Ht                    |
| Maximale Anzahl Benutzerprozesse                     | nproc       | 16384     | ulimit -Hu                    |

Wenn einer der Benutzergrenzwerte geändert werden muss, führen Sie die Anweisungen in der Dokumentation für Ihr Betriebssystem aus.

## Installation auf Linux-Systemen

Führen Sie die folgenden Schritte aus, um Linux x86\_64 auf dem Serversystem zu installieren.

### Vorbereitende Schritte

Das Betriebssystem wird auf den internen Festplatten installiert. Konfigurieren Sie die internen Festplatten für die Verwendung eines RAID 1-Hardware-Arrays. Wenn Sie beispielsweise ein kleines System konfigurieren, werden die beiden internen 300-GB-Platten in RAID 1 gespiegelt, sodass es aussieht, als würde dem Installationsprogramm des Betriebssystems eine einzelne 300-GB-Platte zur Verfügung stehen.

### Vorgehensweise

1. Installieren Sie Red Hat Enterprise Linux Version 7.1 oder höher gemäß den Anweisungen des Herstellers. Fordern Sie eine bootfähige DVD an, die Red Hat Enterprise Linux Version 7.1 enthält, und starten Sie Ihr System von dieser DVD. Für Installationsoptionen siehe die folgende Anleitung. Wenn ein Element in der folgenden Liste nicht aufgeführt ist, übernehmen Sie die Standardauswahl unverändert.
  - a. Wählen Sie nach dem Starten der DVD im Menü Install or upgrade an existing system (Installation oder Aktualisierung eines bestehenden Systems) aus.
  - b. Wählen Sie in der Eingangsanzeige Test this media & install Red Hat Enterprise Linux 7.1 (Diese Medien überprüfen & Red Hat Enterprise Linux 7.1 installieren) aus.
  - c. Wählen Sie Ihre Sprache und Tastaturbelegung aus.
  - d. Wählen Sie Ihren Standort aus, um die korrekte Zeitzone festzulegen.
  - e. Wählen Sie Software Selection (Softwareauswahl) und in der nächsten Anzeige Server with GUI (Server mit GUI) aus.
  - f. Klicken Sie auf der Installationszusammenfassungsseite auf Installation Destination (Installationsziel) und überprüfen Sie die folgenden Einträge:
    - Die lokale 300-GB-Platte ist als Installationsziel ausgewählt.



- Unter 'Other Storage Options' (Weitere Speicheroptionen) ist Automatically configure partitioning (Partitionierung automatisch konfigurieren) ausgewählt.

Klicken Sie auf Done (Fertig).

- g. Klicken Sie auf Begin Installation (Installation starten). Legen Sie nach dem Start der Installation das Rootkennwort für Ihr Rootbenutzerkonto fest.

Führen Sie nach dem Abschluss der Installation einen Neustart für das System durch und melden Sie sich als Rootbenutzer an. Geben Sie den Befehl `df` aus, um die Basispartitionierung zu überprüfen. Auf einem Testsystem hatte die Erstpartitionierung beispielsweise das folgende Ergebnis zur Folge:

```
[root@tvapp02]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/mapper/rhel-root  50G  3.0G  48G   6% /
devtmpfs        32G   0    32G   0% /dev
tmpfs           32G   92K   32G   1% /dev/shm
tmpfs           32G   8.8M   32G   1% /run
tmpfs           32G   0    32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home 220G   37M  220G   1% /home
/dev/sda1       497M  124M  373M  25% /boot
```

2. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Anweisungen zur Installation des Betriebssystems.

Um optimalen Durchsatz und optimale Zuverlässigkeit zu gewährleisten, sollten Sie das Bonding mehrerer Netzports in Erwägung ziehen. Erstellen Sie dazu eine LACP-Netzverbindung (LACP = Link Aggregation Control Protocol), bei der mehrere untergeordnete Ports in einer einzigen logischen Verbindung aggregiert werden. Die bevorzugte Methode ist die Verwendung des Modus 802.3ad, des Werts 100 für die Einstellung `miimon` und der Angabe `'layer3+4'` für die Einstellung `xmit_hash_policy`.

Einschränkung: Um eine LACP-Netzverbindung verwenden zu können, muss ein Netzswitch vorhanden sein, der LACP unterstützt.

Weitere Anweisungen zur Konfiguration von Bonding-Netzverbindungen mit Red Hat Enterprise Linux Version 7 finden Sie unter [Create a Channel Bonding Interface](#).

3. Öffnen Sie die Datei `/etc/hosts` und führen Sie die folgenden Aktionen aus:

- Aktualisieren Sie die Datei, um die IP-Adresse und den Hostnamen des Servers einzuschließen. Beispiel:

```
192.0.2.7 server.yourdomain.com server
```

- Überprüfen Sie, ob die Datei einen Eintrag für localhost mit der Adresse 127.0.0.1 enthält. Beispiel:

```
127.0.0.1 localhost
```

4. Installieren Sie Komponenten, die für die Serverinstallation erforderlich sind. Führen Sie die folgenden Schritte aus, um ein YUM-Repository (YUM = Yellowdog Updater, Modified) zu erstellen und die vorausgesetzten Pakete zu installieren.

- a. Stellen Sie die DVD für die Installation von Red Hat Enterprise Linux in einem Systemverzeichnis bereit. Um sie beispielsweise im Verzeichnis `/mnt` bereitzustellen, geben Sie den folgenden Befehl aus:

```
mount -t iso9660 -o ro /dev/cdrom /mnt
```

- b. Überprüfen Sie, ob die DVD bereitgestellt wurde, indem Sie den Befehl `mount` ausgeben. Es sollte eine ähnliche Ausgabe wie in dem folgenden Beispiel angezeigt werden:

```
/dev/sr0 on /mnt type iso9660
```

- c. Wechseln Sie in das YUM-Repository-Verzeichnis, indem Sie den folgenden Befehl ausgeben:

```
cd /etc/yum/repos.d
```

Wenn das Verzeichnis `repos.d` nicht vorhanden ist, erstellen Sie es.

- d. Listen Sie den Verzeichnisisinhalt auf:

```
ls rhel-source.repo
```

- e. Benennen Sie die ursprüngliche `repo`-Datei um, indem Sie den Befehl `mv` ausgeben. Beispiel:

```
mv rhel-source.repo rhel-source.repo.orig
```

- f. Erstellen Sie mithilfe eines Texteditors eine neue `repo`-Datei. Um beispielsweise den Editor `vi` zu verwenden, geben Sie den folgenden Befehl aus:

```
vi rhel71_dvd.repo
```

- g. Fügen Sie der neuen `repo`-Datei die folgenden Zeilen hinzu. Der Parameter `baseurl` gibt den Verzeichnismountpunkt an:

```
[rhel71_dvd]
name=DVD Redhat Enterprise Linux 7.1
baseurl=file:///mnt
```

```
enabled=1
gpgcheck=0
```

h. Installieren Sie das vorausgesetzte Paket `ksh.x86_64`, indem Sie den Befehl `yum` ausgeben. Beispiel:

```
yum install ksh.x86_64
```

Ausnahme: Sie müssen die Bibliotheken `compat-libstdc++-33-3.2.3-69.el6.i686` und `libstdc++.i686` für Red Hat Enterprise Linux Version 7.1 nicht installieren.

5. Wenn die Softwareinstallation abgeschlossen ist, können Sie die ursprünglichen YUM-Repository-Werte zurückschreiben, indem Sie die folgenden Schritte ausführen:

a. Heben Sie die Bereitstellung der DVD für die Installation von Red Hat Enterprise Linux auf, indem Sie den folgenden Befehl ausgeben:

```
umount /mnt
```

b. Wechseln Sie in das YUM-Repository-Verzeichnis, indem Sie den folgenden Befehl ausgeben:

```
cd /etc/yum/repos.d
```

c. Benennen Sie die von Ihnen erstellte `repo`-Datei um:

```
mv rhel71_dvd.repo rhel71_dvd.repo.orig
```

d. Benennen Sie die ursprüngliche Datei wieder in den ursprünglichen Namen um:

```
mv rhel-source.repo.orig rhel-source.repo
```

6. Bestimmen Sie, ob Änderungen an Kernelparametern erforderlich sind. Führen Sie die folgenden Schritte aus:

a. Listen Sie mithilfe des Befehls `sysctl -a` die Parameterwerte auf.

b. Analysieren Sie die Ergebnisse anhand der Richtlinien in Tabelle 1, um zu bestimmen, ob Änderungen erforderlich sind.

c. Wenn Änderungen erforderlich sind, definieren Sie die Parameter in der Datei `/etc/sysctl.conf`. Die Dateiänderungen werden angewendet, wenn das System gestartet wird.

Tipp: Passen Sie Kernelparametereinstellungen automatisch an und eliminieren Sie die Notwendigkeit manueller Aktualisierungen dieser Einstellungen. Unter Linux passt die DB2-Datenbanksoftware automatisch die Werte der Kernelparameter für die Interprozesskommunikation (IPC) an und setzt sie auf die bevorzugten Einstellungen. Weitere Informationen zu Kernelparametereinstellungen finden Sie bei Verwendung des Suchbegriffs `Linux-Kernelparameter` im Produktdokumentation zu IBM DB2 Version 11.1.

Tabelle 1. Optimale Einstellungen für Linux-Kernelparameter

| Parameter   | Beschreibung  |
|---|---|
| <code>kernel.shmmni</code>                                    | Die maximale Anzahl Segmente.   |
| <code>kernel.shmmax</code>                                    | Die maximale Größe eines gemeinsam genutzten Speichersegments (Byte).<br><br>Dieser Parameter muss definiert werden, bevor der IBM Spectrum Protect-Server beim Systemstart automatisch gestartet wird. |
| <code>kernel.shmall</code>                                    | Die maximale Zuordnung von Seiten im gemeinsam genutzten Speicher (Seiten).   |
| <code>kernel.sem</code>                                       | (SEMMSL)<br>Die maximale Anzahl Semaphore pro Array.  |
| Für den Parameter <code>kernel.sem</code> gibt es vier Werte. | (SEMMNS)<br>Die maximale Anzahl Semaphore pro System.   |
|   | (SEMOPM)<br>Die maximale Anzahl Operationen pro Semaphoraufruf.   |
|   | (SEMMNI)<br>Die maximale Anzahl Arrays.   |
| <code>kernel.msgmni</code>                                    | Die maximale Anzahl systemweiter Nachrichtenwarteschlangen.   |
| <code>kernel.msgmax</code>                                    | Die maximale Größe von Nachrichten (Byte).  |
| <code>kernel.msgmnb</code>                                    | Die standardmäßige maximale Größe der Warteschlange (Byte).   |

| Parameter                 | Beschreibung   |
|---------------------------|--|
| kernel.randomize_va_space | Mit dem Parameter kernel.randomize_va_space wird die Verwendung von Speicher-ASLR für den Kernel konfiguriert. Inaktivieren Sie ASLR, da ASLR Fehler der DB2-Software zur Folge haben kann. Weitere ausführliche Informationen zu Linux-ASLR und DB2 enthält die Technote 1365583. |
| vm.swappiness             | Der Parameter vm.swappiness definiert, ob der Kernel Anwendungsspeicher aus physischem Arbeitsspeicher (RAM) auslagern kann. Weitere Informationen zu Kernelparametern enthält die Produktinformation zu DB2.  |
| vm.overcommit_memory      | Der Parameter vm.overcommit_memory hat Auswirkungen darauf, wie viel virtueller Speicher gemäß dem Kernel zugeordnet werden kann. Weitere Informationen zu Kernelparametern enthält die Produktinformation zu DB2.   |

7. Öffnen Sie Firewall-Ports für die Kommunikation mit dem Server. Führen Sie die folgenden Schritte aus:

a. Legen Sie die von der Netzchnittstelle verwendete Zone fest. Die Zone ist standardmäßig 'public'.

Geben Sie den folgenden Befehl aus:

```
# firewall-cmd --get-active-zones
public
  interfaces: ens4f0
```

b. Um die Standardportadresse für die Kommunikation mit dem Server zu verwenden, öffnen Sie TCP/IP-Port 1500 in der Linux-Firewall.

Geben Sie den folgenden Befehl aus:

```
firewall-cmd --zone=public --add-port=1500/tcp --permanent
```

Wenn ein anderer Wert als der Standardwert verwendet werden soll, können Sie eine Zahl zwischen 1024 und 32767 angeben. Wenn ein anderer Port als der Standardport geöffnet wird, müssen Sie diesen Port bei der Ausführung des Konfigurationsscripts angeben.

c. Wenn Sie planen, dieses System als einen Hub zu verwenden, öffnen Sie Port 11090, den Standardport für die sichere Kommunikation (HTTPS).

Geben Sie den folgenden Befehl aus:

```
firewall-cmd --zone=public --add-port=11090/tcp --permanent
```

d. Laden Sie die Firewalldefinitionen erneut, damit die Änderungen wirksam werden.

Geben Sie den folgenden Befehl aus:

```
firewall-cmd --reload
```

8. Überprüfen Sie, ob Benutzerprozessressourcengrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, gemäß den Richtlinien in Tabelle 2 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

Tabelle 2. Benutzerbegrenzwerte (ulimit-Werte)

| Typ des Benutzerbegrenzwerts                         | Einstellung | Wert      | Befehl zum Abfragen des Werts |
|--|-------------|-----------|-------------------------------|
| Maximale Größe der erstellten Kerndateien            | core        | Unlimited | ulimit -Hc                    |
| Maximale Größe eines Datensegments für einen Prozess | data        | Unlimited | ulimit -Hd                    |
| Maximale Dateigröße                                  | fsize       | Unlimited | ulimit -Hf                    |
| Maximale Anzahl offener Dateien                      | nofile      | 65536     | ulimit -Hn                    |
| Maximale Prozessorzeit in Sekunden                   | cpu         | Unlimited | ulimit -Ht                    |
| Maximale Anzahl Benutzerprozesse                     | nproc       | 16384     | ulimit -Hu                    |

Wenn einer der Benutzergrenzwerte geändert werden muss, führen Sie die Anweisungen in der Dokumentation für Ihr Betriebssystem aus.

## Installation auf Windows-Systemen

---

Installieren Sie Microsoft Windows Server 2012 Standard Edition auf dem Serversystem und bereiten Sie das System für die Installation und Konfiguration des IBM Spectrum Protect-Servers vor.

### Vorgehensweise

---

1. Installieren Sie Windows Server 2016 Standard Edition gemäß den Anweisungen des Herstellers.
2. Ändern Sie die Windows-Kontensteuerungsrichtlinien, indem Sie die folgenden Schritte ausführen.
  - a. Öffnen Sie den Editor für lokale Sicherheitsrichtlinien, indem Sie secpol.msc ausführen.
  - b. Klicken Sie auf Lokale Richtlinien > Sicherheitsoptionen und stellen Sie sicher, dass die folgenden Benutzerkontensteuerungsrichtlinien inaktiviert sind:
    - Administratorbestätigungsmodus für das integrierte Administratorkonto
    - Alle Administratoren im Administratorbestätigungsmodus ausführen
3. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Installationsanweisungen für das Betriebssystem.
4. Wenden Sie Windows-Updates an und aktivieren Sie Zusatzfunktionen (optionale Features), indem Sie die folgenden Schritte ausführen:
  - a. Wenden Sie die neuesten Windows Server 2016-Updates an.
  - b. Installieren und aktivieren Sie das Windows 2012 R2-Feature Microsoft .NET Framework 3.5 über den Windows Server-Manager.
  - c. Aktualisieren Sie, falls erforderlich, die FC- und Ethernet-HBA-Einheitentreiber mit neueren Versionen.
  - d. Installieren Sie den für das verwendete Plattensystem geeigneten Multipath I/O-Treiber.

5. Öffnen Sie den TCP/IP-Standardport (1500) für die Kommunikation mit dem IBM Spectrum Protect-Server. Geben Sie beispielsweise den folgenden Befehl aus:

```
netsh advfirewall firewall add rule name="Sicherungsserver-Port 1500"  
dir=in action=allow protocol=TCP localport=1500
```

6. Öffnen Sie auf dem Operations Center-Hub-Server den Standardport für die sichere Kommunikation (HTTPS) mit dem Operations Center. Die Portnummer ist 11090. Geben Sie beispielsweise den folgenden Befehl aus:

```
netsh advfirewall firewall add rule name="Operations Center-Port 11090"  
dir=in action=allow protocol=TCP localport=11090
```

## Multipath I/O konfigurieren

---

Sie können Multipathing für Plattenspeicher aktivieren und konfigurieren. Die mit Ihrer Hardware zur Verfügung gestellte Dokumentation enthält ausführliche Anweisungen.

- AIX-Systeme
- Linux-Systeme
- Windows-Systeme

## AIX-Systeme

---

### Vorgehensweise

---

1. Bestimmen Sie die Fibre Channel-Portadresse, die für die Hostdefinition auf dem Plattensubsystem verwendet werden muss. Geben Sie den Befehl lscfg für jeden Port aus.

- Geben Sie auf kleinen und mittelgroßen Systemen die folgenden Befehle aus:

```
lscfg -vps -l fcs0 | grep "Netzadresse"  
lscfg -vps -l fcs1 | grep "Netzadresse"
```

- Geben Sie auf großen Systemen die folgenden Befehle aus:

```
lscfg -vps -l fcs0 | grep "Netzadresse"  
lscfg -vps -l fcs1 | grep "Netzadresse"  
lscfg -vps -l fcs2 | grep "Netzadresse"  
lscfg -vps -l fcs3 | grep "Netzadresse"
```

2. Stellen Sie sicher, dass die folgenden AIX-Dateigruppen installiert sind:
  - devices.common.IBM.mpio.rte

- o devices.fcp.disk.array.rte
- o devices.fcp.disk.rte

3. Geben Sie den Befehl `cfgmgr` aus, damit AIX die Hardware erneut überprüft und verfügbare Platten erkennt. Beispiel:

```
cfgmgr
```

4. Um die verfügbaren Platten aufzulisten, geben Sie den folgenden Befehl aus:

```
lsdev -Ccdisk
```

Es sollte eine ähnliche Ausgabe wie die folgende angezeigt werden:

```
hdisk0 Available 00-00-00 SAS Disk Drive
hdisk1 Available 00-00-00 SAS Disk Drive
hdisk2 Available 01-00-00 SAS Disk Drive
hdisk3 Available 01-00-00 SAS Disk Drive
hdisk4 Available 06-01-02 MPIO IBM 2076 FC Disk
hdisk5 Available 07-01-02 MPIO IBM 2076 FC Disk
...
```

5. Verwenden Sie die Ausgabe des Befehls `lsdev`, um die Einheiten-IDs für jede Platteneinheit zu ermitteln und aufzulisten.

Beispielsweise könnte eine Einheiten-ID `hdisk4` lauten. Sichern Sie die Liste der Einheiten-IDs für die Verwendung bei der Erstellung von Dateisystemen für den IBM Spectrum Protect-Server.

6. Korrelieren Sie die SCSI-Einheiten-IDs zu bestimmten Platten-LUNs aus dem Plattensystem, indem Sie detaillierte Informationen zu allen physischen Datenträgern im System auflisten. Geben Sie den folgenden Befehl aus:

```
lspv -u
```

Auf einem IBM® Storwize-System werden beispielsweise die folgenden Informationen für jede Einheit angezeigt:

```
hdisk4 00f8cf083fd97327 None active
3321360050763008101057800000000003004214503IBMfcp
```

In dem Beispiel ist `6005076300810105780000000000030` die UID für den Datenträger, die von der Storwize-Managementsschnittstelle zurückgemeldet wurde.

Um die Plattengröße in Megabyte zu überprüfen und den Wert mit dem für das System aufgelisteten Wert zu vergleichen, geben Sie den folgenden Befehl aus:

```
bootinfo -s hdisk4
```

## Linux-Systeme

---

### Vorgehensweise

---

1. Editieren Sie die Datei `/etc/multipath.conf`, um Multipathing für Linux-Hosts zu aktivieren. Wenn die Datei `multipath.conf` nicht vorhanden ist, können Sie die Datei erstellen, indem Sie den folgenden Befehl ausgeben:

```
mpathconf --enable
```

Die folgenden Parameter wurden in `multipath.conf` zu Testzwecken auf einem IBM Storwize-System festgelegt:

```
defaults {
    user_friendly_names no
}

devices {
    device {
        vendor "IBM "
        product "2145"
        path_grouping_policy group_by_prio
        user_friendly_names no
        path_selector "round-robin 0"
        prio "alua"
        path_checker "tur"
        failback "immediate"
        no_path_retry 5
        rr_weight uniform
        rr_min_io_rq "1"
        dev_loss_tmo 120
    }
}
```

- Definieren Sie die Multipath-Option so, dass Multipath zusammen mit dem System gestartet wird. Geben Sie die folgenden Befehle aus:

```
systemctl enable multipathd.service
systemctl start multipathd.service
```

- Um sicherzustellen, dass Platten für das Betriebssystem sichtbar sind und durch Multipath verwaltet werden, geben Sie den folgenden Befehl aus:

```
multipath -l
```

- Stellen Sie sicher, dass jede Einheit aufgelistet ist und über so viele Pfade wie erwartet verfügt. Anhand der Größe und Einheiten-ID können Sie die aufgelisteten Platten identifizieren.

Beispielsweise zeigt die folgende Ausgabe, dass einer 2-TB-Platte zwei Pfadgruppen und vier aktive Pfade zugeordnet sind. Die Größe von 2 TB bestätigt, dass die Platte einem Pooldateisystem entspricht. Suchen Sie anhand eines Teils der langen Einheiten-ID-Nummer (in diesem Beispiel 12) in der Managementschnittstelle des Plattensystems nach dem Datenträger.

```
[root@tapsrv01 code]# multipath -l
36005076802810c509800000000000012 dm-43 IBM,2145
size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|+- policy='round-robin 0' prio=0 status=active
| |- 2:0:1:18 sdcw 70:64 active undef running
| `-- 4:0:0:18 sdgb 131:112 active undef running
`+- policy='round-robin 0' prio=0 status=enabled
| - 1:0:1:18 sdat 66:208 active undef running
| - 3:0:0:18 sddy 128:0 active undef running
```

- Korrigieren Sie, falls erforderlich, Platten-LUN/Host-Zuordnungen und erzwingen Sie eine erneute Busüberprüfung. Beispiel:

```
echo "-- --" > /sys/class/scsi_host/host0/scan
echo "-- --" > /sys/class/scsi_host/host1/scan
echo "-- --" > /sys/class/scsi_host/host2/scan
```

Sie können für eine erneute Überprüfung der Platten-LUN/Host-Zuordnungen auch das System erneut starten.

- Stellen Sie sicher, dass Platten jetzt für Multipath I/O verfügbar sind, indem Sie den Befehl `multipath -l` erneut ausgeben.
- Verwenden Sie die Multipath-Ausgabe, um die Einheiten-IDs für jede Platteneinheit zu ermitteln und aufzulisten.

Beispielsweise ist die Einheiten-ID für Ihre 2-TB-Platte 36005076802810c509800000000000012.

Sichern Sie die Liste der Einheiten-IDs für die Verwendung im nächsten Schritt.

## Windows-Systeme

### Vorgehensweise

- Stellen Sie sicher, dass Multipath I/O installiert ist. Installieren Sie, falls erforderlich, weitere anbieterspezifische Multipath-Treiber.
- Um sicherzustellen, dass Platten für das Betriebssystem sichtbar sind und durch Multipath I/O verwaltet werden, geben Sie den folgenden Befehl aus:

```
c:\Programme\IBM\SDDDSM\data\path.exe query device
```

- Überprüfen Sie die Multipath-Ausgabe und stellen Sie sicher, dass jede Einheit aufgelistet ist und über so viele Pfade wie erwartet verfügt. Anhand der Größe und Einheiten-ID können Sie die aufgelisteten Platten identifizieren.

Beispielsweise können Sie anhand eines Teils der langen Einheiten-ID-Nummer (in diesem Beispiel 34) in der Managementschnittstelle des Plattensystems nach dem Datenträger suchen. Die Größe von 2 TB bestätigt, dass die Platte einem Speicherpooldateisystem entspricht.

```
DEV#:      4  DEVICE NAME: Disk5 Part0    TYPE: 2145    POLICY: OPTIMIZED
SERIAL:    60050763008101057800000000000034    LUN SIZE: 2.0TB
=====
Path#      Adapter/Hard Disk      State  Mode   Select  Errors
  0        Scsi Port2 Bus0/Disk5 Part0  OPEN  NORMAL  0        0
  1        Scsi Port2 Bus0/Disk5 Part0  OPEN  NORMAL  27176    0
  2        Scsi Port3 Bus0/Disk5 Part0  OPEN  NORMAL  28494    0
  3        Scsi Port3 Bus0/Disk5 Part0  OPEN  NORMAL  0        0
```

- Erstellen Sie unter Verwendung der in der Multipath-Ausgabe im vorherigen Schritt zurückgegebenen Seriennummern eine Liste der Platteneinheiten-IDs.

Beispielsweise ist die Einheiten-ID für Ihre 2-TB-Platte 60050763008101057800000000000034.

Sichern Sie die Liste der Einheiten-IDs für die Verwendung im nächsten Schritt.

- Um neue Platten online zu schalten und das Lesezugriffsattribut zu löschen, führen Sie diskpart.exe mit den folgenden Befehlen aus. Wiederholen Sie diesen Schritt für jede der Platten:

```
diskpart
select Disk 1
online disk
attribute disk clear readonly
select Disk 2
online disk
attribute disk clear readonly
< ... >
select Disk 49
online disk
attribute disk clear readonly
exit
```

## Benutzer-ID für den Server erstellen

---

Erstellen Sie die Benutzer-ID, die Eigner der IBM Spectrum Protect-Serverinstanz ist. Sie geben diese Benutzer-ID an, wenn Sie die Serverinstanz im Rahmen der Erstkonfiguration des Servers erstellen.

### Informationen zu diesem Vorgang

---



Sie können nur Kleinbuchstaben (a-z), Ziffern (0-9) und das Unterstrichungszeichen (\_) für die Benutzer-ID angeben. Die Benutzer-ID und der Gruppenname müssen den folgenden Regeln entsprechen:

- Die Länge darf 8 Zeichen nicht überschreiten.
- Die Benutzer-ID und der Gruppenname dürfen nicht mit *ibm*, *sql*, *sys* oder einer Ziffer beginnen.
- Die Benutzer-ID und der Gruppenname dürfen nicht *user*, *admin*, *guest*, *public*, *local* oder ein in SQL reserviertes Wortes sein.

### Vorgehensweise

---

- Erstellen Sie mithilfe von Betriebssystembefehlen eine Benutzer-ID.

-   Erstellen Sie eine Gruppe und eine Benutzer-ID im Ausgangsverzeichnis des Benutzers, der Eigner der Serverinstanz ist.

Um beispielsweise die Benutzer-ID *tsminst1* in der Gruppe *tsmsrvrs* mit dem Kennwort *tsminst1* zu erstellen, geben Sie die folgenden Befehle mit einer ID für einen Benutzer mit Verwaltungsaufgaben aus:


#### AIX-Betriebssysteme

```
mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

#### Linux-Betriebssysteme

```
groupadd tsmsrvrs
useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
passwd tsminst1
```

Melden Sie sich von Ihrem System ab und anschließend wieder an. Wechseln Sie zu dem von Ihnen erstellten Benutzerkonto. Verwenden Sie ein interaktives Anmeldeprogramm, wie beispielsweise Telnet, damit Sie zur Eingabe des Kennworts aufgefordert werden und es, falls erforderlich, ändern können.

-  Erstellen Sie eine Benutzer-ID und fügen Sie dann die neue ID der Gruppe 'Administratoren' hinzu. Um beispielsweise die Benutzer-ID *tsminst1* zu erstellen, geben Sie den folgenden Befehl aus:

```
net user tsminst1 * /add
```

Fügen Sie, nachdem Sie für den neuen Benutzer ein Kennwort erstellt und bestätigt haben, die Benutzer-ID der Gruppe 'Administratoren' hinzu, indem Sie die folgenden Befehle ausgeben:

```
net localgroup Administratoren tsminst1 /add
net localgroup DB2ADMNS tsminst1 /add
```

- Melden Sie die neue Benutzer-ID ab.

# Dateisysteme für den Server vorbereiten

Sie müssen die Dateisystemkonfiguration ausführen, damit der Plattenspeicher vom Server verwendet werden kann.

- Dateisysteme auf AIX-Systemen vorbereiten  
Sie müssen Datenträgergruppen, logische Datenträger und Dateisysteme für den Server mithilfe von AIX Logical Volume Manager erstellen.
- Dateisysteme auf Linux-Systemen vorbereiten  
Sie müssen ext4- oder xfs-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.
- Dateisysteme auf Windows-Systemen vorbereiten  
Sie müssen NTFS-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

## Dateisysteme auf AIX-Systemen vorbereiten

Sie müssen Datenträgergruppen, logische Datenträger und Dateisysteme für den Server mithilfe von AIX Logical Volume Manager erstellen.

### Vorgehensweise

1. Erhöhen Sie die Warteschlangenlänge und die maximale Übertragungsgröße für alle verfügbaren *hdiskX*-Platten. Geben Sie für jede Platte die folgenden Befehle aus:

```
chdev -l hdisk4 -a max_transfer=0x100000
chdev -l hdisk4 -a queue_depth=32
chdev -l hdisk4 -a reserve_policy=no_reserve
chdev -l hdisk4 -a algorithm=round_robin
```

Sie dürfen diese Befehle nicht für interne Betriebssystemplatten, beispielsweise *hdisk0*, ausführen.

2. Erstellen Sie Datenträgergruppen für die IBM Spectrum Protect-Datenbank, die aktive Protokolldatei, das Archivprotokoll, die Datenbanksicherung und den Speicherpool. Geben Sie den Befehl *mkvg* unter Angabe der Einheiten-IDs für die entsprechenden zuvor ermittelten Platten aus.

Wenn beispielsweise die Einheitennamen *hdisk4*, *hdisk5* und *hdisk6* Datenbankplatten entsprechen, schließen Sie diese in die Datenbankdatenträgergruppe ein.

Systemgröße: Die folgenden Befehle basieren auf einer Konfiguration für ein mittelgroßes System. Für kleine und große Systeme müssen Sie die Syntax wie erforderlich anpassen.

```
mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
mkvg -S -y tsmactlog hdisk5
mkvg -S -y tsmarchlog hdisk6
mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
```

3. Bestimmen Sie die Namen der physischen Datenträger und die Anzahl freier physischer Partitionen, die beim Erstellen logischer Datenträger verwendet werden sollen. Geben Sie den Befehl *lsvg* für jede Datenträgergruppe aus, die Sie im vorherigen Schritt erstellt haben.

Beispiel:

```
lsvg -p tsmdb
```

Die Ausgabe sieht ähnlich wie die folgende aus. Die Spalte *FREE PPs* gibt die freien physischen Partitionen an:

```
tsmdb:
PV_NAME  PV STATE  TOTAL PPs  FREE PPs  FREE DISTRIBUTION
hdisk4   active    1631       1631      327..326..326..326..326
hdisk5   active    1631       1631      327..326..326..326..326
hdisk6   active    1631       1631      327..326..326..326..326
```

4. Erstellen Sie mit dem Befehl *mklv* logische Datenträger in jeder Datenträgergruppe. Die Datenträgergröße, die Datenträgergruppe und die Einheitennamen sind, abhängig von der Größe Ihres Systems und Variationen in Ihrer Plattenkonfiguration, unterschiedlich.

Um beispielsweise die Datenträger für die IBM Spectrum Protect-Datenbank auf einem mittelgroßen System zu erstellen, geben Sie die folgenden Befehle aus:

```
mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
```



5. Formatieren Sie Dateisysteme auf jedem logischen Datenträger mit dem Befehl `crfs`.

Um beispielsweise die Dateisysteme für die Datenbank auf einem mittelgroßen System zu formatieren, geben Sie die folgenden Befehle aus:

```
crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
```

6. Führen Sie für alle neu erstellten Dateisysteme einen Mount durch, indem Sie den folgenden Befehl eingeben:

```
mount -a
```

7. Listen Sie alle Dateisysteme auf, indem Sie den Befehl `df` ausgeben. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Überprüfen Sie außerdem den verfügbaren Speicherbereich. Das folgende Beispiel der Befehlsausgabe zeigt, dass der Umfang des belegten Speicherbereichs normalerweise 1 % beträgt:

```
tapsrv07> df -g /tsminst1/*
Filesystem      GB blocks   Free    %Used   Iused   %Iused   Mounted on
/dev/tsmact00   195.12     194.59    1%        4        1%       /tsminst1/TSMalog
```

8. Überprüfen Sie, ob die in Benutzer-ID für den Server erstellen erstellte Benutzer-ID Schreib-/Lesezugriff auf die Verzeichnisse für den Server hat.

## Dateisysteme auf Linux-Systemen vorbereiten

---

Sie müssen `ext4`- oder `xfs`-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

### Vorgehensweise

---

1. Verwenden Sie die zuvor generierte Liste der Einheiten-IDs und geben Sie den Befehl `mkfs` aus, um für jede LUN-Speichereinheit ein Dateisystem zu erstellen und zu formatieren. Geben Sie die Einheiten-ID im Befehl an. Siehe die folgenden Beispiele. Formatieren Sie für die Datenbank `ext4`-Dateisysteme:

```
mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c50980000000000012
```

Formatieren Sie für Speicherpool-LUNs `xfs`-Dateisysteme:

```
mkfs -t xfs /dev/mapper/3600507630081010578000000000002c3
```

Abhängig davon, wie viele verschiedene Einheiten vorhanden sind, können Sie den Befehl `mkfs` bis zu 50 Mal ausgeben.

2. Erstellen Sie Mountpunktverzeichnisse für Dateisysteme.

Geben Sie den Befehl `mkdir` für jedes Verzeichnis aus, das erstellt werden muss. Verwenden Sie die in den Arbeitsblättern zur Planung verwendeten Verzeichniswerte.

Um beispielsweise das Serverinstanzverzeichnis unter Verwendung des Standardwerts zu erstellen, geben Sie den folgenden Befehl aus:

```
mkdir /tsminst1
```

Wiederholen Sie den Befehl `mkdir` für jedes Dateisystem.

3. Fügen Sie in der Datei `/etc/fstab` für jedes Dateisystem einen Eintrag hinzu, damit für die Dateisysteme beim Serverstart automatisch ein Mount durchgeführt wird.

Beispiel:

```
/dev/mapper/36005076802810c50980000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
```

4. Führen Sie für die Dateisysteme, die der Datei `/etc/fstab` hinzugefügt wurden, einen Mount durch, indem Sie den Befehl `mount -a` ausgeben.
5. Listen Sie alle Dateisysteme auf, indem Sie den Befehl `df` ausgeben. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Überprüfen Sie außerdem den verfügbaren Speicherbereich. Das folgende Beispiel für ein IBM® Storwize-System zeigt, dass der Umfang des belegten Speicherbereichs normalerweise 1 % beträgt:

```
[root@tapsrv04 ~]# df -h /tsminst1/*
Filesystem      Size  Used Avail Use% Mounted on
```

- Überprüfen Sie, ob die in Benutzer-ID für den Server erstellen erstellte Benutzer-ID Schreib-/Lesezugriff auf die Verzeichnisse für den IBM Spectrum Protect-Server hat.

## Dateisysteme auf Windows-Systemen vorbereiten

---

Sie müssen NTFS-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

### Vorgehensweise

---

- Erstellen Sie Mountpunktverzeichnisse für Dateisysteme.  
Geben Sie den Befehl `md` für jedes Verzeichnis aus, das erstellt werden muss. Verwenden Sie die in den Arbeitsblättern zur Planung verwendeten Verzeichniswerte. Um beispielsweise das Serverinstanzverzeichnis unter Verwendung des Standardwerts zu erstellen, geben Sie den folgenden Befehl aus:

```
md c:\tsminst1
```

Wiederholen Sie den Befehl `md` für jedes Dateisystem.

- Erstellen Sie für jede Platten-LUN, die einem Verzeichnis unter dem Serverinstanzverzeichnis zugeordnet ist, unter Verwendung des Windows-Datenträgermanagers (Volume-Manager) einen Datenträger.

Rufen Sie **Server-Manager > Datei- und Speicherdienste** auf und führen Sie die folgenden Schritte für jede Platte aus, die der im vorherigen Schritt erstellten LUN-Zuordnung entspricht:

- Schalten Sie die Platte online.
- Initialisieren Sie die Platte mit dem GPT-Basistyp, dem Standardwert.
- Erstellen Sie einen einfachen Datenträger, der den gesamten Speicherbereich auf der Platte belegt. Formatieren Sie das Dateisystem mit NTFS und ordnen Sie einen Kennsatz zu, der den Zweck des Datenträgers angibt, wie beispielsweise `TSMfile00`. Ordnen Sie den neuen Datenträger keinem Laufwerksbuchstaben zu. Ordnen Sie den Datenträger stattdessen einem Verzeichnis unter dem Instanzverzeichnis zu, wie beispielsweise `C:\tsminst1\TSMfile00`.  
Tipp: Legen Sie den Datenträgerkennsatz und die Bezeichnungen für Verzeichniszuordnungen auf der Basis der Größe der aufgelisteten Platte fest.

- Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Listen Sie alle Dateisysteme auf, indem Sie den Befehl `mountvol` ausgeben; überprüfen Sie dann die Ausgabe. Beispiel:

```
\\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\  
C:\tsminst1\TSMdbspace00\
```

- Starten Sie nach dem Abschluss der Plattenkonfiguration das System erneut.

### Nächste Schritte

---

Mithilfe von Windows Explorer können Sie den Umfang des freien Speicherbereichs für jeden Datenträger prüfen.

## Server und das Operations Center installieren

---

Verwenden Sie den grafisch orientierten Assistenten von IBM® Installation Manager, um die Komponenten zu installieren.

- Installation auf AIX- und Linux-Systemen  
Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.
- Installation auf Windows-Systemen  
Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.

## Installation auf AIX- und Linux-Systemen

---

Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.


### Vorbereitende Schritte

---

Überprüfen Sie, ob das Betriebssystem auf die erforderliche Sprache gesetzt ist. Standardmäßig entspricht die Sprache für das Betriebssystem der Sprache für den Installationsassistenten.

### Vorgehensweise

---

1.  Überprüfen Sie, ob die erforderlichen RPM-Dateien auf Ihrem System installiert sind.

Ausführliche Informationen befinden sich in Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren.

2. Überprüfen Sie vor dem Herunterladen des Installationspakets, ob genügend Speicherbereich zum Speichern der Installationsdateien vorhanden ist, wenn die Dateien aus dem Produktpaket extrahiert werden. Informationen zum Speicherbedarf enthält das Downloaddokument unter Technote 4042992.
3. Rufen Sie Passport Advantage auf und laden Sie die Paketdatei in ein leeres Verzeichnis Ihrer Wahl herunter.
4. Stellen Sie sicher, dass für das Paket die Berechtigung zur Ausführung festgelegt ist. Ändern Sie, falls erforderlich, die Dateiberechtigungen, indem Sie den folgenden Befehl ausgeben:

```
chmod a+x Paketname.bin
```

5. Extrahieren Sie das Paket, indem Sie den folgenden Befehl ausgeben:

```
./Paketname.bin
```

Dabei ist *Paketname* der Name der Downloaddatei.

6.  Stellen Sie sicher, dass der folgende Befehl aktiviert ist, damit die Assistenten korrekt ausgeführt werden:

```
lsuser
```

Standardmäßig ist der Befehl aktiviert.

7. Wechseln Sie in das Verzeichnis, in das die ausführbare Datei gestellt wurde.
8. Starten Sie den Installationsassistenten, indem Sie den folgenden Befehl ausgeben:

```
./install.sh
```

Wenn Sie die zu installierenden Pakete auswählen, wählen Sie sowohl den Server als auch das Operations Center aus.

## Nächste Schritte



---

- Wenn während des Installationsprozesses Fehler auftreten, werden die Fehler in Protokolldateien aufgezeichnet, die im Protokollverzeichnis von IBM Installation Manager gespeichert sind.

Um Installationsprotokolldateien in Installation Manager anzuzeigen, klicken Sie auf Datei > Protokoll anzeigen. Um diese Protokolldateien in Installation Manager zu erfassen, klicken Sie auf Hilfe > Daten zur Fehleranalyse exportieren.

- Rufen Sie nach der Installation des Servers, aber vor der Anpassung des Servers für Ihre Verwendung die IBM Spectrum Protect-Unterstützungssite auf. Klicken Sie auf Support und Downloads und wenden Sie alle zutreffenden Fixes an.
- Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren  
RPM-Dateien sind für den grafisch orientierten Assistenten von IBM Installation Manager erforderlich.

### Zugehörige Tasks:

-  Andere Methoden zum Installieren von IBM Spectrum Protect-Komponenten (AIX)
-  Andere Methoden zum Installieren von IBM Spectrum Protect-Komponenten (Linux)

## Installation auf Windows-Systemen

---

Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.

## Vorbereitende Schritte

---

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Überprüfen Sie, ob das Betriebssystem auf die erforderliche Sprache gesetzt ist. Standardmäßig entspricht die Sprache für das Betriebssystem der Sprache für den Installationsassistenten.
- Stellen Sie sicher, dass die Benutzer-ID, die während der Installation verwendet werden soll, für einen Benutzer mit der Berechtigung eines lokalen Administrators gilt.

## Vorgehensweise

---

1. Überprüfen Sie vor dem Herunterladen des Installationspakets, ob genügend Speicherbereich zum Speichern der Installationsdateien vorhanden ist, wenn die Dateien aus dem Produktpaket extrahiert werden. Informationen zum Speicherbedarf enthält das Downloaddokument unter Technote 4042993.
2. Rufen Sie Passport Advantage auf und laden Sie die Paketdatei in ein leeres Verzeichnis Ihrer Wahl herunter.
3. Wechseln Sie in das Verzeichnis, in das die ausführbare Datei gestellt wurde.

4. Doppelklicken Sie auf die ausführbare Datei, um die Datei in das aktuelle Verzeichnis zu extrahieren.
5. Starten Sie in dem Verzeichnis, in das die Installationsdateien extrahiert wurden, den Installationsassistenten, indem Sie auf die Datei install.bat doppelklicken. Wenn Sie die zu installierenden Pakete auswählen, wählen Sie sowohl den Server als auch das Operations Center aus.

## Nächste Schritte


---

- Wenn während des Installationsprozesses Fehler auftreten, werden die Fehler in Protokolldateien aufgezeichnet, die im Protokollverzeichnis von IBM® Installation Manager gespeichert sind.

Um Installationsprotokolldateien in Installation Manager anzuzeigen, klicken Sie auf Datei > Protokoll anzeigen. Um diese Protokolldateien in Installation Manager zu erfassen, klicken Sie auf Hilfe > Daten zur Fehleranalyse exportieren.

- Rufen Sie nach der Installation des Servers, aber vor der Anpassung des Servers für Ihre Verwendung die IBM Spectrum Protect-Unterstützungssite auf. Klicken Sie auf Support und Downloads und wenden Sie alle zutreffenden Fixes an.

### Zugehörige Tasks:

 Andere Methoden zum Installieren von IBM Spectrum Protect-Komponenten

## Server und das Operations Center konfigurieren

---

Nachdem Sie die Komponenten installiert haben, führen Sie die Konfiguration für den IBM Spectrum Protect-Server und das Operations Center aus.

- Serverinstanz konfigurieren  
Verwenden Sie den IBM Spectrum Protect-Assistenten für die Serverinstanzkonfiguration, um die Erstkonfiguration für den Server auszuführen.
- Client für Sichern/Archivieren installieren  
Installieren Sie als Best Practice den IBM Spectrum Protect-Client für Sichern/Archivieren auf dem Serversystem, sodass der Verwaltungsbefehlszeilenclient und der Scheduler verfügbar sind.
- Optionen für den Server festlegen  
Überprüfen Sie die Serveroptionsdatei, die mit dem IBM Spectrum Protect-Server installiert wird, um sicherzustellen, dass die korrekten Werte für Ihr System festgelegt sind.
- Sichere Kommunikation mit Transport Layer Security konfigurieren  
Um Daten zu verschlüsseln und die sichere Kommunikation in Ihrer Umgebung zu ermöglichen, ist Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) auf dem IBM Spectrum Protect-Server und dem Client für Sichern/Archivieren aktiviert. Kommunikationsanforderungen zwischen dem Server und dem Client werden mithilfe eines SSL-Zertifikats geprüft.
- Operations Center konfigurieren  
Führen Sie nach der Installation des Operations Center die folgenden Konfigurationsschritte aus, um mit der Verwaltung Ihrer Speicherumgebung zu beginnen.
- Produktlizenz registrieren  
Verwenden Sie zum Registrieren Ihrer Lizenz für das Produkt IBM Spectrum Protect den Befehl REGISTER LICENSE.
- Datenduplizierung konfigurieren  
Erstellen Sie einen Verzeichniscontainerspeicherpool und mindestens ein Verzeichnis für die Verwendung der Inline-Datenduplizierung.
- Datenaufbewahrungsregeln für Ihr Unternehmen definieren  
Nachdem Sie einen Verzeichniscontainerspeicherpool für die Datenduplizierung erstellt haben, aktualisieren Sie die Serverstandardmaßnahme für die Verwendung des neuen Speicherpools. Die Seite Services im Operations Center wird vom Assistenten Speicherpool hinzufügen zur Ausführung dieser Task geöffnet.
- Zeitpläne für Serververwaltungsaktivitäten definieren  
Erstellen Sie Zeitpläne für jede Serververwaltungsoperation, indem Sie den Befehl DEFINE SCHEDULE im Command Builder des Operations Center verwenden.
- Clientzeitpläne definieren  
Erstellen Sie mithilfe des Operations Center Zeitpläne für Clientoperationen.

## Serverinstanz konfigurieren

---

Verwenden Sie den IBM Spectrum Protect-Assistenten für die Serverinstanzkonfiguration, um die Erstkonfiguration für den Server auszuführen.


## Vorbereitende Schritte

---

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

 AIX-Betriebssysteme  Linux-Betriebssysteme

- Auf dem System, auf dem IBM Spectrum Protect installiert wurde, muss der X Window System-Client vorhanden sein. Außerdem muss ein X Window System-Server auf Ihrem Desktop ausgeführt werden.
- Für das System muss das Secure Shell-Protokoll (SSH-Protokoll) aktiviert sein. Stellen Sie sicher, dass der Port auf den Standardwert 22 gesetzt ist und dass der Port nicht durch eine Firewall blockiert wird. Sie müssen die Kennwortauthentifizierung in der Datei `sshd_config` im Verzeichnis `/etc/ssh/` aktivieren. Stellen Sie außerdem sicher, dass der SSH-Dämonservice über die Zugriffsberechtigungen verfügt, um mithilfe des Werts `localhost` eine Verbindung zum System herstellen zu können.
- Sie müssen sich mit der Benutzer-ID, die Sie für die Serverinstanz erstellt hatten, unter Verwendung des SSH-Protokolls bei IBM Spectrum Protect anmelden können. Wenn Sie den Assistenten verwenden, müssen Sie diese Benutzer-ID und das Kennwort für den Zugriff auf dieses System angeben.
- Wenn Sie in den vorhergehenden Schritten Änderungen an den Einstellungen vorgenommen haben, starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.

 Windows-Betriebssysteme Überprüfen Sie, ob der Remoteregistrierungsdienst gestartet wurde, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie auf Start > Verwaltung > Dienste. Wählen Sie im Fenster Dienste Remoteregistrierung aus. Wurde der Dienst nicht gestartet, klicken Sie auf Starten.
2. Stellen Sie sicher, dass die Ports 137, 139 und 445 nicht durch eine Firewall blockiert sind:
  - a. Klicken Sie auf Start > Systemsteuerung > Windows-Firewall.
  - b. Wählen Sie Erweiterte Einstellungen aus.
  - c. Wählen Sie Eingehende Regeln aus.
  - d. Wählen Sie Neue Regel aus.
  - e. Erstellen Sie eine Portregel für die TCP-Ports 137, 139 und 445, um Verbindungen für Domänennetze und private Netze zu ermöglichen.
3. Konfigurieren Sie die Benutzerkontensteuerung, indem Sie auf die Optionen für die lokale Sicherheitsrichtlinie zugreifen und die folgenden Schritte ausführen.
  - a. Klicken Sie auf Start > Verwaltung > Lokale Sicherheitsrichtlinie. Erweitern Sie Lokale Richtlinien > Sicherheitsoptionen.
  - b. Falls noch nicht bereits aktiviert, aktivieren Sie das integrierte Administratorkonto, indem Sie Konten: Administratorkontostatus > Aktivieren > OK auswählen.
  - c. Falls noch nicht bereits inaktiviert, inaktivieren Sie die Benutzerkontensteuerung für alle Windows-Administratoren, indem Sie Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen > Inaktivieren > OK auswählen.
  - d. Falls noch nicht bereits inaktiviert, inaktivieren Sie die Benutzerkontensteuerung für das integrierte Administratorkonto, indem Sie Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto > Inaktivieren > OK auswählen.
4. Wenn Sie in den vorhergehenden Schritten Änderungen an den Einstellungen vorgenommen haben, starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.




## Informationen zu diesem Vorgang



---


Der Assistent kann gestoppt und erneut gestartet werden, der Server ist jedoch erst betriebsbereit, wenn der gesamte Konfigurationsprozess abgeschlossen ist.

## Vorgehensweise

---

1. Starten Sie die lokale Version des Assistenten.
  -  AIX-Betriebssysteme  Linux-Betriebssysteme Öffnen Sie das Programm `dsmicfgx` im Verzeichnis `/opt/tivoli/tsm/server/bin`. Dieser Assistent kann nur als Rootbenutzer ausgeführt werden.
  -  Windows-Betriebssysteme Klicken Sie auf Start > Alle Programme > IBM Spectrum Protect > Konfigurationsassistent.
2. Führen Sie die Anweisungen aus, um die Konfiguration auszuführen. Verwenden Sie die während der IBM Spectrum Protect-Systemkonfiguration aufgezeichneten Informationen (siehe Arbeitsblätter zur Planung), um Verzeichnisse und Optionen im Assistenten anzugeben.

 AIX-Betriebssysteme  Linux-Betriebssysteme Legen Sie im Fenster Serverinformationen fest, dass der Server automatisch unter Verwendung der Instanzbenutzer-ID gestartet werden soll, wenn das System bootet.

 Windows-Betriebssysteme Mithilfe des Konfigurationsassistenten wird festgelegt, dass der Server automatisch gestartet werden soll, wenn ein Warmstart durchgeführt wird.

## Client für Sichern/Archivieren installieren

---

Installieren Sie als Best Practice den IBM Spectrum Protect-Client für Sichern/Archivieren auf dem Serversystem, sodass der Verwaltungsbefehlszeilenclient und der Scheduler verfügbar sind.

## Vorgehensweise

---

Um den Client für Sichern/Archivieren zu installieren, führen Sie die Installationsanweisungen für Ihr Betriebssystem aus.

- UNIX- und Linux-Clients für Sichern/Archivieren installieren
- Windows-Client für Sichern/Archivieren installieren

## Optionen für den Server festlegen

Überprüfen Sie die Serveroptionsdatei, die mit dem IBM Spectrum Protect-Server installiert wird, um sicherzustellen, dass die korrekten Werte für Ihr System festgelegt sind.

### Vorgehensweise

1. Wechseln Sie in das Serverinstanzverzeichnis und öffnen Sie die Datei dmserv.opt.
2. Überprüfen Sie die Werte in der folgenden Tabelle und Ihre Serveroptionseinstellungen auf der Basis der Systemgröße.

| Serveroption        | Wert für kleine Systeme                               | Wert für mittelgroße Systeme                          | Wert für große Systeme                                |
|---------------------|---|---|---|
| ACTIVELOGDIRECTORY  | Während der Konfiguration angegebener Verzeichnispfad | Während der Konfiguration angegebener Verzeichnispfad | Während der Konfiguration angegebener Verzeichnispfad |
| ACTIVELOGSIZE       | 131072  | 131072  | 262144  |
| ARCHLOGCOMPRESS     | Yes   | No  | No  |
| ARCHLOGDIRECTORY    | Während der Konfiguration angegebener Verzeichnispfad | Während der Konfiguration angegebener Verzeichnispfad | Während der Konfiguration angegebener Verzeichnispfad |
| COMMMETHOD          | TCPIP   | TCPIP   | TCPIP   |
| COMMTIMEOUT         | 3600  | 3600  | 3600  |
| DEDUPREQUIRESBACKUP | No  | No  | No  |
| DEVCONFIG           | devconf.dat   | devconf.dat   | devconf.dat   |
| EXPINTERVAL         | 0   | 0   | 0   |
| IDLETIMEOUT         | 60  | 60  | 60  |
| MAXSESSIONS         | 250   | 500   | 1000  |
| NUMOPENVOLSALLOWED  | 20  | 20  | 20  |
| TCPADMINPORT        | 1500  | 1500  | 1500  |
| TCPPORT             | 1500  | 1500  | 1500  |
| VOLUMEHISTORY       | volhist.dat   | volhist.dat   | volhist.dat   |

Aktualisieren Sie, falls erforderlich, Serveroptionseinstellungen in Übereinstimmung mit den Werten in der Tabelle. Um Aktualisierungen durchzuführen, schließen Sie die Datei dmserv.opt und definieren Sie die Optionen mit dem Befehl SETOPT in der Verwaltungsbefehlszeilenschnittstelle.

Um beispielsweise die Option IDLETIMEOUT mit 60 zu aktualisieren, geben Sie den folgenden Befehl aus:

```
setopt idletimeout 60
```

3. Um für den Server, die Clients und das Operations Center die sichere Kommunikation zu konfigurieren, überprüfen Sie die Optionen in der folgenden Tabelle.

| Serveroption | Alle Systemgrößen   |
|--------------|---|
| SSLFIPSMODE  | NO  |
| TCPPORT      | Geben Sie die Nummer des Ports an, an dem der Server auf Anforderungen von TCP/IP- und SSL-fähigen Sitzungen des Clients wartet.                          |
| TCPADMINPORT | Geben Sie die Adresse des Ports an, an dem der Server auf Anforderungen von TCP/IP- und SSL-fähigen Sitzungen des Verwaltungsbefehlszeilenclients wartet. |

Wenn einer der Optionswerte aktualisiert werden muss, editieren Sie die Datei dmserv.opt unter Verwendung der folgenden Anleitungen:

- Entfernen Sie den Stern am Anfang einer Zeile, um eine Option zu aktivieren.
- Geben Sie in jeder Zeile nur eine einzige Option und den für die Option angegebenen Wert ein.
- Wenn eine Option in mehreren Einträgen in der Datei vorkommt, verwendet der Server den letzten Eintrag.

Sichern Sie Ihre Änderungen und schließen Sie die Datei. Wenn Sie die Datei `dmserv.opt` direkt editieren, müssen Sie den Server erneut starten, damit die Änderungen wirksam werden.

#### Zugehörige Verweise:

- Referenz für Serveroptionen
- SETOPT (Serveroption für dynamische Aktualisierung definieren)

## Sichere Kommunikation mit Transport Layer Security konfigurieren

Um Daten zu verschlüsseln und die sichere Kommunikation in Ihrer Umgebung zu ermöglichen, ist Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) auf dem IBM Spectrum Protect-Server und dem Client für Sichern/Archivieren aktiviert. Kommunikationsanforderungen zwischen dem Server und dem Client werden mithilfe eines SSL-Zertifikats geprüft.

### Informationen zu diesem Vorgang

Wie in der folgenden Abbildung gezeigt können Sie die sichere Kommunikation zwischen dem Server und dem Client für Sichern/Archivieren manuell konfigurieren, indem Sie Optionen in der Server- und der Clientoptionsdatei definieren und dann das selbst signierte Zertifikat, das auf dem Server generiert wird, an den Client übertragen. Sie können auch stattdessen ein eindeutiges Zertifikat, das von einer Zertifizierungsstelle (CA) signiert ist, anfordern und übertragen.



Weitere Informationen zum Konfigurieren des Servers und von Clients für die SSL- oder TLS-Kommunikation finden Sie in Speicheragenten, Server, Clients und das Operations Center für die Verbindung zum Server unter Verwendung von SSL konfigurieren.

## Operations Center konfigurieren

Führen Sie nach der Installation des Operations Center die folgenden Konfigurationsschritte aus, um mit der Verwaltung Ihrer Speicherumgebung zu beginnen.

### Vorbereitende Schritte

Wenn Sie zum ersten Mal die Verbindung zum Operations Center herstellen, müssen Sie die folgenden Informationen angeben:

- Verbindungsinformationen für den Server, der als Hub-Server festgelegt werden soll
- Anmeldeberechtigungs-nachweise für eine Administrator-ID, die für diesen Server definiert ist

### Vorgehensweise

- Legen Sie den Hub-Server fest. Geben Sie in einem Web-Browser die folgende Adresse ein:

```
https://Hostname:sicherer_Port/oc
```

Erläuterungen:

- `Hostname` gibt den Namen des Computers an, auf dem das Operations Center installiert ist.
- `Sicherer_Port` gibt die Portnummer an, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet.

Wenn beispielsweise der Hostname `tsm.storage.mylocation.com` lautet und der standardmäßige sichere Port für das Operations Center (Port 11090) verwendet wird, ist die Adresse wie folgt:

```
https://tsm.storage.mylocation.com:11090/oc
```

Wenn Sie sich zum ersten Mal beim Operations Center anmelden, führt Sie ein Assistent durch eine Erstkonfiguration, um einen neuen Administrator mit Systemberechtigung auf dem Server zu konfigurieren.

- Konfigurieren Sie die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server, indem Sie das Protokoll Secure Sockets Layer (SSL) konfigurieren.

Führen Sie die Anweisungen in Kommunikation zwischen dem Operations Center und dem Hub-Server schützen aus.

3. Optional: Um einen täglichen E-Mail-Bericht mit einer Zusammenfassung des Systemstatus zu empfangen, konfigurieren Sie Ihre E-Mail-Einstellungen im Operations Center.

Führen Sie die Anweisungen in Systemstatus mithilfe von E-Mail-Berichten verfolgen aus.

- Kommunikation zwischen dem Operations Center und dem Hub-Server schützen  
Um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server zu ermöglichen, fügen Sie das TLS-Zertifikat des Hub-Servers der Truststore-Datei des Operations Center hinzu.

## Produktlizenz registrieren

---

Verwenden Sie zum Registrieren Ihrer Lizenz für das Produkt IBM Spectrum Protect den Befehl REGISTER LICENSE.

### Informationen zu diesem Vorgang


---

Lizenzen werden in Registrierungszertifikatsdateien gespeichert, die Lizenzinformationen für das Produkt enthalten. Die Registrierungszertifikatsdateien befinden sich auf den Installationsmedien und werden während der Installation auf den Server gestellt. Wenn Sie das Produkt registrieren, werden die Lizenzen in einer NODELOCK-Datei im aktuellen Verzeichnis gespeichert.

### Vorgehensweise

---

Registrieren Sie eine Lizenz, indem Sie den Namen der Registrierungszertifikatsdatei angeben, die die Lizenz enthält. Um den Command Builder des Operations Center für diese Task zu verwenden, führen Sie die folgenden Schritte aus.


1. Öffnen Sie das Operations Center.
2. Öffnen Sie den Command Builder des Operations Center, indem Sie den Mauszeiger über das Symbol für Einstellungen  bewegen und auf Command Builder klicken.
3. Geben Sie den Befehl REGISTER LICENSE aus. Um beispielsweise eine IBM Spectrum Protect-Basislizenz zu registrieren, geben Sie den folgenden Befehl aus:

```
register license file=tsmbasic.lic
```


### Nächste Schritte

---

Sichern Sie die Installationsmedien, die Ihre Registrierungszertifikatsdateien enthalten. Möglicherweise müssen Sie Ihre Lizenz erneut registrieren, wenn beispielsweise eine der folgenden Bedingungen erfüllt ist:

- Der Server wird auf einen anderen Computer versetzt.
- Die NODELOCK-Datei ist beschädigt. Der Server speichert Lizenzinformationen in der NODELOCK-Datei, die sich in dem Verzeichnis befindet, von dem aus der Server gestartet wird.
-  Linux-Betriebssysteme Sie ändern den Prozessorchip, der dem Server zugeordnet ist, auf dem der Server installiert ist.

#### Zugehörige Verweise:

-  REGISTER LICENSE (Neue Lizenz registrieren)

## Dateneduplizierung konfigurieren

---

Erstellen Sie einen Verzeichniscontainerspeicherpool und mindestens ein Verzeichnis für die Verwendung der Inline-Dateneduplizierung.

### Vorbereitende Schritte

---

Verwenden Sie für diese Task die aufgezeichneten Informationen zu Speicherpoolverzeichnissen (siehe Arbeitsblätter zur Planung).

### Vorgehensweise

---

1. Öffnen Sie das Operations Center.
2. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Speicher.
3. Klicken Sie in der angezeigten Liste auf Speicherpools.
4. Klicken Sie auf die Schaltfläche +Speicherpool.
5. Führen Sie die Schritte im Assistenten Speicherpool hinzufügen aus:



- Um die Inline-Dateneduplizierung verwenden zu können, wählen Sie einen Speicherpool Verzeichnis unter dem containerbasierten Speicher aus.
  - Wenn Sie Verzeichnisse für den Verzeichniscontainerspeicherpool konfigurieren, geben Sie die Verzeichnispfade an, die während der Systemkonfiguration für Speicher erstellt wurden.
6. Klicken Sie nach dem Konfigurieren des neuen Verzeichniscontainerspeicherpools auf Schließen & Maßnahmen anzeigen, um eine Verwaltungsklasse zu aktualisieren und mit der Verwendung des Speicherpools zu beginnen.

## Datenaufbewahrungsregeln für Ihr Unternehmen definieren

Nachdem Sie einen Verzeichniscontainerspeicherpool für die Dateneduplizierung erstellt haben, aktualisieren Sie die Serverstandardmaßnahme für die Verwendung des neuen Speicherpools. Die Seite Services im Operations Center wird vom Assistenten Speicherpool hinzufügen zur Ausführung dieser Task geöffnet.

### Vorgehensweise

1. Wählen Sie auf der Seite Services im Operations Center die Domäne STANDARD aus und klicken Sie auf Details.
2. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen. Die Seite Maßnahmengruppen gibt den Namen der aktiven Maßnahmengruppe an und listet alle Verwaltungsklassen für diese Maßnahmengruppe auf.
3. Klicken Sie auf die Umschaltfläche Konfigurieren und führen Sie die folgenden Änderungen durch:
  - Ändern Sie das Sicherungsziel für die Verwaltungsklasse STANDARD in den Verzeichniscontainerspeicherpool.
  - Ändern Sie den Wert für die Spalte 'Sicherungen' in Keine Begrenzung.
  - Ändern Sie den Aufbewahrungszeitraum. Setzen Sie den Wert für die Spalte 'Zusätzliche Sicherungen aufbewahren' abhängig von Ihren Geschäftsanforderungen auf 30 Tage oder mehr.
4. Sichern Sie Ihre Änderungen und klicken Sie erneut auf die Umschaltfläche Konfigurieren, damit die Maßnahmengruppe nicht mehr editierbar ist.
5. Aktivieren Sie die Maßnahmengruppe, indem Sie auf Aktivieren klicken.

#### Zugehörige Tasks:

Regeln zum Sichern und Archivieren von Clientdaten angeben

## Zeitpläne für Serververwaltungsaktivitäten definieren

Erstellen Sie Zeitpläne für jede Serververwaltungsoperation, indem Sie den Befehl DEFINE SCHEDULE im Command Builder des Operations Center verwenden.

### Informationen zu diesem Vorgang

Planen Sie die Ausführung von Serververwaltungsoperationen im Anschluss an Clientsicherungsoperationen. Sie können das Timing von Zeitplänen steuern, indem Sie die Startzeit in Kombination mit der Dauer für jede Operation definieren.

Das folgende Beispiel zeigt die Planung von Serververwaltungsoperationen in Kombination mit dem Clientsicherungszeitplan für eine Plattenspeicherlösung für einen einzelnen Standort.

| Operation  | Zeitplan  |
|--|---|
| Clientsicherung  | Startet um 22:00 Uhr.   |
| Verarbeitung für die Datenbank und die Dateien zur Wiederherstellung nach einem Katastrophenfall | <ul style="list-style-type: none"> <li>• Die Datenbanksicherungsoperation startet um 11:00 Uhr bzw. 13 Stunden nach dem Start der Clientsicherungsoperation. Dieser Prozess wird bis zum Abschluss ausgeführt.</li> <li>• Die Sicherungsoperationen für Einheitenkonfigurationsinformationen und das Datenträgerprotokoll starten um 17:00 Uhr bzw. 6 Stunden nach dem Start der Datenbanksicherungsoperation.</li> <li>• Das Löschen des Datenträgerprotokolls startet um 20:00 Uhr bzw. 9 Stunden nach dem Start der Datenbanksicherungsoperation.</li> </ul> |
| Bestandsverfall  | Startet um 12:00 Uhr bzw. 14 Stunden nach dem Start der Clientsicherungsoperation. Dieser Prozess wird bis zum Abschluss ausgeführt.  |



### Vorgehensweise

Erstellen Sie nach dem Konfigurieren der Einheitenklasse für die Datenbanksicherungsoperationen Zeitpläne für Datenbanksicherungsoperationen und andere erforderliche Verwaltungsoperationen mithilfe des Befehls DEFINE SCHEDULE. Abhängig von der Größe Ihrer Umgebung müssen Sie die Startzeiten für jeden Zeitplan in dem Beispiel gegebenenfalls anpassen.


- Definieren Sie eine Einheitenklasse für die Sicherungsoperationen. Erstellen Sie beispielsweise mit dem Befehl DEFINE DEVCLASS eine Einheitenklasse mit dem Namen DBBACK\_FILEDEV:

```
define devclass dbback_filedev devtype=file
  directory=Datenbanksicherungsverzeichnisse
```

Dabei ist *Datenbanksicherungsverzeichnisse* eine Liste der für die Datenbanksicherung erstellten Verzeichnisse.

 AIX-Betriebssysteme  Linux-Betriebssysteme Wenn beispielsweise vier Verzeichnisse für Datenbanksicherungen mit /tsminst1/TSMbkup00 als Startpunkt vorhanden sind, geben Sie den folgenden Befehl aus:

```
define devclass dbback_filedev devtype=file
  directory=/tsminst1/TSMbkup00,
  /tsminst1/TSMbkup01,/tsminst1/TSMbkup02,
  /tsminst1/TSMbkup03"
```

 Windows-Betriebssysteme Wenn beispielsweise vier Verzeichnisse für Datenbanksicherungen mit C:\tsminst1\TSMbkup00 als Startpunkt vorhanden sind, geben Sie den folgenden Befehl aus:

```
define devclass dbback_filedev devtype=file
  directory="c:\tsminst1\TSMbkup00,
  c:\tsminst1\TSMbkup01,c:\tsminst1\TSMbkup02,c:\tsminst1\TSMbkup03"
```

- Legen Sie die Einheitenklasse für automatische Datenbanksicherungsoperationen fest. Geben Sie mit dem Befehl SET DBRECOVERY die im vorhergehenden Schritt erstellte Einheitenklasse an. Wenn beispielsweise die Einheitenklasse den Namen dbback\_filedev hat, geben Sie den folgenden Befehl aus:

```
set dbrecovery dbback_filedev
```

- Erstellen Sie mithilfe des Befehls DEFINE SCHEDULE Zeitpläne für die Verwaltungsoperationen. Die folgende Tabelle enthält die erforderlichen Operationen und Beispiele der Befehle.

| Operation  | Beispielbefehl  |
|--|---|
| Sichern der Datenbank                            | Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP DB. Wenn Sie ein kleines System konfigurieren, setzen Sie den Parameter COMPRESS auf YES.<br>Geben Sie beispielsweise auf einem kleinen System den folgenden Befehl aus, um einen Sicherungszeitplan zu erstellen, der die neue Einheitenklasse verwendet:<br><br>define schedule DBBACKUP type=admin cmd="backup db devclass=dbback_filedev type=full numstreams=3 wait=yes compress=yes" active=yes desc="Datenbank sichern."<br>startdate=today starttime=11:00:00 duration=45 durunits=minutes |
| Sichern der Einheitenkonfigurationsinformationen | Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP DEVCONFIG:<br><br>define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Einheitenkonfigurationsdatei sichern." startdate=today starttime=17:00:00 duration=45 durunits=minutes  |
| Sichern des Datenträgerprotokolls                | Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP VOLHISTORY:<br><br>define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Datenträgerprotokoll sichern." startdate=today starttime=17:00:00 duration=45 durunits=minutes  |

| Operation  | Beispielbefehl  |
|--|---|
| Entfernen älterer Versionen von Datenbanksicherungen, die nicht mehr erforderlich sind | Erstellen Sie einen Zeitplan für die Ausführung des Befehls DELETE VOLHISTORY:<br><br><pre>define schedule DELVOLHIST type=admin cmd="delete volhistory   type=dbb todate=today-6 totime=now" active=yes desc="Alte Datenbanksicherungen entfernen." startdate=today starttime=20:00:00 duration=45 durunits=minutes</pre>  |
| Entfernen von Objekten, deren zulässige Aufbewahrungsdauer überschritten wurde         | Erstellen Sie einen Zeitplan für die Ausführung des Befehls EXPIRE INVENTORY.<br>Definieren Sie den Parameter RESOURCE auf der Basis der Systemgröße, die Sie konfigurieren: <ul style="list-style-type: none"> <li>o Kleine Systeme: 10</li> <li>o Mittlere Systeme: 30</li> <li>o Große Systeme: 40</li> </ul> Geben Sie beispielsweise auf einem mittelgroßen System den folgenden Befehl aus, um einen Zeitplan mit dem Namen EXPINVENTORY zu erstellen:<br><br><pre>define schedule EXPINVENTORY type=admin cmd="expire inventory   wait=yes resource=30 duration=120" active=yes desc="Verfallene Objekte entfernen." startdate=today starttime=12:00:00 duration=45 durunits=minutes</pre> |

## Nächste Schritte

Nachdem Sie Zeitpläne für die Serververwaltungstasks erstellt haben, können Sie diese im Operations Center anzeigen, indem Sie die folgenden Schritte ausführen:

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Server.
2. Klicken Sie auf Verwaltung.

### Zugehörige Verweise:

➔ DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)

## Clientzeitpläne definieren

Erstellen Sie mithilfe des Operations Center Zeitpläne für Clientoperationen.

### Vorgehensweise

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Clients.
2. Klicken Sie auf Zeitpläne.
3. Klicken Sie auf +Zeitplan.
4. Führen Sie die Schritte im Assistenten Zeitplan erstellen aus. Definieren Sie auf der Basis der in Zeitpläne für Serververwaltungsaktivitäten definierten geplanten Serververwaltungsaktivitäten für Clientsicherungszeitpläne eine Startzeit von 22:00 Uhr.

## Clients für Sichern/Archivieren installieren und konfigurieren

Installieren und konfigurieren Sie im Anschluss an die erfolgreiche Konfiguration Ihres IBM Spectrum Protect-Serversystems die Client-Software, um mit dem Sichern von Daten beginnen zu können.

### Vorgehensweise

Um den Client für Sichern/Archivieren zu installieren, führen Sie die Installationsanweisungen für Ihr Betriebssystem aus.

- UNIX- und Linux-Clients für Sichern/Archivieren installieren
- Windows-Client für Sichern/Archivieren installieren

## Nächste Schritte

---

Registrieren Sie Ihre Clients und ordnen Sie Ihre Clients Zeitplänen zu.

- Clients registrieren und Zeitplänen zuordnen  
Sie können Ihre Clients über das Operations Center mithilfe des Assistenten Client hinzufügen hinzufügen und registrieren.
- Clientverwaltungsservice installieren  
Installieren Sie den Clientverwaltungsservice für Clients für Sichern/Archivieren, die unter Linux- und Windows-Betriebssystemen ausgeführt werden. Der Clientverwaltungsservice erfasst Diagnoseinformationen zu Clients für Sichern/Archivieren und stellt die Informationen dem Operations Center für die grundlegende Überwachungsfunktion zur Verfügung.

## Clients registrieren und Zeitplänen zuordnen

---

Sie können Ihre Clients über das Operations Center mithilfe des Assistenten Client hinzufügen hinzufügen und registrieren.

### Vorbereitende Schritte

---

Bestimmen Sie, ob der Client eine Benutzer-ID mit Administratorberechtigung mit Clienteignerberechtigung für den Clientknoten erfordert. Informationen zum Bestimmen der Clients, die eine Benutzer-ID mit Administratorberechtigung erfordern, finden Sie in Technote 7048963.

Einschränkung: Bei einigen Clienttypen müssen der Clientknotenname und die Benutzer-ID mit Administratorberechtigung übereinstimmen. Sie können diese Clients nicht mithilfe der in Version 7.1.7 eingeführten LDAP-Authentifizierungsmethode authentifizieren. Ausführliche Informationen zu dieser Authentifizierungsmethode, die manchmal als integrierter Modus bezeichnet wird, finden Sie in Benutzer mithilfe einer Active Directory-Datenbank authentifizieren.

### Vorgehensweise

---

Um einen Client zu registrieren, führen Sie eine der folgenden Aktionen aus.

- Wenn der Client eine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Befehl REGISTER NODE unter Angabe des Parameters USERID:

```
register node Knotenname Kennwort userid=Knotenname
```

Dabei gibt *Knotenname* den Knotennamen und *Kennwort* das Knotenkennwort an. Ausführliche Informationen finden Sie in Knoten registrieren.

- Wenn der Client keine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Assistenten 'Client hinzufügen' im Operations Center. Führen Sie die folgenden Schritte aus:
  - a. Klicken Sie in der Menüleiste des Operations Center auf Clients.
  - b. Klicken Sie in der Tabelle 'Clients' auf + Client.
  - c. Führen Sie die Schritte im Assistenten Client hinzufügen aus:
    - i. Geben Sie an, dass redundante Daten sowohl auf dem Client als auch auf dem Server gelöscht werden können. Wählen Sie im Bereich 'Clientseitige Datendeduplizierung' das Kontrollkästchen Aktivieren aus.
    - ii. Kopieren Sie im Fenster Konfiguration die Werte für die Optionen TCPSERVERADDRESS, TCPPORT, NODENAME und DEPLICATION.  
Tipp: Notieren Sie die Optionswerte und bewahren Sie die Unterlagen an einem sicheren Ort auf. Nachdem Sie die Clientregistrierung abgeschlossen und die Software auf dem Clientknoten installiert haben, verwenden Sie die Werte zum Konfigurieren des Clients.
    - iii. Führen Sie die Anweisungen im Assistenten aus, um die Maßnahmendomäne, den Zeitplan und die Optionsgruppe anzugeben.
    - iv. Legen Sie fest, wie Risiken für den Client angezeigt werden, indem Sie die Einstellung für die Gefährdung angeben.
    - v. Klicken Sie auf Client hinzufügen.

## Clientverwaltungsservice installieren

---

Installieren Sie den Clientverwaltungsservice für Clients für Sichern/Archivieren, die unter Linux- und Windows-Betriebssystemen ausgeführt werden. Der Clientverwaltungsservice erfasst Diagnoseinformationen zu Clients für Sichern/Archivieren und stellt die Informationen dem Operations Center für die grundlegende Überwachungsfunktion zur Verfügung.

### Vorgehensweise

---

Installieren Sie den Clientverwaltungsservice auf demselben Computer wie den Client für Sichern/Archivieren, indem Sie die folgenden Schritte ausführen:

1. Laden Sie das Installationspaket für den Clientverwaltungsservice von einer IBM® Download-Site, wie beispielsweise IBM Passport Advantage® oder IBM Fix Central, herunter. Suchen Sie nach einem ähnlichen Dateinamen wie `<Version>-IBM_Spectrum_Protect-CMS-Betriebssystem.bin`.
  2. Erstellen Sie auf dem Clientsystem, das verwaltet werden soll, ein Verzeichnis und kopieren Sie das Installationspaket in dieses Verzeichnis.
  3. Extrahieren Sie den Inhalt der Installationspaketdatei.
  4. Führen Sie die Installationsstapeldatei in dem Verzeichnis aus, in das die Installationsdateien und die zugehörigen Dateien extrahiert wurden. Dabei handelt es sich um das in Schritt 2 erstellte Verzeichnis.
  5. Um den Clientverwaltungsservice zu installieren, führen Sie die Anweisungen im Assistenten von IBM Installation Manager aus. Wenn IBM Installation Manager noch nicht auf dem Clientsystem installiert ist, müssen Sie sowohl IBM Installation Manager als auch die IBM Spectrum Protect-Clientverwaltungsservices auswählen.
- Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen  
Bevor Sie den Clientverwaltungsservice zum Erfassen von Diagnoseinformationen zu einem Client für Sichern/Archivieren verwenden, können Sie überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist.
  - Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren  
Wenn für den Clientverwaltungsservice nicht die Standardkonfiguration verwendet wurde, müssen Sie das Operations Center für den Zugriff auf den Clientverwaltungsservice konfigurieren.

#### Zugehörige Tasks:

- ☛ Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren

## Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen

Bevor Sie den Clientverwaltungsservice zum Erfassen von Diagnoseinformationen zu einem Client für Sichern/Archivieren verwenden, können Sie überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist.

### Vorgehensweise

Führen Sie auf dem Clientsystem in der Befehlszeile die folgenden Befehle aus, um die Konfiguration des Clientverwaltungsservice anzuzeigen:

- Geben Sie auf Linux-Clientsystemen den folgenden Befehl aus:

```
Clientinstallationsverzeichnis/cms/bin/CmsConfig.sh list
```

Dabei ist *Clientinstallationsverzeichnis* das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist. Geben Sie beispielsweise bei der Standardclientinstallation den folgenden Befehl aus:

```
/opt/tivoli/tsm/cms/bin/CmsConfig.sh list
```

Die Ausgabe sieht ähnlich wie die folgende aus:

```
Listing CMS configuration
```

```
server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
  Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

  Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
            en_US MM/dd/yyyy HH:mm:ss Windows-1252
  Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
            en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

- Geben Sie auf Windows-Clientsystemen den folgenden Befehl aus:

```
Clientinstallationsverzeichnis\cms\bin\CmsConfig.bat list
```

Dabei ist *Clientinstallationsverzeichnis* das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist. Geben Sie beispielsweise bei der Standardclientinstallation den folgenden Befehl aus:

```
C:"Programme"\Tivoli\TSM\cms\bin\CmsConfig.bat list
```

Die Ausgabe sieht ähnlich wie die folgende aus:

```
Listing CMS configuration
```

```
server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
  Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt
```

```
Log File: C:\Program Files\Tivoli\TSM\baclient\dsmserror.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252
Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

Wenn der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist, wird in der Ausgabe die Position der Fehlerprotokolldatei angezeigt.

Der Ausgabebetext wird aus der folgenden Konfigurationsdatei extrahiert:

- Auf Linux-Clientsystemen:

```
Clientinstallationsverzeichnis/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
```

- Auf Windows-Clientsystemen:

```
Clientinstallationsverzeichnis\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
```

Wenn die Ausgabe keine Einträge enthält, müssen Sie die Datei client-configuration.xml konfigurieren. Anweisungen zum Konfigurieren dieser Datei finden Sie in Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren. Mit dem Befehl CmsConfig verify können Sie überprüfen, ob eine Knotendefinition in der Datei client-configuration.xml korrekt erstellt wurde.

## Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren

Wenn für den Clientverwaltungsservice nicht die Standardkonfiguration verwendet wurde, müssen Sie das Operations Center für den Zugriff auf den Clientverwaltungsservice konfigurieren.

### Vorbereitende Schritte

Stellen Sie sicher, dass der Clientverwaltungsservice auf dem Clientsystem installiert und gestartet wurde. Überprüfen Sie, ob die Standardkonfiguration verwendet wird. Die Standardkonfiguration wird nicht verwendet, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Clientverwaltungsservice verwendet nicht die Standardportnummer 9028.
- Der Zugriff auf den Client für Sichern/Archivieren erfolgt nicht über dieselbe IP-Adresse wie für das Clientsystem, auf dem der Client für Sichern/Archivieren installiert ist. Eine andere IP-Adresse kann beispielsweise in den folgenden Situationen verwendet werden:
  - Das Computersystem verfügt über zwei Netzkarten. Der Client für Sichern/Archivieren ist für die Kommunikation in einem Netz konfiguriert, der Clientverwaltungsservice kommuniziert jedoch in dem anderen Netz.
  - Das Clientsystem ist mit DHCP (Dynamic Host Configuration Protocol) konfiguriert. Demzufolge wird dem Clientsystem dynamisch eine IP-Adresse zugeordnet, die während der vorherigen Operation des Clients für Sichern/Archivieren auf dem Server gespeichert wurde. Wenn das Clientsystem erneut gestartet wird, wird ihm möglicherweise eine andere IP-Adresse zugeordnet. Um sicherzustellen, dass das Operations Center das Clientsystem immer finden kann, müssen Sie einen vollständig qualifizierten Domännennamen angeben.

### Vorgehensweise

Um das Operations Center für die Verwendung des Clientverwaltungsservice zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie auf der Seite 'Clients' im Operations Center den Client aus.
2. Klicken Sie auf Details > Merkmale.
3. Geben Sie im Feld 'URL für Ferndiagnose' im Abschnitt 'Allgemein' die URL für den Clientverwaltungsservice auf dem Clientsystem an. Die Adresse muss mit `https` beginnen. In der folgenden Tabelle sind Beispiele für die URL für Ferndiagnose aufgeführt.

| Typ der URL  | Beispiel                                     |
|--|--|
| Mit DNS-Hostname und Standardport 9028                       | <code>https://server.example.com</code>      |
| Mit DNS-Hostname und einem anderen Port als dem Standardport | <code>https://server.example.com:1599</code> |
| Mit IP-Adresse und einem anderen Port als dem Standardport   | <code>https://192.0.2.0:1599</code>          |

4. Klicken Sie auf Sichern.

### Nächste Schritte

Über die Registerkarte Diagnose im Operations Center können Sie auf Clientdiagnoseinformationen, wie beispielsweise Clientprotokolldateien, zugreifen.

## Implementierung abschließen

---

Nachdem die IBM Spectrum Protect- Lösung konfiguriert wurde und aktiv ist, testen Sie Sicherungsoperationen und konfigurieren Sie die Überwachung, um sicherzustellen, dass alles ordnungsgemäß funktioniert.

### Vorgehensweise

---

1. Testen Sie Sicherungsoperationen, um sicherzustellen, dass Ihre Daten wie erwartet geschützt werden.
  - a. Wählen Sie auf der Seite Clients im Operations Center die Clients aus, die gesichert werden sollen, und klicken Sie auf Sichern.
  - b. Wählen Sie auf der Seite Server im Operations Center den Server aus, dessen Datenbank gesichert werden soll. Klicken Sie auf Sichern und führen Sie die Anweisungen im Fenster Datenbank sichern aus.
  - c. Überprüfen Sie, ob die Sicherungsoperationen erfolgreich ohne Warnungen oder Fehlermeldungen ausgeführt wurden.  
Tipp: Sie können auch stattdessen die GUI des Clients für Sichern/Archivieren zum Sichern von Clientdaten verwenden und die Serverdatenbank sichern, indem Sie den Befehl BACKUP DB in einer Verwaltungsbefehlszeile ausgeben.
2. Konfigurieren Sie die Überwachung für Ihre Lösung, indem Sie die Anweisungen in Plattenspeicherlösung für einen einzelnen Standort überwachen ausführen.

## Plattenspeicherlösung für einen einzelnen Standort überwachen

---

Überwachen Sie nach der Implementierung einer Plattenspeicherlösung für einen einzelnen Standort mit IBM Spectrum Protect die Lösung auf ihre korrekte Funktionsweise. Indem die Lösung täglich und regelmäßig überwacht wird, können Sie bestehende und potenzielle Probleme erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden.

### Informationen zu diesem Vorgang

---

Die Überwachung einer Lösung erfolgt bevorzugt über die Verwendung des Operations Center, das den Gesamtsystemstatus und den detaillierten Systemstatus in einer grafischen Benutzerschnittstelle bereitstellt. Darüber hinaus können Sie das Operations Center zum Generieren eines täglichen E-Mail-Berichts mit einer Zusammenfassung des Systemstatus konfigurieren.

In einigen Fällen möchten Sie vielleicht erweiterte Überwachungstools verwenden, um bestimmte Überwachungs- oder Fehlerbehebungstasks auszuführen.

Tipp: Wenn Sie planen, Probleme bei Clients für Sichern/Archivieren unter Linux- oder Windows-Betriebssystemen zu diagnostizieren, installieren Sie IBM Spectrum Protect-Clientverwaltungsservices auf jedem Computer, auf dem ein Client für Sichern/Archivieren installiert ist. Auf diese Art und Weise können Sie sicherstellen, dass die Schaltfläche Diagnose im Operations Center zur Diagnose von Problemen bei Clients für Sichern/Archivieren verfügbar ist. Um den Clientverwaltungsservice zu installieren, führen Sie die Anweisungen in Clientverwaltungsservice installieren aus.

### Vorgehensweise

---

1. Führen Sie tägliche Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für tägliche Tasks.
2. Führen Sie regelmäßige Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für regelmäßige Überwachungstasks.
3. Um zu überprüfen, ob Ihre IBM Spectrum Protect-Lösung die Lizenzierungsanforderungen erfüllt, führen Sie die Anweisungen in Lizenzierung überprüfen aus.
4. Informationen zur Konfiguration des Operations Center zum Erstellen von E-Mail-Statusberichten finden Sie in Systemstatus mithilfe von E-Mail-Berichten verfolgen.

### Nächste Schritte

---

Beheben Sie alle erkannten Probleme. Wenn ein Problem durch Ändern der Konfiguration Ihrer Lösung behoben werden soll, führen Sie die Anweisungen in Operationen für eine Plattenspeicherlösung für einen einzelnen Standort verwalten aus. Die folgenden Ressourcen sind ebenfalls verfügbar:

- Informationen zur Behebung von Leistungsproblemen finden Sie in Leistung.
- Informationen zur Behebung anderer Typen von Problemen finden Sie in Fehlerbehebung.

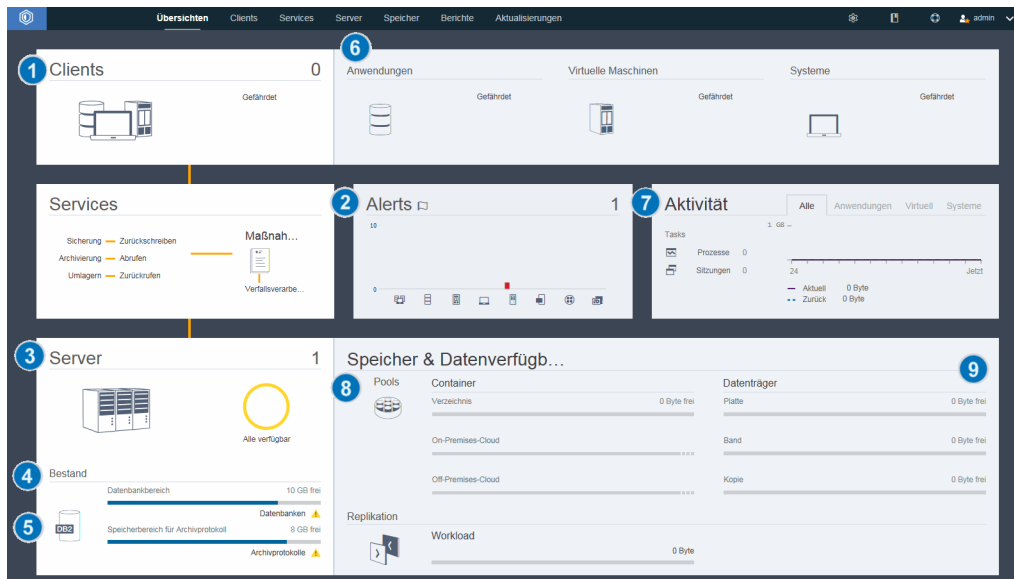
## Prüfliste für tägliche Überwachungstasks


---

Um sicherzustellen, dass die täglichen Überwachungstasks für Ihre IBM Spectrum Protect-Lösung ausgeführt werden, überprüfen Sie die Prüfliste für tägliche Überwachungstasks.

Führen Sie die täglichen Überwachungstasks über die Seite Übersicht im Operations Center aus. Sie können auf die Seite Übersicht zugreifen, indem Sie das Operations Center öffnen und auf Übersichten klicken.

Die folgende Abbildung zeigt die Position zur Ausführung der jeweiligen Task.



Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen  und klicken Sie auf Command Builder.






In der folgenden Tabelle sind die täglichen Überwachungstasks sowie Anweisungen zur Ausführung jeder Task aufgeführt.


Tabelle 1. Tägliche Überwachungstasks

| Task   | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen  |
|--|--|---|
| <p><b>1</b> Bestimmen Sie, ob Clients vorhanden sind, bei denen die Gefahr besteht, dass sie aufgrund fehlgeschlagener oder versäumter Sicherungsoperationen ungeschützt sind.</p> | <p>Um zu überprüfen, ob Clients gefährdet sind, suchen Sie nach einem Hinweis Gefährdet. Um Details anzuzeigen, klicken Sie auf den Bereich 'Clients'.</p> <p>Achtung: Wenn der Prozentsatz für Gefährdet sehr viel höher als üblicherweise ist, kann dies eine Ransomware-Attacke anzeigen. Eine Ransomware-Attacke kann das Fehlschlagen von Sicherungsoperationen zur Folge haben und somit Clients in den Status 'Gefährdet' versetzen. Wenn beispielsweise der Prozentsatz gefährdeter Clients normalerweise zwischen 5 % und 10 % liegt, sich aber auf 40 % oder 50 % erhöht, ermitteln Sie die Ursache.</p> <p>Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie die Clientfehler- und -planungsprotokolle anzeigen, indem Sie die folgenden Schritte ausführen:</p> <ol style="list-style-type: none"> <li>1. Wählen Sie in der Tabelle 'Clients' den Client aus und klicken Sie auf Details.</li> <li>2. Um ein Problem zu diagnostizieren, klicken Sie auf Diagnose.</li> </ol> | <p>Greifen Sie bei Clients, für die der Clientverwaltungsservice nicht installiert ist, auf das Clientsystem zu, um die Clientfehlerprotokolle zu überprüfen.</p> |







| Task   | Basisprozeduren   | Erweiterte Prozeduren und Fehlerbehebungsinformationen  |
|--|---|---|
| <p><b>2</b> Bestimmen Sie, ob clientbezogene oder serverbezogene Fehler einen Bedieneringriff erfordern.</p>                                       | <p>Um die Bewertung jedes zurückgemeldeten Alerts zu bestimmen, bewegen Sie den Mauszeiger im Bereich 'Alerts' über die Spalten.</p>  | <p>Um zusätzliche Informationen zu Alerts anzuzeigen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf den Bereich 'Alerts'.</li> <li>2. Wählen Sie in der Tabelle 'Alerts' einen Alert aus.</li> <li>3. Überprüfen Sie die Nachrichten im Fenster 'Aktivitätenprotokoll'. In dem Fenster werden zugehörige Nachrichten angezeigt, die vor und nach dem Auftreten des ausgewählten Alerts ausgegeben wurden.</li> </ol> |
| <p><b>3</b> Bestimmen Sie, ob die vom Operations Center verwalteten Server verfügbar sind, um Datenschutzservices für Clients bereitzustellen.</p> | <ol style="list-style-type: none"> <li>1. Um zu überprüfen, ob Server gefährdet sind, suchen Sie im Bereich 'Server' nach einem Hinweis Nicht verfügbar.</li> <li>2. Um zusätzliche Informationen anzuzeigen, klicken Sie auf den Bereich 'Server'.</li> <li>3. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details.</li> </ol> | <p> Tipp: Wenn Sie ein Problem erkennen, das sich auf die Servermerkmale bezieht, aktualisieren Sie die Servermerkmale:</p> <ol style="list-style-type: none"> <li>1. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details.</li> <li>2. Um die Servermerkmale zu aktualisieren, klicken Sie auf Merkmale.</li> </ol>   |

| Task   | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|--|--|--|
| <p>4 Bestimmen Sie, ob für den Serverbestand, der aus der Serverdatenbank, der aktiven Protokolldatei und dem Archivprotokoll besteht, genügend Speicherbereich verfügbar ist.</p> | <ol style="list-style-type: none"> <li>1. Klicken Sie auf den Bereich 'Server'.</li> <li>2. Zeigen Sie in der Spalte 'Status' der Tabelle den Status des Servers an und beheben Sie alle Probleme: <ul style="list-style-type: none"> <li>o Normal  Für die Serverdatenbank, die aktive Protokolldatei und das Archivprotokoll ist genügend Speicherbereich verfügbar.</li> <li>o Kritisch  Für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll ist nicht genügend Speicherbereich verfügbar. Sie müssen unverzüglich Speicherbereich hinzufügen; andernfalls werden die vom Server bereitgestellten Datenschutzservices unterbrochen.</li> <li>o Warnung  Der Speicherbereich für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll wird knapp. Wenn diese Bedingung bestehen bleibt, müssen Sie Speicherbereich hinzufügen.</li> <li>o Nicht verfügbar  Der Status kann nicht abgerufen werden. Stellen Sie sicher, dass der Server aktiv ist und keine Netzprobleme vorliegen. Dieser Status wird auch angezeigt, wenn die Überwachungsadministrator-ID gesperrt ist oder aus anderen Gründen auf dem Server nicht verfügbar ist. Diese ID hat den Namen IBM-OC-Name_des_Hub-Servers.</li> <li>o Nicht überwacht  Nicht überwachte Server sind für den Hub-Server definiert, aber nicht für die Verwaltung durch das Operations Center konfiguriert. Um einen nicht überwachten Server zu konfigurieren, wählen Sie den Server aus und klicken Sie auf Peripherieserver überwachen.</li> </ul> </li> </ol> | <p>Sie können auch auf der Seite Alerts nach zugehörigen Alerts suchen. Weitere Anweisungen zur Fehlerbehebung finden Sie in Serverprobleme beheben.</p> |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|---|--|--|
| <p><b>5</b> Überprüfen Sie Operationen zur Sicherung der Serverdatenbank.</p>   | <p>Um zu bestimmen, ob ein Server kürzlich gesichert wurde, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf den Bereich 'Server'.</li> <li>2. Überprüfen Sie in der Tabelle 'Server' die Spalte 'Letzte Datenbanksicherung'.</li> </ol>   | <p>Um detaillierte Informationen zu Sicherungsoperationen abzurufen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Wählen Sie in der Tabelle 'Server' eine Zeile aus und klicken Sie auf Details.</li> <li>2. Bewegen Sie im Bereich 'Datenbanksicherung' den Mauszeiger über die Häkchen, um Informationen zu Sicherungsoperation zu überprüfen.</li> </ol> <p>Wenn eine Datenbank nicht kürzlich (beispielsweise innerhalb der letzten 24 Stunden) gesichert wurde, können Sie eine Sicherungsoperation starten:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Server'.</li> <li>2. Wählen Sie in der Tabelle einen Server aus und klicken Sie auf Sichern.</li> </ol> <p>Um zu bestimmen, ob die Serverdatenbank für automatische Sicherungsoperationen konfiguriert ist, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>2. Geben Sie den Befehl QUERY DB aus: <pre>query db f=d</pre> </li> <li>3. Überprüfen Sie in der Ausgabe das Feld Einheitenklassenname für Gesamtsicherungen. Wenn eine Einheitenklasse angegeben ist, ist der Server für automatische Datenbanksicherungen konfiguriert.</li> </ol> |
| <p><b>6</b> Überwachen Sie andere Serververwaltungstasks. Serververwaltungstasks können die Ausführung von Zeitplänen für Verwaltungsbefehle, Verwaltungsscripts und zugehörigen Befehlen umfassen.</p> | <p>Um nach Informationen zu Prozessen zu suchen, die aufgrund von Serverproblemen fehlgeschlagen sind, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf Server &gt; Verwaltung.</li> <li>2. Um das zwei Wochen umfassende Verlaufsprotokoll eines Prozesses abzurufen, zeigen Sie Spalte 'History' an.</li> <li>3. Um weitere Informationen zu einem geplanten Prozess abzurufen, bewegen Sie den Mauszeiger über das Kontrollkästchen, das dem Prozess zugeordnet ist.</li> </ol> | <p>Weitere Informationen zum Überwachen von Prozessen und Beheben von Problemen, finden Sie in der Onlinehilfe des Operations Center.</p>  |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|---|--|--|
| <p><b>7</b> Überprüfen Sie, ob das Datenvolumen, das kürzlich an Server bzw. von Servern gesendet wurde, innerhalb des erwarteten Bereichs liegt.</p> | <ul style="list-style-type: none"> <li>• Um eine Übersicht über die Aktivität der letzten 24 Stunden abzurufen, zeigen Sie den Bereich 'Aktivität' an.</li> <li>• Um die Aktivität der letzten 24 Stunden mit der Aktivität der vorherigen 24 Stunden zu vergleichen, studieren Sie die Zahlen in den Bereichen 'Aktuell' und 'Vorherig'.</li> </ul> | <ul style="list-style-type: none"> <li>• Wenn mehr Daten als erwartet an den Server gesendet wurden, bestimmen Sie die Clients, die mehr Daten sichern und ermitteln Sie die Ursache. Möglicherweise funktioniert die clientseitige Datenduplizierung nicht ordnungsgemäß.<br/>Achtung: Wenn das Volumen gesicherter Daten deutlich umfangreicher als üblicherweise ist, kann dies eine Ransomware-Attacke anzeigen. Wenn Daten durch Ransomware verschlüsselt werden, werden die Daten vom System als geändert wahrgenommen und die geänderten Daten werden gesichert. Demzufolge wird das Volumen gesicherter Daten umfangreicher. Um die betroffenen Clients zu bestimmen, klicken Sie auf die Registerkarten Anwendungen, Virtuell oder Systeme.</li> <li>• Wenn weniger Daten als erwartet an den Server gesendet wurden, überprüfen Sie, ob Clientsicherungsoperationen gemäß Zeitplan ausgeführt werden.</li> </ul> |

| Task   | Basisprozeduren   | Erweiterte Prozeduren und Fehlerbehebungsinformationen  |
|--|---|---|
| <p><b>8</b> Stellen Sie sicher, dass Speicherpools zum Sichern von Clientdaten verfügbar sind.</p> | <p>1. Wenn im Bereich 'Speicher &amp; Datenverfügbarkeit' Probleme angezeigt werden, klicken Sie auf Pools, um die Details anzuzeigen:</p> <ul style="list-style-type: none"> <li>○ Wenn der Status Kritisch  angezeigt wird, ist in dem Speicherpool nicht genügend Speicherbereich verfügbar oder der Speicherpool hat den Zugriffsstatus UNAVAILABLE (Nicht verfügbar).<br/>Achtung: Wenn der Status kritisch ist, ermitteln Sie die Ursache: <ul style="list-style-type: none"> <li>■ Wenn die Dateneduplizierungsrate für einen Speicherpool deutlich fällt, kann dies eine Ransomware-Attacke anzeigen. Während einer Ransomware-Attacke werden Daten verschlüsselt und können nicht dedupliziert werden. Um die Dateneduplizierungsrate zu verifizieren, überprüfen Sie in der Tabelle 'Speicherpools' den Wert in der Spalte 'Einsparungen in %'.</li> <li>■ Wenn ein Speicherpool wider Erwarten zu 100 % ausgelastet ist, kann dies eine Ransomware-Attacke anzeigen. Um die Auslastung zu verifizieren, überprüfen Sie den Wert in der Spalte 'Verwendete Kapazität'.<br/>Bewegen Sie den Mauszeiger über die Werte, um den Prozentsatz für den verwendeten Speicherbereich und den Prozentsatz für den freien Speicherbereich anzuzeigen.</li> </ul> </li> <li>○ Wenn der Status Warnung  angezeigt wird, wird der Speicherbereich für den Speicherpool knapp oder der Speicherpool hat den Zugriffsstatus READONLY (Lesezugriff).</li> </ul> <p>2. Um den verwendeten Speicherbereich, den freien Speicherbereich und den Gesamtspeicherbereich für Ihren ausgewählten Speicherpool anzuzeigen, bewegen Sie den Mauszeiger über die Einträge in der Spalte 'Verwendete Kapazität'.</p> | <p>Um die Speicherpoolkapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie eine Zeile in der Tabelle 'Speicherpools' aus und klicken Sie auf Details.</p> |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|---|--|--|
| <p>9 Stellen Sie sicher, dass Speichereinheiten für Sicherungsoperationen verfügbar sind.</p> | <p>Überprüfen Sie im Bereich 'Speicher &amp; Datenverfügbarkeit' im Abschnitt 'Datenträger' unterhalb der Balken für die Kapazität den Status, der neben Einheiten angegeben ist. Wenn der Status Kritisch  oder Warnung  für eine Einheit angezeigt wird, müssen Sie das Problem untersuchen. Um Details anzuzeigen, klicken Sie auf Einheiten.</p> | <p>Platteneinheiten können aus den folgenden Gründen den Status 'Kritisch' oder 'Warnung' haben:</p> <ul style="list-style-type: none"> <li>• Für Einheitenklassen DISK können Datenträger offline sein oder den Zugriffsstatus READONLY (Lesezugriff) haben. In der Spalte 'Plattenspeicher' der Tabelle 'Platteneinheiten' wird der Status der Datenträger angezeigt.</li> <li>• Für nicht gemeinsam genutzte Einheitenklassen FILE können Verzeichnisse offline sein. Außerdem ist unter Umständen nicht genügend freier Speicherbereich für die Zuordnung von Arbeitsdatenträgern verfügbar. In der Spalte 'Plattenspeicher' der Tabelle 'Platteneinheiten' wird der Status der Verzeichnisse angezeigt.</li> <li>• Für gemeinsam genutzte Einheitenklassen FILE sind Laufwerke unter Umständen nicht verfügbar. Ein Laufwerk ist nicht verfügbar, wenn es offline ist, während der Antwort an den Server gestoppt wurde oder sein Pfad offline ist. In anderen Spalten der Tabelle 'Platteneinheiten' wird der Status der Laufwerke und Pfade angezeigt.</li> </ul> |

## Prüfliste für regelmäßige Überwachungstasks

Um sicherzustellen, dass Ihre IBM Spectrum Protect-Lösung ordnungsgemäß funktioniert, führen Sie die Tasks in der Prüfliste für regelmäßige Überwachungstasks aus. Planen Sie regelmäßige Tasks häufig genug, sodass Sie potenzielle Probleme erkennen können, bevor diese wirklich problematisch werden.




Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen  und klicken Sie auf Command Builder.







Tabelle 1. Regelmäßige Überwachungstasks

| Task | Basisprozeduren | Erweiterte Prozeduren und Fehlerbehebung |
|------|-----------------|--|
|------|-----------------|--|

| Task                                      | Basisprozeduren   | Erweiterte Prozeduren und Fehlerbehebung  |
|---|---|---|
| <p>Überwachen Sie die Systemleistung.</p> | <p>Bestimmen Sie den für Clientsicherungsoperationen erforderlichen Zeitraum:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients. Suchen Sie den Server, der dem Client zugeordnet ist.</li> <li>2. Klicken Sie auf Server. Wählen Sie den Server aus und klicken Sie auf Details.</li> <li>3. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die in den letzten 24 Stunden abgeschlossen wurden, klicken Sie auf Abgeschlossene Tasks.</li> <li>4. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die vor mehr als 24 Stunden abgeschlossen wurden, verwenden Sie den Befehl QUERY ACTLOG. Führen Sie die Anweisungen in QUERY ACTLOG (Aktivitätenprotokoll abfragen) aus.</li> <li>5. Wenn die Dauer von Clientsicherungsoperationen zunimmt, ohne dass ein offensichtlicher Grund erkennbar ist, überprüfen Sie Ursache.</li> </ol> <p>Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie Leistungsprobleme für den Client für Sichern/Archivieren diagnostizieren, indem Sie die folgenden Schritte ausführen:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients.</li> <li>2. Wählen Sie einen Client für Sichern/Archivieren aus und klicken Sie auf Details.</li> <li>3. Um Clientprotokolle abzurufen, klicken Sie auf Diagnose.</li> </ol> | <p>Informationen zur Verkürzung der Zeit, die der Client zum Sichern von Daten auf dem Server benötigt, finden Sie in Häufig auftretende Clientleistungsprobleme lösen.</p> <p>Suchen Sie nach Leistungsengpässen. Anweisungen finden Sie in Leistungsengpässe identifizieren.</p> <p>Informationen zur Identifikation und Behebung anderer Leistungsprobleme finden Sie in Leistung.</p> |


| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung   |
|---|--|--|
| <p>Bestimmen Sie die Platteneinsparungen, die durch die Datendeduplizierung bereitgestellt werden.</p>                                  | <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf Pools.</li> <li>2. Wählen Sie einen Pool aus und klicken Sie auf Kurzübersicht.</li> <li>3. Zeigen Sie im Bereich 'Datendeduplizierung' die Zeile 'Eingesparter Speicherbereich' an.</li> </ol>   | <p>Um für die erweiterte Überwachung detaillierte Statistikdaten zu dem Datendeduplizierungsprozess für einen bestimmten Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool abzurufen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>2. Fordern Sie einen Statistikbericht an, indem Sie den Befehl GENERATE DEDUPSTATS ausgeben. Führen Sie die Anweisungen in GENERATE DEDUPSTATS (Datendeduplizierungsstatistikdaten für einen Verzeichniscontainerspeicherpool generieren) aus.</li> <li>3. Zeigen Sie den Statistikbericht an, indem Sie den Befehl QUERY DEDUPSTATS ausgeben. Führen Sie die Anweisungen in QUERY DEDUPSTATS (Datendeduplizierungsstatistikdaten abfragen) aus.</li> </ol> |
| <p>Stellen Sie sicher, dass aktuelle Sicherungsdateien für Einheitenkonfigurations- und Datenträgerprotokolldaten gesichert werden.</p> | <p>Greifen Sie auf Ihre Speicherpositionen zu, um sicherzustellen, dass die Dateien verfügbar sind. Die bevorzugte Methode ist die Sicherung der Dateien an zwei Positionen.</p> <p>Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>2. Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, geben Sie die folgenden Befehle aus: <pre>query option volhistory query option devconfig</pre> </li> <li>3. Überprüfen Sie in der Ausgabe die Spalte 'Optionseinstellung', um die Dateipositionen zu finden.</li> </ol> <p>Wenn ein Katastrophenfall eintritt, sind sowohl die Protokolldatei für Datenträger als auch die Einheitenkonfigurationsdatei für die Zurückschreibung der Serverdatenbank erforderlich.</p> |  |






| Task   | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung |
|--|--|--|
| <p>Bestimmen Sie, ob für das Instanzverzeichnisdateisystem genügend Speicherbereich verfügbar ist.</p> | <p>Stellen Sie sicher, dass im Instanzverzeichnisdateisystem mindestens 20 % freier Speicherbereich verfügbar ist. Führen Sie die für Ihr Betriebssystem zutreffende Aktion aus:</p> <ul style="list-style-type: none"> <li>•  <b>AIX-Betriebssysteme</b> Um den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus: <pre>df -g Instanzverzeichnis</pre> <p>Dabei gibt <i>Instanzverzeichnis</i> das Instanzverzeichnis an.</p> </li> <li>•  <b>Linux-Betriebssysteme</b> Um den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus: <pre>df -h Instanzverzeichnis</pre> <p>Dabei gibt <i>Instanzverzeichnis</i> das Instanzverzeichnis an.</p> </li> <li>•  <b>Windows-Betriebssysteme</b> Klicken Sie in Windows-Explorer mit der rechten Maustaste auf das Dateisystem und klicken Sie auf Eigenschaften. Zeigen Sie die Kapazitätsdaten an.</li> </ul> <p>Die bevorzugte Position des Instanzverzeichnisses ist von dem Betriebssystem abhängig, unter dem der Server installiert ist:</p> <ul style="list-style-type: none"> <li>•  <b>AIX-Betriebssysteme</b></li> <li>•  <b>Linux-Betriebssysteme</b><br/>/home/tsminst1/tsminst1</li> <li>•  <b>Windows-Betriebssysteme</b><br/>C:\tsminst1</li> </ul> <p>Tipp: Wenn Sie ein Arbeitsblatt zur Planung ausgefüllt haben, ist die Position des Instanzverzeichnisses im Arbeitsblatt vermerkt.</p> |  |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung  |
|---|--|---|
| <p>Ermitteln Sie nicht erwartete Clientaktivität.</p> | <p>Um im Rahmen der Überwachung der Clientaktivität zu bestimmen, ob das Datenvolumen das erwartete Volumen überschreitet, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Clients'.</li> <li>2. Um die Aktivität der vergangen zwei Wochen anzuzeigen, doppelklicken Sie auf einen beliebigen Client.</li> <li>3. Um die Anzahl Byte anzuzeigen, die an den Client gesendet wurden, klicken Sie auf die Registerkarte Merkmale.</li> <li>4. Zeigen Sie im Bereich 'Letzte Sitzung' die Zeile 'An Client gesendet' an.</li> </ol> | <p>Wenn Sie auf einen Client in der Tabelle 'Clients' doppelklicken, wird im Bereich Aktivität im Lauf von 2 Wochen das Datenvolumen angezeigt, das vom Client jeden Tag an den Server gesendet wurde.</p> <p>Überprüfen Sie in regelmäßigen Abständen die SQL-Aktivitätsübersichtstabelle, die statistische Daten zu Clientsitzungen enthält. Um die aktuelle Aktivität mit der vorherigen Aktivität zu vergleichen, verwenden Sie eine Anweisung SQL SELECT. Wenn der Grad an Aktivität sich deutlich von dem für die vorherige Aktivität unterscheidet, kann dies eine Ransomware-Attacke anzeigen.</p> <p>Überprüfen Sie das Aktivitätenprotokoll in regelmäßigen Abständen. Suchen Sie nach ANE-Nachrichten, die angeben, wie viele Dateien gesichert und überprüft wurden. Vergleichen Sie die aktuellen Dateneduplizierungsraten mit den vorherigen Raten. Wenn eine ungewöhnlich hohe Anzahl Dateien gesichert wurde oder die Dateneduplizierungsrate wider Erwarten auf 0 fällt, kann dies eine Ransomware-Attacke anzeigen.</p> |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung  |
|---|--|---|
| <p>Überwachen Sie das Speicherpoolwachstum im Laufe der Zeit.</p> | <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Pools'.</li> <li>2. Um die Kapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie einen Pool aus und klicken Sie auf Details.</li> </ol> | <p>Tipps:</p> <ul style="list-style-type: none"> <li>• Um die Zeit anzugeben, die verstreichen muss, bevor alle deduplizierten Speicherbereiche aus einem Verzeichniscontainerspeicherpool oder einem Cloud-Containerspeicherpool entfernt werden, nachdem sie nicht mehr vom Bestand referenziert werden, führen Sie die folgenden Schritte aus: <ol style="list-style-type: none"> <li>1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus.</li> <li>2. Klicken Sie auf Details &gt; Merkmale.</li> <li>3. Geben Sie im Feld <code>Verzögerungszeitraum für Containerwiederverwendung</code> den Zeitraum an.</li> </ol> </li> <li>• Bestimmen Sie die Dateneduplizierungsleistung für Verzeichniscontainer- und Cloud-Containerspeicherpools mithilfe des Befehls <code>GENERATE DEDUPSTATS</code>.</li> <li>• Um Deduplizierungsstatistikdaten für einen Speicherpool anzuzeigen, führen Sie die folgenden Schritte aus: <ol style="list-style-type: none"> <li>1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus.</li> <li>2. Klicken Sie auf Details &gt; Merkmale.</li> </ol> </li> </ul> <p>Verwenden Sie dementsprechend den Befehl <code>QUERY EXTENTUPDATES</code>, um Informationen zu Aktualisierungen an Datenbereichen in Verzeichniscontainer- oder Cloud-Containerspeicherpools anzuzeigen. Anhand der Befehlsausgabe können Sie die Datenbereiche bestimmen, die nicht mehr referenziert werden, sowie die Datenbereiche, die zum Löschen vom System auswählbar sind. Überwachen Sie in der Ausgabe die Anzahl Datenbereiche, die zum Löschen vom System auswählbar sind. Diese Messgröße steht in direkten Zusammenhang mit dem Umfang des freien Speicherbereichs in dem Containerspeicherpool.</p> <ul style="list-style-type: none"> <li>• Um den Umfang des physischen Speicherbereichs anzuzeigen, der von einem Dateibereich nach dem Entfernen der Dateneduplizierungseinsparungen belegt wird, verwenden Sie den Befehl <code>select * from occupancy</code>. Die Befehlsausgabe umfasst den Wert für <code>LOGICAL_MB</code>. <code>LOGICAL_MB</code> gibt an, wie viel Speicherbereich von diesem Dateibereich belegt wird.</li> </ul> |

| Task   | Basisprozeduren   | Erweiterte Prozeduren und Fehlerbehebung   |
|--|---|--|
| Werten Sie das Timing von Clientzeitplänen aus. Stellen Sie sicher, dass die Start- und Endzeiten von Clientzeitplänen Ihre Geschäftsanforderungen erfüllen. | <p>Klicken Sie auf der Seite Übersicht im Operations Center auf Clients &gt; Zeitpläne.</p> <p>In der Tabelle 'Zeitpläne' wird in der Spalte 'Start' die konfigurierte Startzeit für die geplante Operation angezeigt. Um anzuzeigen, wann die letzte Operation gestartet wurde, bewegen Sie den Mauszeiger über das Uhrsymbol.</p> | <p>Tipp: Wenn die Ausführung einer Clientoperation länger als erwartet dauert, empfangen Sie unter Umständen eine Warnung. Führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite 'Übersicht' im Operations Center den Mauszeiger über Clients und klicken Sie auf Zeitpläne.</li> <li>2. Wählen Sie einen Zeitplan aus und klicken Sie auf Details.</li> <li>3. Zeigen Sie die Details eines Zeitplans an, indem Sie auf den blauen Pfeil neben der Zeile klicken.</li> <li>4. Geben Sie im Feld Ausführungszeitalter die Uhrzeit an, zu der eine Warnung ausgegeben wird, wenn die geplante Operation nicht ausgeführt wird.</li> <li>5. Klicken Sie auf Sichern.</li> </ol> |
| Werten Sie das Timing von Verwaltungstasks aus. Stellen Sie sicher, dass die Start- und Endzeiten von Verwaltungstasks Ihre Geschäftsanforderungen erfüllen. | <p>Klicken Sie auf der Seite Übersicht im Operations Center auf Server &gt; Verwaltung.</p> <p>Überprüfen Sie in der Tabelle 'Verwaltung' die Informationen in der Spalte 'Letzte Ausführungsdauer'. Um anzuzeigen, wann die letzte Verwaltungstask gestartet wurde, bewegen Sie den Mauszeiger über das Uhrsymbol.</p>             | <p>Tipp: Wenn die Ausführung einer Verwaltungstask zu lange dauert, ändern Sie die Startzeit oder die maximale Ausführungszeit. Führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>2. Um die Startzeit oder die maximale Ausführungszeit für eine Task zu ändern, geben Sie den Befehl UPDATE SCHEDULE aus. Anweisungen finden Sie in UPDATE SCHEDULE (Clientzeitplan aktualisieren).</li> </ol>   |

**Zugehörige Verweise:**

-  QUERY ACTLOG (Aktivitätenprotokoll abfragen)
-  UPDATE STGPOOL (Speicherpool aktualisieren)
-  QUERY EXTENTUPDATES (Aktualisierte Datenbereiche abfragen)

## Lizenzeinhaltung überprüfen

Stellen Sie sicher, dass die Bedingungen Ihrer Lizenzvereinbarung von Ihrer IBM Spectrum Protect-Lösung eingehalten werden. Indem die Einhaltung regelmäßig überprüft wird, können Sie Trends beim Datenwachstum oder der PVU-Nutzung verfolgen. Planen Sie anhand dieser Informationen den weiteren Kauf von Lizenzen.

### Informationen zu diesem Vorgang

Die Methode zur Überprüfung der Einhaltung der Lizenzbedingungen durch Ihre Lösung variiert abhängig von den Bedingungen Ihrer IBM Spectrum Protect-Lizenzvereinbarung.

**Front-End-Kapazitätslizenzierung**

Das Front-End-Modell bestimmt die Lizenzvoraussetzungen auf der Basis des zurückgemeldeten Volumens an primären Daten, das von Clients gesichert wird. Clients umfassen Anwendungen, virtuelle Maschinen und Systeme.

**Back-End-Kapazitätslizenzierung**

Das Back-End-Modell bestimmt Lizenzvoraussetzungen auf der Basis der Terabyte Daten, die in primären Speicherpools und Repositories gespeichert werden.

Tipps:

- Um die Genauigkeit von Schätzungen der Front-End- und Back-End-Kapazität zu gewährleisten, installieren Sie die neueste Version der Client-Software auf jedem Clientknoten.
- Die Informationen zur Front-End- und Back-End-Kapazität im Operations Center dienen zum Zweck der Planung und Schätzung.

**PVU-Lizenzierung**



Das PVU-Modell basiert auf der Nutzung von PVUs durch Servereinheiten.

Wichtig: Die von IBM Spectrum Protect bereitgestellten PVU-Berechnungen werden als Schätzungen betrachtet und sind nicht rechtsverbindlich. Die von IBM Spectrum Protect zurückgemeldeten PVU-Lizenzinformationen werden nicht als zulässiger Ersatz für das IBM® License Metric Tool angesehen.

Die neuesten Informationen zu Lizenzierungsmodellen finden Sie in den Informationen zu Produktdetails und Lizenzen auf der Website der IBM Spectrum Protect-Produktfamilie. Wenden Sie sich bei Fragen oder Problemstellungen zu Lizenzierungsanforderungen an Ihren IBM Spectrum Protect-Software-Provider.

## Vorgehensweise

Führen Sie zur Überwachung der Lizenz Einhaltung die Schritte aus, die den Bedingungen Ihrer Lizenzvereinbarung entsprechen. Tipp: Das Operations Center stellt einen E-Mail-Bericht bereit, in dem die Front-End- und Back-End-Kapazitätsnutzung zusammengefasst sind. Berichte können automatisch regelmäßig an einen oder mehrere Empfänger gesendet werden. Klicken Sie für die Konfiguration und Verwaltung von E-Mail-Berichten in der Menüleiste des Operations Center auf Berichte.

| Option                  | Bezeichnung   |
|-------------------------|---|
| <b>Front-End-Modell</b> | <p>a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen  und klicken Sie auf Lizenzierung.</p> <p>Die Schätzung der Front-End-Kapazität wird auf der Seite 'Front-End-Nutzung' angezeigt.</p> <p>b. Wenn in der Spalte 'Keine Zurückmeldung' ein Wert angezeigt wird, klicken Sie auf die Zahl, um Clients zu identifizieren, von denen keine Kapazitätsnutzung zurückgemeldet wurde.</p> <p>c. Um die Kapazität für Clients zu schätzen, für die keine Kapazitätsnutzung zurückgemeldet wurde, rufen Sie die folgende FTP-Site auf, auf der Tools und Anweisungen zum Messen der Kapazität bereitgestellt werden:</p> <p><code>ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools</code></p> <p>Um die Front-End-Kapazität mithilfe eines Scripts zu messen, führen Sie die Anweisungen im aktuellen Lizenzierungshandbuch aus.</p> <p>d. Addieren Sie den Operations Center-Schätzwert und alle Schätzwerte, die Sie mithilfe eines Scripts ermittelt haben.</p> <p>e. Überprüfen Sie, ob die geschätzte Kapazität die Bedingungen Ihrer Lizenzvereinbarung einhält.</p> |
| <b>Back-End-Modell</b>  | <p>Einschränkung: Wenn der Quellen- und der Zielreplikationsserver nicht dieselben Maßnahmeneinstellungen verwenden, können Sie das Operations Center nicht zur Überwachung der Back-End-Kapazitätsnutzung für replizierte Clients verwenden. Informationen zur Schätzung der Kapazitätsnutzung für diese Clients finden Sie in Technote 1656476.</p> <p>a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen  und klicken Sie auf Lizenzierung.</p> <p>b. Klicken Sie auf die Registerkarte Back-End.</p> <p>c. Überprüfen Sie, ob das geschätzte Datenvolumen die Bedingungen Ihrer Lizenzvereinbarung einhält.</p>   |
| <b>PVU-Modell</b>       | Informationen zur Vorgehensweise beim Prüfen der Einhaltung der PVU-Lizenzbedingungen finden Sie in Einhaltung des PVU-Lizenzierungsmodells prüfen.   |

## Systemstatus mithilfe von E-Mail-Berichten verfolgen

Konfigurieren Sie das Operations Center für die Generierung von E-Mail-Berichten zur Zusammenfassung des Systemstatus. Sie können eine Mail-Server-Verbindung konfigurieren, Berichtseinstellungen ändern und wahlweise angepasste SQL-Berichte erstellen.

## Vorbereitende Schritte

Bevor Sie E-Mail-Berichte konfigurieren, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- Es ist ein SMTP-Host-Server (SMTP = Simple Mail Transfer Protocol) verfügbar, um Berichte als E-Mail senden und empfangen zu können. Der SMTP-Server muss als offenes Mail-Relay konfiguriert sein. Außerdem müssen Sie sicherstellen, dass der IBM Spectrum Protect-Server, der E-Mail-Nachrichten sendet, Zugriff auf den SMTP-Server hat. Wenn das Operations Center auf einem anderen Computer installiert ist, ist für diesen Computer kein Zugriff auf den SMTP-Server erforderlich.
- Um E-Mail-Berichte konfigurieren zu können, müssen Sie über Systemberechtigung für den Server verfügen.

- Um die Empfänger anzugeben, können Sie eine oder mehrere E-Mail-Adressen oder Administrator-IDs eingeben. Wenn eine Administrator-ID eingegeben werden soll, muss die ID auf dem Hub-Server registriert sein und der ID muss eine E-Mail-Adresse zugeordnet sein. Eine E-Mail-Adresse für einen Administrator können Sie mithilfe des Parameters EMAILADDRESS im Befehl UPDATE ADMIN angeben.

## Informationen zu diesem Vorgang

---

Sie können das Operations Center zum Senden eines Berichts über allgemeine Operationen, eines Lizenz eingehaltsberichts und eines oder mehrerer angepasster Berichte, die SQL-Anweisungen SELECT zum Abfragen verwalteter Server verwenden, konfigurieren.

## Vorgehensweise

---

Um E-Mail-Berichte zu konfigurieren und zu verwalten, führen Sie die folgenden Schritte aus:


1. Klicken Sie in der Menüleiste des Operations Center auf Berichte.
2. Wenn noch keine E-Mail-Server-Verbindung konfiguriert ist, klicken Sie auf Mail-Server konfigurieren und füllen Sie die Felder aus. Nach der Konfiguration des Mail-Servers sind der Bericht über allgemeine Operationen und der Lizenz eingehaltsbericht aktiviert.
3. Um Berichtseinstellungen zu ändern, wählen Sie einen Bericht aus, klicken Sie auf Details und aktualisieren Sie das Formular.
4. Optional: Um einen angepassten SQL-Bericht hinzuzufügen, klicken Sie auf + Bericht und füllen Sie die Felder aus.  
Tipp: Um einen Bericht sofort auszuführen und zu senden, wählen Sie den Bericht aus und klicken Sie auf Senden.

## Ergebnisse

---

Aktivierte Berichte werden gemäß den angegebenen Einstellungen gesendet.

### Zugehörige Verweise:

 UPDATE ADMIN (Administrator aktualisieren)

## Operationen für eine Plattenspeicherlösung für einen einzelnen Standort verwalten

---

Verwenden Sie diese Informationen, um Operationen für eine Plattenspeicherlösung für einen einzelnen Standort mit IBM Spectrum Protect zu verwalten, die einen Server umfasst und Datenduplizierung für einen einzelnen Standort verwendet.

- **Operations Center verwalten**  
Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt.
- **Anwendungen, virtuelle Maschinen und Systeme schützen**  
Der Server schützt Daten für Clients, die Anwendungen, virtuelle Maschinen und Systeme umfassen können. Um Clientdaten schützen zu können, müssen Sie den Clientknoten beim Server registrieren und einen Sicherungszeitplan zum Schützen der Clientdaten auswählen.
- **Datenspeicher verwalten**  
Verwalten Sie Ihre Daten effizient und fügen Sie dem Server unterstützte Einheiten und Datenträger zum Speichern von Clientdaten hinzu.
- **IBM Spectrum Protect-Server schützen**  
Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.
- **Server stoppen und starten**  
Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.
- **Durchführung eines Upgrades für den Server planen**  
Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.
- **Vorbereitungen für einen Ausfall oder eine Systemaktualisierung**  
Treffen Sie Vorbereitungen in IBM Spectrum Protect, damit Ihr System während eines geplanten Stromausfalls oder einer geplanten Systemaktualisierung in einem konsistenten Zustand verbleibt.
- **Plan zur Wiederherstellung nach einem Katastrophenfall implementieren**  
Implementieren Sie eine Strategie zur Wiederherstellung nach einem Katastrophenfall, um Ihre Anwendungen in einem Katastrophenfall wiederherstellen und hohe Serververfügbarkeit sicherstellen zu können.

- Wiederherstellung nach einem Systemausfall  
Bei IBM Spectrum Protect-Plattenspeicherlösungen für einen einzelnen Standort können Sie den Bestand nur lokal wiederherstellen und die Datenbank zum Schutz Ihrer Daten zurückschreiben.

## Operations Center verwalten

---

Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt.

- Peripherieserver hinzufügen und entfernen  
In einer Umgebung mit mehreren Servern können Sie dem Hub-Server die anderen Server, die als *Peripherieserver* bezeichnet werden, hinzufügen.
- Web-Server starten und stoppen  
Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Unter Umständen müssen Sie den Web-Server stoppen und starten, um beispielsweise Konfigurationsänderungen durchzuführen.
- Assistenten für die Erstkonfiguration erneut starten  
Unter Umständen müssen Sie den Assistenten für die Erstkonfiguration im Operations Center erneut starten, um beispielsweise Konfigurationsänderungen durchzuführen.
- Hub-Server ändern  
Mithilfe des Operations Center können Sie den Hub-Server von IBM Spectrum Protect entfernen und einen anderen Hub-Server konfigurieren.
- Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben  
Wenn bestimmte Probleme auftreten, möchten Sie möglicherweise die Operations Center-Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben, bei dem die IBM Spectrum Protect-Server nicht als Hub- oder Peripherieserver definiert sind.

## Peripherieserver hinzufügen und entfernen

---

In einer Umgebung mit mehreren Servern können Sie dem Hub-Server die anderen Server, die als *Peripherieserver* bezeichnet werden, hinzufügen.

### Informationen zu diesem Vorgang

---

Die Peripherieserver senden Alerts und Statusinformationen an den Hub-Server. Das Operations Center zeigt eine konsolidierte Sicht der Alerts und Statusinformationen für den Hub-Server und alle Peripherieserver.

- Peripherieserver hinzufügen  
Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server einen oder mehrere Peripherieserver hinzufügen.
- Peripherieserver entfernen  
Sie können einen Peripherieserver aus dem Operations Center entfernen.

## Peripherieserver hinzufügen

---

Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server einen oder mehrere Peripherieserver hinzufügen.

### Vorbereitende Schritte

---

Die Kommunikation zwischen dem Peripherieserver und dem Hub-Server muss unter Verwendung des Protokolls Transport Layer Security (TLS) geschützt werden. Um die Kommunikation zu schützen, fügen Sie das Zertifikat des Peripherieservers der Truststore-Datei des Hub-Servers hinzu.

### Vorgehensweise

---

1. Klicken Sie in der Menüleiste des Operations Center auf Server. Die Seite Server wird geöffnet.

In der Tabelle auf der Seite Server könnte ein Server den Status "Nicht überwacht" haben. Dieser Status bedeutet, dass - obwohl ein Administrator diesen Server mit dem Befehl DEFINE SERVER für den Hub-Server definiert hat - der Server noch nicht als Peripherieserver konfiguriert ist.

2. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf den Server, um ihn hervorzuheben, und klicken Sie in der Menüleiste der Tabelle auf Peripherieserver überwachen.
  - Wenn der Server, der hinzugefügt werden soll, in der Tabelle nicht angezeigt wird und die sichere SSL-/TLS-Kommunikation nicht erforderlich ist, klicken Sie in der Menüleiste der Tabelle auf +Peripherieserver.
3. Geben Sie die erforderlichen Informationen an und führen Sie die Schritte im Konfigurationsassistenten für den Peripherieserver aus.
- Tipp: Wenn der Aufbewahrungszeitraum für Ereignissätze des Servers weniger als 14 Tage beträgt, wird der Zeitraum automatisch auf 14 Tage zurückgesetzt, wenn Sie den Server als Peripherieserver konfigurieren.

## Peripherieserver entfernen

---

Sie können einen Peripherieserver aus dem Operations Center entfernen.

### Informationen zu diesem Vorgang

---

Unter Umständen müssen Sie einen Peripherieserver in den folgenden Situationen entfernen:

- Der Peripherieserver soll von einem Hub-Server auf einen anderen Hub-Server versetzt werden.
- Der Peripherieserver soll stillgelegt werden.

### Vorgehensweise

---

Um den Peripherieserver aus der Gruppe der Server zu entfernen, die vom Hub-Server verwaltet werden, führen Sie die folgenden Schritte aus:

1. Geben Sie in der IBM Spectrum Protect-Befehlszeile auf dem Hub-Server den folgenden Befehl aus:

```
QUERY MONITORSETTINGS
```

2. Kopieren Sie in der Ausgabe des Befehls den Namen im Feld Überwachte Gruppe.
3. Geben Sie auf dem Hub-Server den folgenden Befehl aus; dabei ist *Gruppenname* der Name der überwachten Gruppe und *Mitgliedsname* der Name des Peripherieservers:

```
DELETE GRPMEMBER Gruppenname Mitgliedsname
```

4. Optional: Wenn der Peripherieserver von einem Hub-Server auf einen anderen Hub-Server versetzt werden soll, dürfen Sie diesen Schritt **nicht** ausführen. Andernfalls können Sie die Alertausgabe und Überwachung auf dem Peripherieserver inaktivieren, indem Sie auf dem Peripherieserver die folgenden Befehle ausgeben:

```
SET STATUSMONITOR OFF
SET ALERTMONITOR OFF
```

5. Optional: Wenn die Definition des Peripherieservers für andere Zwecke verwendet wird, wie beispielsweise unternehmensweite Konfiguration, Befehlsweiterleitung, Speichern virtueller Datenträger oder Speicherarchivverwaltung, dürfen Sie diesen Schritt **nicht** ausführen. Andernfalls können Sie die Definition des Peripherieservers auf dem Hub-Server löschen, indem Sie auf dem Hub-Server den folgenden Befehl ausgeben:

```
DELETE SERVER Name_des_Peripherieservers
```

Tipp: Wenn eine Serverdefinition sofort nach dem Entfernen des Servers aus der überwachten Gruppe gelöscht wird, können Statusinformationen für den Server ohne zeitliche Begrenzung im Operations Center verbleiben.

Um dieses Problem zu verhindern, warten Sie, bis das Intervall für die Erfassung von Statusdaten überschritten wurde, bevor Sie die Serverdefinition löschen. Das Intervall für die Erfassung von Statusdaten wird auf der Seite 'Einstellungen' des Operations Center angezeigt.


## Web-Server starten und stoppen

---

Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Unter Umständen müssen Sie den Web-Server stoppen und starten, um beispielsweise Konfigurationsänderungen durchzuführen.


### Vorgehensweise

---

1. Stoppen Sie den Web-Server.
  -  AIX-Betriebssysteme Geben Sie im Verzeichnis */Installationsverzeichnis/ui/utls* (dabei gibt *Installationsverzeichnis* das Verzeichnis an, in dem das Operations Center installiert ist) den folgenden Befehl aus:




```
./stopserver.sh
```

-  Linux-Betriebssysteme Geben Sie den folgenden Befehl aus:


```
service opscenter.rc stop
```

-  Windows-Betriebssysteme Stoppen Sie den Dienst IBM Spectrum Protect Operations Center im Fenster Dienste.

## 2. Starten Sie den Web-Server.

-  AIX-Betriebssysteme Geben Sie im Verzeichnis */Installationsverzeichnis/ui/utls* (dabei gibt *Installationsverzeichnis* das Verzeichnis an, in dem das Operations Center installiert ist) den folgenden Befehl aus:

```
./startserver.sh
```

-  Linux-Betriebssysteme Geben Sie die folgenden Befehle aus:

Starten Sie den Server:

```
service opscenter.rc start
```

Starten Sie den Server erneut:

```
service opscenter.rc restart
```

Bestimmen Sie, ob der Server aktiv ist:

```
service opscenter.rc status
```

-  Windows-Betriebssysteme Starten Sie den Dienst IBM Spectrum Protect Operations Center im Fenster Dienste.

## Assistenten für die Erstkonfiguration erneut starten

---

Unter Umständen müssen Sie den Assistenten für die Erstkonfiguration im Operations Center erneut starten, um beispielsweise Konfigurationsänderungen durchzuführen.

### Vorbereitende Schritte

---

Um die folgenden Einstellungen zu ändern, verwenden Sie die Seite Einstellungen im Operations Center, anstatt den Assistenten für die Erstkonfiguration erneut zu starten:

- Häufigkeit, mit der Statusdaten aktualisiert werden
- Dauer, die Alerts aktiv, inaktiv oder geschlossen bleiben
- Bedingungen, die angeben, dass Clients gefährdet sind

Die Hilfe des Operations Center enthält weitere Informationen zum Ändern dieser Einstellungen.







### Informationen zu diesem Vorgang

---

Um den Assistenten für die Erstkonfiguration erneut zu starten, müssen Sie eine Merkmaldatei löschen, die Informationen zur Hub-Server-Verbindung enthält. Alle für den Hub-Server konfigurierten Einstellungen für Alertausgabe, Überwachung oder Gefährdung bzw. serverübergreifenden Einstellungen werden nicht gelöscht. Diese Einstellungen werden als Standardeinstellungen im Konfigurationsassistenten verwendet, wenn der Assistent erneut gestartet wird.

### Vorgehensweise

---

1. Stoppen Sie den Web-Server des Operations Center.
  2. Wechseln Sie auf dem Computer, auf dem das Operations Center installiert ist, in das folgende Verzeichnis (dabei ist *Installationsverzeichnis* das Verzeichnis, in dem das Operations Center installiert ist):
    -  AIX-Betriebssysteme  Linux-Betriebssysteme *Installationsverzeichnis/ui/Liberty/usr/servers/guiServer*
    -  Windows-Betriebssysteme *Installationsverzeichnis\ui\Liberty\usr\servers\guiServer*
- Beispiel:
-  AIX-Betriebssysteme  Linux-Betriebssysteme */opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer*
  -  Windows-Betriebssysteme *c:\Programme\Tivoli\TSM\ui\Liberty\usr\servers\guiServer*
3. Löschen Sie im Verzeichnis *guiServer* die Datei *serverConnection.properties*.
  4. Starten Sie den Web-Server des Operations Center.
  5. Öffnen Sie das Operations Center.
  6. Rekonfigurieren Sie mithilfe des Konfigurationsassistenten das Operations Center. Geben Sie ein neues Kennwort für die Überwachungsadministrator-ID an.

7. Aktualisieren auf jedem Peripherieserver, der bereits zuvor mit dem Hub-Server verbunden war, das Kennwort für die Überwachungsadministrator-ID, indem Sie den folgenden Befehl in der IBM Spectrum Protect-Befehlszeilenschnittstelle ausgeben:

```
UPDATE ADMIN IBM-OC-Name_des_Hub-Servers neues_Kennwort
```

Einschränkung: Übernehmen Sie alle anderen Einstellungen für diese Administrator-ID unverändert. Nachdem Sie das Anfangskennwort angegeben haben, wird dieses Kennwort automatisch vom Operations Center verwaltet.

## Hub-Server ändern

---

Mithilfe des Operations Center können Sie den Hub-Server von IBM Spectrum Protect entfernen und einen anderen Hub-Server konfigurieren.

### Vorgehensweise

---

1. Starten Sie den Assistenten für die Erstkonfiguration des Operations Center erneut. Im Rahmen dieser Prozedur löschen Sie die bestehende Hub-Server-Verbindung.
2. Verwenden Sie den Assistenten, um das Operations Center für die Verbindung zu dem neuen Hub-Server zu konfigurieren.

#### Zugehörige Tasks:

Assistenten für die Erstkonfiguration erneut starten

## Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben

---

Wenn bestimmte Probleme auftreten, möchten Sie möglicherweise die Operations Center-Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben, bei dem die IBM Spectrum Protect-Server nicht als Hub- oder Peripherieserver definiert sind.

### Vorgehensweise

---

Um die Konfiguration zurückzuschreiben, führen Sie die folgenden Schritte aus:

1. Stoppen Sie den Web-Server des Operations Center.
2. Dekonfigurieren Sie den Hub-Server, indem Sie die folgenden Schritte ausführen:

- a. Geben Sie auf dem Hub-Server die folgenden Befehle aus:

```
SET MONITORINGADMIN ""
SET MONITOREDSEVERGROUP ""
SET STATUSMONITOR OFF
SET ALERTMONITOR OFF
REMOVE ADMIN IBM-OC-Name_des_Hub-Servers
```

Tipp: *IBM-OC-Name\_des\_Hub-Servers* ist die Überwachungsadministrator-ID, die bei der Erstkonfiguration des Hub-Servers automatisch erstellt wurde.

- b. Setzen Sie das Kennwort für den Hub-Server zurück, indem Sie den folgenden Befehl auf dem Hub-Server ausgeben:

```
SET SERVERPASSWORD ""
```

Achtung: Führen Sie diesen Schritt nicht aus, wenn der Hub-Server für andere Server für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation konfiguriert ist.

3. Dekonfigurieren Sie alle Peripherieserver, indem Sie die folgenden Schritte ausführen:

  - a. Um zu bestimmen, ob noch Peripherieserver vorhanden sind, die als Mitglieder der Servergruppe definiert sind, geben Sie auf dem Hub-Server den folgenden Befehl aus:

```
QUERY SERVERGROUP IBM-OC-Name_des_Hub-Servers
```

Tipp: *IBM-OC-Name\_des\_Hub-Servers* ist der Name der überwachten Servergruppe, die bei der Konfiguration des ersten Peripherieservers automatisch erstellt wurde. Dieser Servergruppenname stimmt auch mit der Überwachungsadministrator-ID überein, die bei der Erstkonfiguration des Hub-Servers automatisch erstellt wurde.

- b. Um Peripherieserver aus der Servergruppe zu löschen, geben Sie auf dem Hub-Server für jeden Peripherieserver den folgenden Befehl aus:

```
DELETE GRPMEMBER IBM-OC-Name_des_Hub-Servers Name_des_Peripherieservers
```

- c. Nachdem alle Peripherieserver aus der Servergruppe gelöscht wurden, geben Sie auf dem Hub-Server die folgenden Befehle aus:

```
DELETE SERVERGROUP IBM-OC-Name_des_Hub-Servers
SET MONITOREDSEVERGROUP ""
```

d. Geben Sie auf jedem Peripherieserver die folgenden Befehle aus:

```
REMOVE ADMIN IBM-OC-Name_des_Hub-Servers
SETOPT PUSHSTATUS NO
SET ALERTMONITOR OFF
SET STATUSMONITOR OFF
```

e. Löschen Sie die Definition des Hub-Servers, indem Sie auf jedem Peripherieserver den folgenden Befehl ausgeben:

```
DELETE SERVER Name_des_Hub-Servers
```

Achtung: Führen Sie diesen Schritt nicht aus, wenn die Definition für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation verwendet wird.

f. Löschen Sie die Definition jedes Peripherieservers, indem Sie auf dem Hub-Server den folgenden Befehl ausgeben:

```
DELETE SERVER Name_des_Peripherieservers
```

Achtung: Führen Sie diesen Schritt nicht aus, wenn die Serverdefinition für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation verwendet wird.

4. Schreiben Sie die Standardeinstellungen auf jeden Server zurück, indem Sie die folgenden Befehle ausgeben:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Starten Sie den Assistenten für die Erstkonfiguration des Operations Center erneut.

#### Zugehörige Tasks:

Assistenten für die Erstkonfiguration erneut starten  
Web-Server starten und stoppen

## Anwendungen, virtuelle Maschinen und Systeme schützen

---

Der Server schützt Daten für Clients, die Anwendungen, virtuelle Maschinen und Systeme umfassen können. Um Clientdaten schützen zu können, müssen Sie den Clientknoten beim Server registrieren und einen Sicherungszeitplan zum Schützen der Clientdaten auswählen.

- Clients hinzufügen  
Nach der Implementierung einer Datenschutzlösung mit IBM Spectrum Protect können Sie die Lösung durch Hinzufügen von Clients erweitern.
- Clientoperationen verwalten  
Sie können Fehler, die einen Client für Sichern/Archivieren betreffen, mithilfe des Operations Center, das Vorschläge zur Behebung von Fehlern bereitstellt, auswerten und beheben. Bei Fehlern für andere Typen von Clients müssen Sie die Fehlerprotokolle auf dem Client überprüfen und in der Produktdokumentation nachlesen.
- Client-Upgrades verwalten  
Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.
- Clientknoten stilllegen  
Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.
- Daten zum Freigeben von Speicherbereich inaktivieren  
In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegebenen Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

## Clients hinzufügen

---

Nach der Implementierung einer Datenschutzlösung mit IBM Spectrum Protect können Sie die Lösung durch Hinzufügen von Clients erweitern.

## Informationen zu diesem Vorgang

---

Die Prozedur beschreibt grundlegende Schritte zum Hinzufügen eines Clients. Spezifischere Anweisungen zum Konfigurieren von Clients enthält die Dokumentation für das auf dem Clientknoten installierte Produkt. Folgende Typen von Clients können vorhanden sein:

### Anwendungsclientknoten

Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

### Systemclientknoten

Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

### VM-Clientknoten

Clientknoten virtueller Maschinen bestehen aus einem einzelnen Gasthost in einem Hypervisor. Jede virtuelle Maschine wird als ein Dateibereich dargestellt.

## Vorgehensweise

---

Um einen Client hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Wählen Sie die Software aus, die auf dem Clientknoten installiert werden soll, und planen Sie die Installation. Führen Sie die Anweisungen in Client-Software auswählen und Installation planen aus.
2. Geben Sie an, wie Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in Regeln zum Sichern und Archivieren von Clientdaten angeben aus.
3. Geben Sie an, wann Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in Sicherungs- und Archivierungsoperationen planen aus.
4. Um Clients das Herstellen einer Verbindung zum Server zu ermöglichen, registrieren Sie den Client. Führen Sie die Anweisungen in Clients registrieren aus.
5. Um einen Clientknoten zu schützen, installieren und konfigurieren Sie die ausgewählte Software auf dem Clientknoten. Führen Sie die Anweisungen in Clients installieren und konfigurieren aus.

## Client-Software auswählen und Installation planen

---

Unterschiedliche Typen von Daten erfordern unterschiedliche Typen von Schutz. Geben Sie den Typ der Daten an, die geschützt werden müssen, und wählen Sie die geeignete Software aus.

## Informationen zu diesem Vorgang

---

Das bevorzugte Verfahren ist die Installation des Clients für Sichern/Archivieren auf allen Clientknoten, sodass Sie den Clientakzeptor auf dem Clientknoten konfigurieren und starten können. Der Clientakzeptor ist für die effiziente Ausführung geplanter Operationen konzipiert.

Der Clientakzeptor führt Zeitpläne für die folgenden Produkte aus: Client für Sichern/Archivieren, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail und IBM Spectrum Protect for Virtual Environments. Wenn Sie ein Produkt installieren, für das der Clientakzeptor keine Zeitpläne ausführt, müssen Sie die Konfigurationsanweisungen in der Produktdokumentation ausführen, um sicherzustellen, dass geplante Operationen ausgeführt werden können.

## Vorgehensweise

---

Wählen Sie abhängig von Ihrer Zielsetzung die zu installierenden Produkte aus und lesen Sie die Installationsanweisungen. Tipp: Wenn Sie die Client-Software jetzt installieren, müssen Sie auch die in Clients installieren und konfigurieren beschriebenen Clientkonfigurationstasks ausführen, bevor Sie den Client verwenden können.

| Ziel | Produkt und Beschreibung | Installationsanweisungen |
|------|--------------------------|--------------------------|
|------|--------------------------|--------------------------|

| Ziel  | Produkt und Beschreibung  | Installationsanweisungen   |
|---|---|--|
| Schutz eines Dateiservers oder einer Workstation  | Der Client für Sichern/Archivieren sichert und archiviert Dateien und Verzeichnisse von Dateiservern und Workstations in Speicher. Es ist auch möglich, Sicherungsversionen und archivierte Kopien von Dateien zurückzuschreiben und abzurufen.   | <ul style="list-style-type: none"> <li>• Anforderungen für den Client für Sichern/Archivieren</li> <li>• UNIX- und Linux-Clients für Sichern/Archivieren installieren</li> <li>• Windows-Client für Sichern/Archivieren installieren</li> </ul>  |
| Schutz von Anwendungen mit Momentaufnahme sicherungs- und -zurückschreibungs funktionalität | IBM Spectrum Protect Snapshot schützt Daten mit integrierter anwendungsgesteuerter Momentaufnahmesicherungs- und -zurückschreibungs funktionalität. Sie können Daten schützen, die von IBM DB2-Datenbanksoftware sowie SAP-, Oracle-, Microsoft Exchange Server- und Microsoft SQL Server-Anwendungen gespeichert werden. | <ul style="list-style-type: none"> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen</li> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen</li> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen</li> </ul> |
| Schutz einer E-Mail-Anwendung auf einem IBM Domino-Server                                   | IBM Spectrum Protect for Mail: Data Protection for IBM® Domino automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass IBM Domino-Server heruntergefahren werden.  | <ul style="list-style-type: none"> <li>• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0)</li> <li>• Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0)</li> </ul>  |
| Schutz einer E-Mail-Anwendung auf einem Server mit Microsoft Exchange Server                | IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass Server mit Microsoft Exchange Server heruntergefahren werden.   | Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server   |
| Schutz einer IBM DB2-Datenbank  | Mithilfe der Anwendungsprogrammierschnittstelle (API) des Clients für Sichern/Archivieren können DB2-Daten auf dem IBM Spectrum Protect-Server gesichert werden.  | IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)  |
| Schutz einer IBM Informix-Datenbank   | Mithilfe der API des Clients für Sichern/Archivieren können Informix-Daten auf dem IBM Spectrum Protect-Server gesichert werden.  | IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)  |
| Schutz einer Microsoft SQL-Datenbank  | IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server schützt Microsoft SQL-Daten.   | Data Protection for SQL Server unter Windows Server Core installieren  |
| Schutz einer Oracle-Datenbank   | IBM Spectrum Protect for Databases: Data Protection for Oracle schützt Oracle-Daten.  | Installation von Data Protection for Oracle  |
| Schutz einer SAP-Umgebung   | IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP stellt Schutz bereit, der für SAP-Umgebungen angepasst ist. Das Produkt dient der Verbesserung der Verfügbarkeit von SAP-Datenbankservern und der Verringerung des Verwaltungsaufwands.  | <ul style="list-style-type: none"> <li>• IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 installieren</li> <li>• IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle installieren</li> </ul>  |

| Ziel                             | Produkt und Beschreibung   | Installationsanweisungen   |
|----------------------------------|--|--|
| Schutz einer virtuellen Maschine | <p>IBM Spectrum Protect for Virtual Environments stellt Schutz bereit, der für virtuelle Microsoft Hyper-V- und VMware-Umgebungen angepasst ist. Mithilfe von IBM Spectrum Protect for Virtual Environments können Sie immer inkrementelle Sicherungen erstellen, die auf einem zentralen Server gespeichert werden, Sicherungsmaßnahmen erstellen und virtuelle Maschinen oder einzelne Dateien zurückschreiben.</p> <p>Sie können auch stattdessen den Client für Sichern/Archivieren zum Sichern und Zurückschreiben einer vollständigen virtuellen VMware- oder Microsoft Hyper-V-Maschine verwenden. Es ist auch möglich, Dateien oder Verzeichnisse von einer virtuellen VMware-Maschine zu sichern und zurückzuschreiben.</p> | <ul style="list-style-type: none"> <li>• Data Protection for Microsoft Hyper-V installieren</li> <li>• Installation und Upgrade für Data Protection for VMware durchführen</li> <li>• IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)</li> </ul> |

Tipp: Um den Client für die Speicherbereichsverwaltung zu verwenden, können Sie IBM Spectrum Protect for Space Management oder IBM Spectrum Protect HSM for Windows installieren.

## Regeln zum Sichern und Archivieren von Clientdaten angeben

Stellen Sie vor dem Hinzufügen eines Clients sicher, dass entsprechende Regeln zum Sichern und Archivieren der Clientdaten angegeben sind. Während des Clientregistrierungsprozesses ordnen Sie den Clientknoten einer Maßnahmendomäne zu, die die Regeln enthält, die die Regeln enthält, die steuern, wie und wann Clientdaten gespeichert werden.

### Vorbereitende Schritte

Legen Sie die weitere Vorgehensweise fest:

- Wenn Sie mit den Maßnahmen, die für Ihre Lösung konfiguriert sind, vertraut sind und wissen, dass für die Maßnahmen keine Änderungen erforderlich sind, fahren Sie mit Sicherungs- und Archivierungsoperationen planen fort.
- Wenn Sie mit den Maßnahmen nicht vertraut sind, führen Sie die Schritte in dieser Prozedur aus.

### Informationen zu diesem Vorgang

Maßnahmen haben Auswirkungen auf das Datenvolumen, das im Laufe der Zeit gespeichert wird, und den Zeitraum, den Daten aufbewahrt werden und für die Zurückschreibung durch Clients verfügbar sind. Um Datenschutzziele zu erreichen, können Sie die Standardmaßnahme aktualisieren und eigene Maßnahmen erstellen. Eine Maßnahme umfasst die folgenden Regeln:

- Angabe, wie und wann Dateien in Serverspeicher gesichert und archiviert werden
- Anzahl Kopien einer Datei und Zeitraum, den Kopien im Serverspeicher aufbewahrt werden

Während des Clientregistrierungsprozesses ordnen Sie einen Client einer *Maßnahmendomäne* zu. Die Maßnahme für einen bestimmten Client wird durch die Regeln in der Maßnahmendomäne festgelegt, der der Client zugeordnet ist. In der Maßnahmendomäne befinden sich die Regeln, die wirksam sind, in der aktiven *Maßnahmengruppe*.

Wenn ein Client eine Datei sichert oder archiviert, wird die Datei an eine Verwaltungsklasse in der aktiven Maßnahmengruppe der Maßnahmendomäne gebunden. Eine *Verwaltungsklasse* ist die wichtigste Gruppe von Regeln zur Verwaltung von Clientdaten. Die Sicherungs- und Archivierungsoperationen auf dem Client verwenden die Einstellungen in der Standardverwaltungsklasse der Maßnahmendomäne, es sei denn, Sie passen die Maßnahme weiter an. Eine Maßnahme kann angepasst werden, indem weitere Verwaltungsklassen definiert werden und ihre Verwendung über Clientoptionen zugeordnet wird.

Clientoptionen können in einer lokalen, editierbaren Datei auf dem Clientsystem und in einer Clientoptionsgruppe auf dem Server angegeben werden. Die Optionen in der Clientoptionsgruppe auf dem Server können die Optionen in der lokalen Clientoptionsdatei überschreiben oder den Optionen in der lokalen Clientoptionsdatei hinzugefügt werden.

### Vorgehensweise

1. Überprüfen Sie die Maßnahmen, die für Ihre Lösung konfiguriert sind, indem Sie die Anweisungen in Maßnahmen anzeigen ausführen.

2. Wenn geringfügige Änderungen erforderlich sind, um die Datenaufbewahrungsanforderungen zu erfüllen, führen Sie die Anweisungen in Maßnahmen editieren aus.
3. Optional: Wenn Maßnahmendomänen erstellt oder umfangreiche Änderungen an Maßnahmen durchgeführt werden müssen, um Datenaufbewahrungsanforderungen zu erfüllen, lesen Sie die Informationen in Maßnahmen anpassen.

## Maßnahmen anzeigen

---

Zeigen Sie Maßnahmen an, um zu bestimmen, ob die Maßnahmen zur Erfüllung Ihrer Anforderungen editiert werden müssen.

### Vorgehensweise

---

1. Um die aktive Maßnahmengruppe für eine Maßnahmendomäne anzuzeigen, führen Sie die folgenden Schritte aus:
  - a. Wählen Sie auf der Seite Services im Operations Center eine Maßnahmendomäne aus und klicken Sie auf Details.
  - b. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen.  
Tipp: Um sicherzustellen, dass Sie Daten nach einer Ransomware-Attacke wiederherstellen können, beachten Sie die folgenden Richtlinien:
    - Stellen Sie sicher, dass der Wert in der Spalte 'Sicherungen' mindestens 2 beträgt. Der bevorzugte Wert ist 3, 4 oder höher.
    - Stellen Sie sicher, dass der Wert in der Spalte 'Zusätzliche Sicherungen aufbewahren' mindestens 14 Tage beträgt. Der bevorzugte Wert ist 30 Tage oder mehr.
    - Stellen Sie sicher, dass der Wert in der Spalte 'Archivierungen aufbewahren' mindestens 30 Tage beträgt.Wenn IBM Spectrum Protect for Space Management-Software auf dem Client installiert ist, stellen Sie sicher, dass diese Daten vor ihrer Umlagerung gesichert werden. Geben Sie im Befehl `DEFINE MGMTCLASS` oder `UPDATE MGMTCLASS MIGREQUIRESBKUP=YES` an. Befolgen Sie dann die Richtlinien im Tipp.
2. Um inaktive Maßnahmengruppen für eine Maßnahmendomäne anzuzeigen, führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf der Seite Maßnahmengruppen auf die Umschaltfläche Konfigurieren. Jetzt können Sie die inaktiven Maßnahmengruppen anzeigen und editieren.
  - b. Blättern Sie mithilfe der vorwärts und rückwärts gerichteten Pfeile durch die inaktiven Maßnahmengruppen. Wenn Sie eine inaktive Maßnahmengruppe anzeigen, sind die unterschiedlichen Einstellungen für die inaktive und aktive Maßnahmengruppe hervorgehoben.
  - c. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppen sind nicht mehr editierbar.

## Maßnahmen editieren

---

Um die Regeln zu ändern, die für eine Maßnahmendomäne gelten, editieren Sie die aktive Maßnahmengruppe für die Maßnahmendomäne. Sie können auch eine andere Maßnahmengruppe für eine Domäne aktivieren.

### Vorbereitende Schritte

---

Änderungen an Maßnahmen können sich auf die Datenaufbewahrung auswirken. Stellen Sie sicher, dass weiterhin Daten gesichert werden, die für Ihr Unternehmen von entscheidender Bedeutung sind, sodass Sie diese Daten in einem Katastrophenfall zurückschreiben können. Stellen Sie außerdem sicher, dass Ihr System über genügend Speicherbereich für geplante Sicherungsoperationen verfügt.

### Informationen zu diesem Vorgang

---

Sie editieren eine Maßnahmengruppe, indem Sie eine oder mehrere Verwaltungsklassen in der Maßnahmengruppe ändern. Wenn Sie die aktive Maßnahmengruppe editieren, stehen die Änderungen den Clients erst zur Verfügung, nachdem Sie die Maßnahmengruppe reaktiviert haben. Um die editierte Maßnahmengruppe Clients zur Verfügung zu stellen, aktivieren Sie die Maßnahmengruppe.

Obwohl Sie mehrere Maßnahmengruppen für eine Maßnahmendomäne definieren können, kann nur eine einzige Maßnahmengruppe aktiv sein. Wenn Sie eine andere Maßnahmengruppe aktivieren, ersetzt diese die momentan aktive Maßnahmengruppe.

Informationen zu bevorzugten Verfahren zum Definieren von Maßnahmen finden Sie in Maßnahmen anpassen.

### Vorgehensweise

---

1. Wählen Sie auf der Seite Services im Operations Center eine Maßnahmendomäne aus und klicken Sie auf Details.
2. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen.

Die Seite Maßnahmengruppen gibt den Namen der aktiven Maßnahmengruppe an und listet alle Verwaltungsklassen für diese Maßnahmengruppe auf.

3. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppe ist editierbar.

4. Optional: Um eine Maßnahmengruppe zu editieren, die nicht aktiv ist, klicken Sie auf die vorwärts und rückwärts gerichteten Pfeile, um die Maßnahmengruppe zu lokalisieren.
5. Editieren Sie die Maßnahmengruppe, indem Sie eine der folgenden Aktionen ausführen:

| Option  | Bezeichnung   |
|---|---|
| <b>Verwaltungsklasse hinzufügen</b>   | <ol style="list-style-type: none"> <li>a. Klicken Sie in der Tabelle 'Maßnahmengruppen' auf + Verwaltungsklasse.</li> <li>b. Um die Regeln zum Sichern und Archivieren von Daten anzugeben, füllen Sie die Felder im Fenster Verwaltungsklasse hinzufügen aus.</li> <li>c. Um die Verwaltungsklasse als Standardverwaltungsklasse festzulegen, wählen Sie das Kontrollkästchen Als Standardwert definieren aus.</li> <li>d. Klicken Sie auf Hinzufügen.</li> </ol>                                    |
| <b>Verwaltungsklasse löschen</b>  | Klicken Sie in der Spalte 'Verwaltungsklasse' auf -.<br>Tipp: Um die Standardverwaltungsklasse zu löschen, müssen Sie zunächst eine andere Verwaltungsklasse als Standardverwaltungsklasse zuordnen.  |
| <b>Legen Sie eine Verwaltungsklasse als Standardverwaltungsklasse fest.</b> | Klicken Sie in der Spalte 'Standard' für die Verwaltungsklasse auf das Optionsfeld.<br>Tipp: Die Standardverwaltungsklasse verwaltet Clientdateien, wenn einer Datei keine andere Verwaltungsklasse zugeordnet ist oder keine andere Verwaltungsklasse zur Verwaltung geeignet ist. Um sicherzustellen, dass Clients immer Dateien sichern und archivieren können, wählen Sie eine Standardverwaltungsklasse aus, die sowohl Regeln für das Sichern als auch für das Archivieren von Dateien enthält. |
| <b>Verwaltungsklasse ändern</b>   | Um die Merkmale einer Verwaltungsklasse zu ändern, aktualisieren Sie die Felder in der Tabelle.   |

6. Klicken Sie auf Sichern.  
Achtung: Wenn Sie eine neue Maßnahmengruppe aktivieren, können Daten verloren gehen. Daten, die unter einer Maßnahmengruppe geschützt werden, werden möglicherweise unter einer anderen Maßnahmengruppe nicht geschützt. Daher müssen Sie vor dem Aktivieren einer Maßnahmengruppe sicherstellen, dass die Unterschiede zwischen der vorherigen Maßnahmengruppe und der neuen Maßnahmengruppe keinen Datenverlust zur Folge haben.
7. Klicken Sie auf Aktivieren. Es wird eine Zusammenfassung der Unterschiede zwischen der aktiven Maßnahmengruppe und der neuen Maßnahmengruppe angezeigt. Stellen Sie sicher, dass die Änderungen in der neuen Maßnahmengruppe mit Ihren Datenaufbewahrungsanforderungen konsistent sind, indem Sie die folgenden Schritte ausführen:
  - a. Überprüfen Sie die Unterschiede zwischen entsprechenden Verwaltungsklassen in den beiden Maßnahmengruppen und wägen Sie die Konsequenzen für Clientdateien ab. Clientdateien, die an Verwaltungsklassen in der aktiven Maßnahmengruppe gebunden sind, werden in der neuen Maßnahmengruppe an die Verwaltungsklassen mit denselben Namen gebunden.
  - b. Ermitteln Sie Verwaltungsklassen in der aktiven Maßnahmengruppe, die in der neuen Maßnahmengruppe keine Entsprechung haben und wägen Sie die Konsequenzen für Clientdateien ab. Clientdateien, die an diese Verwaltungsklassen gebunden sind, werden von der Standardverwaltungsklasse in der neuen Maßnahmengruppe verwaltet.
  - c. Wenn die Änderungen, die durch die Maßnahmengruppe implementiert werden sollen, akzeptabel sind, wählen Sie das Kontrollkästchen Ich weiß, dass diese Aktualisierungen zu einem Datenverlust führen können aus und klicken Sie auf Aktivieren.

## Sicherungs- und Archivierungsoperationen planen

Bevor Sie einen neuen Client beim Server registrieren, müssen Sie sicherstellen, dass ein Zeitplan verfügbar ist, um anzugeben, wann Sicherungs- und Archivierungsoperationen ausgeführt werden. Während des Registrierungsprozesses können Sie dem Client einen Zeitplan zuordnen.

### Vorbereitende Schritte

Legen Sie die weitere Vorgehensweise fest:

- Wenn Sie mit den Zeitplänen, die für die Lösung konfiguriert sind, vertraut sind und für die Zeitpläne keine Änderungen erforderlich sind, fahren Sie mit Clients registrieren fort.
- Wenn Sie mit den Zeitplänen nicht vertraut sind oder für die Zeitpläne Änderungen erforderlich sind, führen Sie die Schritte in dieser Prozedur aus.

### Informationen zu diesem Vorgang

Normalerweise müssen Sicherungsoperationen für alle Clients täglich ausgeführt werden. Planen Sie Client- und Server-Workloads mit Bedacht, um die beste Leistung für Ihre Speicherumgebung zu erzielen. Um die Überschneidung von Client- und Serveroperationen zu verhindern, planen Sie die Ausführung von Clientsicherungs- und -archivierungsoperationen gegebenenfalls für die Nacht. Wenn sich




Client- und Serveroperationen überschneiden oder ihnen nicht genügend Zeit und Ressourcen zur Verarbeitung zur Verfügung gestellt werden, können eine Verschlechterung der Systemleistung, fehlgeschlagene Operationen und andere Probleme die Folge sein.


## Vorgehensweise

- Überprüfen Sie die verfügbaren Zeitpläne, indem Sie den Mauszeiger in der Menüleiste des Operations Center über Clients bewegen. Klicken Sie auf Zeitpläne.
- Optional: Ändern oder Erstellen Sie einen Zeitplan, indem Sie die folgenden Schritte ausführen:

| Option                    | Bezeichnung  |
|---------------------------|--|
| <b>Zeitplan ändern</b>    | <ol style="list-style-type: none"><li>Wählen Sie in der Sicht Zeitpläne den Zeitplan aus und klicken Sie auf Details.</li><li>Zeigen Sie auf der Seite Zeitplandetails Details an, indem Sie auf die blauen Pfeile am Anfang der Zeilen klicken.</li><li>Ändern Sie die Einstellungen im Zeitplan und klicken Sie auf Sichern.</li></ol> |
| <b>Zeitplan erstellen</b> | Klicken Sie in der Sicht Zeitpläne auf +Zeitplan und führen Sie die Schritte zum Erstellen eines Zeitplans aus.  |

- Optional: Verwenden Sie zum Konfigurieren von Zeitplaneinstellungen, die im Operations Center nicht sichtbar sind, einen Serverbefehl. Angenommen, Sie möchten eine Clientoperation planen, mit der ein bestimmtes Verzeichnis gesichert und einer anderen Verwaltungsklasse als der Standardverwaltungsklasse zugeordnet wird.
  - Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.
  - Geben Sie zum Erstellen eines Zeitplans den Befehl DEFINE SCHEDULE und zum Ändern eines Zeitplans den Befehl UPDATE SCHEDULE aus. Ausführliche Informationen zu den Befehlen finden Sie in DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren) bzw. UPDATE SCHEDULE (Clientzeitplan aktualisieren).

### Zugehörige Tasks:

-  Zeitplan für tägliche Operationen optimieren

## Clients registrieren

Registrieren Sie einen Client, um sicherzustellen, dass der Client die Verbindung zum Server herstellen und der Server Clientdaten schützen kann.

## Vorbereitende Schritte

Bestimmen Sie, ob der Client eine Benutzer-ID mit Administratorberechtigung mit Clienteignerberechtigung für den Clientknoten erfordert. Informationen zum Bestimmen der Clients, die eine Benutzer-ID mit Administratorberechtigung erfordern, finden Sie in Technote 7048963.

Einschränkung: Bei einigen Clienttypen müssen der Clientknotenname und die Benutzer-ID mit Administratorberechtigung übereinstimmen. Sie können diese Clients nicht mithilfe der in Version 7.1.7 eingeführten LDAP-Authentifizierungsmethode authentifizieren. Ausführliche Informationen zu dieser Authentifizierungsmethode, die manchmal als integrierter Modus bezeichnet wird, finden Sie in Benutzer mithilfe einer Active Directory-Datenbank authentifizieren.

## Vorgehensweise

Um einen Client zu registrieren, führen Sie eine der folgenden Aktionen aus.

- Wenn der Client eine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Befehl REGISTER NODE unter Angabe des Parameters USERID:

```
register node Knotenname Kennwort userid=Knotenname
```

Dabei gibt *Knotenname* den Knotennamen und *Kennwort* das Knotenkennwort an. Ausführliche Informationen finden Sie in Knoten registrieren.

- Wenn der Client keine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Assistenten 'Client hinzufügen' im Operations Center. Führen Sie die folgenden Schritte aus:
  - Klicken Sie in der Menüleiste des Operations Center auf Clients.
  - Klicken Sie in der Tabelle 'Clients' auf + Client.
  - Führen Sie die Schritte im Assistenten Client hinzufügen aus:
    - Geben Sie an, dass redundante Daten sowohl auf dem Client als auch auf dem Server gelöscht werden können. Wählen Sie im Bereich 'Clientseitige Dateneduplizierung' das Kontrollkästchen Aktivieren aus.
    - Kopieren Sie im Fenster Konfiguration die Werte für die Optionen TCPSERVERADDRESS, TCPPORT, NODENAME und DEPLICATION.

- Tipp: Notieren Sie die Optionswerte und bewahren Sie die Unterlagen an einem sicheren Ort auf. Nachdem Sie die Clientregistrierung abgeschlossen und die Software auf dem Clientknoten installiert haben, verwenden Sie die Werte zum Konfigurieren des Clients.
- iii. Führen Sie die Anweisungen im Assistenten aus, um die Maßnahmendomäne, den Zeitplan und die Optionsgruppe anzugeben.
  - iv. Legen Sie fest, wie Risiken für den Client angezeigt werden, indem Sie die Einstellung für die Gefährdung angeben.
  - v. Klicken Sie auf Client hinzufügen.

**Zugehörige Verweise:**

- ➔ Option 'tcpserveraddress'
- ➔ Option 'tcpport'
- ➔ Option 'nodename'
- ➔ Option 'deduplication'

## Clients installieren und konfigurieren

Bevor Sie einen Clientknoten schützen können, müssen Sie die ausgewählte Software installieren und konfigurieren.

### Vorgehensweise

Wenn Sie die Software bereits installiert haben, starten Sie mit Schritt 2.

1. Führen Sie eine der folgenden Aktionen aus:
  - o Um Software auf einem Anwendungs- oder Clientknoten zu installieren, führen Sie die Anweisungen aus.

| Software  | Link zu Anweisungen   |
|---|---|
| IBM Spectrum Protect-Client für Sichern/Archivieren   | <ul style="list-style-type: none"> <li>■ UNIX- und Linux-Clients für Sichern/Archivieren installieren</li> <li>■ Windows-Client für Sichern/Archivieren installieren</li> </ul> <p>Tipp: Sie können vorhandene Clients auch mithilfe des Operations Center aktualisieren. Anweisungen finden Sie in Clientaktualisierungen planen.</p>  |
| IBM Spectrum Protect for Databases                    | <ul style="list-style-type: none"> <li>■ Installation von Data Protection for Oracle</li> <li>■ Data Protection for SQL Server unter Windows Server Core installieren</li> </ul>  |
| IBM Spectrum Protect for Mail                         | <ul style="list-style-type: none"> <li>■ Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0)</li> <li>■ Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0)</li> <li>■ Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li> </ul> |
| IBM Spectrum Protect Snapshot                         | <ul style="list-style-type: none"> <li>■ Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen</li> <li>■ Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen</li> <li>■ Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen</li> </ul>  |
| IBM Spectrum Protect for Enterprise Resource Planning | <ul style="list-style-type: none"> <li>■ IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 installieren</li> <li>■ IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle installieren</li> </ul>   |

- o Um Software auf einem VM-Clientknoten zu installieren, führen Sie die Anweisungen für den ausgewählten Sicherungstyp aus.

| Sicherungstyp  | Link zu Anweisungen   |
|--|---|
| Wenn Sie planen, VMware-Gesamtsicherungen virtueller Maschinen zu erstellen, installieren und konfigurieren Sie den IBM Spectrum Protect-Client für Sichern/Archivieren. | <ul style="list-style-type: none"> <li>■ UNIX- und Linux-Clients für Sichern/Archivieren installieren</li> <li>■ Windows-Client für Sichern/Archivieren installieren</li> </ul> |

| Sicherungstyp   | Link zu Anweisungen   |
|---|---|
| Wenn Sie planen, immer inkrementelle Gesamtsicherungen virtueller Maschinen zu erstellen, installieren und konfigurieren Sie IBM Spectrum Protect for Virtual Environments und den Client für Sichern/Archivieren auf demselben Clientknoten oder auf unterschiedlichen Clientknoten. | <ul style="list-style-type: none"> <li>■ IBM Spectrum Protect for Virtual Environments-Onlineproduktokumentation</li> </ul> Tipp: Die Software für IBM Spectrum Protect for Virtual Environments und den Client für Sichern/Archivieren sind im IBM Spectrum Protect for Virtual Environments-Installationspaket enthalten. |

2. Um Clients das Herstellen einer Verbindung zum Server zu ermöglichen, fügen Sie die Werte für die Optionen TCPSERVERADDRESS, TCPPORT und NODENAME in der Clientoptionsdatei hinzu oder aktualisieren Sie diese. Verwenden Sie die Werte, die Sie beim Registrieren des Clients notiert haben (Clients registrieren).
  - Fügen Sie für Clients, die unter einem AIX-, Linux- oder Mac OS X-Betriebssystem installiert sind, die Werte der Clientsystemoptionsdatei dsm.sys hinzu.
  - Fügen Sie für Clients, die unter einem Windows-Betriebssystem installiert sind, die Werte der Clientsystemoptionsdatei dsm.opt hinzu.
 Standardmäßig befinden sich die Optionsdateien im Installationsverzeichnis.
3. Wenn ein Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem installiert wurde, installieren Sie den Clientverwaltungsservice auf dem Client. Führen Sie die Anweisungen in Clientverwaltungsservice installieren aus.
4. Konfigurieren Sie den Client für die Ausführung geplanter Operationen. Führen Sie die Anweisungen in Client für die Ausführung geplanter Operationen konfigurieren aus.
5. Optional: Konfigurieren Sie die Kommunikation durch eine Firewall. Führen Sie die Anweisungen in Client/Server-Kommunikation durch eine Firewall konfigurieren aus.
6. Führen Sie eine Testsicherung aus, um sicherzustellen, dass Daten wie geplant geschützt werden. Führen Sie beispielsweise für einen Client für Sichern/Archivieren die folgenden Schritte aus:
  - a. Wählen Sie auf der Seite 'Clients' im Operations Center den Client aus, der gesichert werden soll, und klicken Sie auf Sichern.
  - b. Überprüfen Sie, ob die Sicherung erfolgreich ausgeführt wird und keine Warnungen oder Fehlermeldungen vorhanden sind.
7. Überwachen Sie die Ergebnisse der geplanten Operationen für den Client im Operations Center.

## Nächste Schritte

Wenn geändert werden muss, welche Daten vom Client gesichert werden, führen Sie die Anweisungen in Bereich einer Clientsicherung ändern aus.

## Client für die Ausführung geplanter Operationen konfigurieren

Sie müssen einen Client-Scheduler auf dem Clientknoten konfigurieren und starten. Der Client-Scheduler ermöglicht die Kommunikation zwischen dem Client und dem Server, sodass geplante Operationen erfolgen können. Beispielsweise umfassen geplante Operationen normalerweise das Sichern von Dateien von einem Client.

### Informationen zu diesem Vorgang

Die bevorzugte Methode ist die Installation des Clients für Sichern/Archivieren auf allen Clientknoten, sodass Sie den Clientakzeptor auf dem Clientknoten konfigurieren und starten können. Der Clientakzeptor ist für die effiziente Ausführung geplanter Operationen konzipiert. Der Clientakzeptor verwaltet den Client-Scheduler derart, dass der Scheduler nur in erforderlichen Fällen ausgeführt wird:

- Wenn der Zeitpunkt erreicht ist, an dem der Server nach der nächsten geplanten Operation abgefragt werden soll
- Wenn der Zeitpunkt erreicht ist, an dem die nächste geplante Operation gestartet werden soll

Durch die Verwendung des Clientakzeptors ist es möglich, die Anzahl Hintergrundprozesse auf dem Client zu reduzieren und Probleme in Bezug auf die Speicheraufbewahrungsdauer zu vermeiden.

Der Clientakzeptor führt Zeitpläne für die folgenden Produkte aus: Client für Sichern/Archivieren, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail und IBM Spectrum Protect for Virtual Environments. Wenn Sie ein Produkt installiert hatten, für das der Clientakzeptor keine Zeitpläne ausführt, führen Sie die Konfigurationsanweisungen in der Produktdokumentation aus, um sicherzustellen, dass geplante Operationen ausgeführt werden können.

Wenn Ihr Unternehmen standardmäßig ein Zeitplanungstool eines anderen Anbieters verwendet, können Sie statt des Clientakzeptors dieses Zeitplanungstool verwenden. Normalerweise starten Zeitplanungstools anderer Anbieter Clientprogramme direkt mithilfe von Betriebssystembefehlen. Informationen zum Konfigurieren eines Zeitplanungstools eines anderen Anbieters enthält die Produktdokumentation.

Um den Client-Scheduler mithilfe des Clientakzeptors zu konfigurieren und zu starten, führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

### AIX und Oracle Solaris

- Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
- Klicken Sie auf die Registerkarte Web-Client.
- Klicken Sie im Feld Optionen für verwaltete Services auf Zeitplan. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option Beides.
- Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, setzen Sie in der Datei `dsm.sys` die Option `passwordaccess` auf `generate`.
- Um das Clientknotenkenntwort zu speichern, geben Sie den folgenden Befehl aus und geben Sie auf Anforderung das Clientknotenkenntwort ein:

```
dsmc query sess
```

- Starten Sie den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

```
/usr/bin/dsmcad
```

- Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie der Systemstartdatei (normalerweise `/etc/inittab`) den folgenden Eintrag hinzu:

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Clientakzeptordämon
```

### Linux

- Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
- Klicken Sie auf die Registerkarte Web-Client.
- Klicken Sie im Feld Optionen für verwaltete Services auf Zeitplan. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option Beides.
- Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, setzen Sie in der Datei `dsm.sys` die Option `passwordaccess` auf `generate`.
- Um das Clientknotenkenntwort zu speichern, geben Sie den folgenden Befehl aus und geben Sie auf Anforderung das Clientknotenkenntwort ein:

```
dsmc query sess
```

- Starten Sie den Clientakzeptor, indem Sie sich mit der Rootbenutzer-ID anmelden und den folgenden Befehl ausgeben:

```
service dsmcad start
```

- Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie den Service hinzu, indem Sie in einer Shellingabeaufforderung den folgenden Befehl ausgeben:

```
# chkconfig --add dsmcad
```

### MAC OS X

- Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
- Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, klicken Sie auf Berechtigung, wählen Sie Kennwort generieren aus und klicken Sie auf Anwenden.
- Um anzugeben, wie Services verwaltet werden, klicken Sie auf Web-Client, wählen Sie Zeitplan aus, klicken Sie auf Anwenden und dann auf OK.
- Um sicherzustellen, dass das generierte Kennwort gespeichert wird, starten Sie den Client für Sichern/Archivieren erneut.
- Starten Sie den Clientakzeptor mithilfe der Anwendung 'IBM Spectrum Protect Tools for Administrators'.

### Windows

- Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Dienstprogramme > Setup-Assistent > Hilfe zum Konfigurieren des Client-Schedulers. Klicken Sie auf Weiter.
- Lesen Sie die Informationen auf der Seite Schedulerassistent und klicken Sie auf Weiter.
- Wählen Sie auf der Seite Scheduler-Task die Option Neuen oder zusätzlichen Scheduler installieren aus und klicken Sie auf Weiter.
- Geben Sie auf der Seite Schedulername und -position einen Namen für den Client-Scheduler an, der hinzugefügt wird. Wählen Sie dann Scheduler mit Clientakzeptordämon (CAD) verwalten aus, um den Scheduler zu verwalten, und klicken Sie auf Weiter.

- e. Geben Sie den Namen ein, der diesem Clientakzeptor zugeordnet werden soll. Der Standardname ist 'Clientakzeptor'. Klicken Sie auf Weiter.
- f. Schließen Sie die Konfiguration ab, indem Sie den Assistenten durchlaufen.
- g. Aktualisieren Sie die Clientoptionsdatei, dsm.opt, und setzen Sie die Option passwordaccess auf generate.
- h. Um das Clientknotenkenwort zu speichern, geben Sie den folgenden Befehl in der Eingabeaufforderung aus:

```
dsmc query sess
```

- Geben Sie auf Anforderung das Clientknotenkenwort ein.
- i. Starten Sie den Clientakzeptorservice über die Seite Systemsteuerung. Wenn Sie beispielsweise den Standardnamen verwendet haben, starten Sie den Service 'Clientakzeptor'. Starten Sie nicht den Scheduler-Service, den Sie auf der Seite Schedulername und -position angegeben haben. Der Scheduler-Service wird wie erforderlich automatisch vom Clientakzeptorservice gestartet und gestoppt.

## Client/Server-Kommunikation durch eine Firewall konfigurieren

---

Wenn ein Client durch eine Firewall mit einem Server kommunizieren muss, müssen Sie die Client/Server-Kommunikation durch die Firewall ermöglichen.

### Vorbereitende Schritte

---

Wenn Sie den Assistenten 'Client hinzufügen' zum Registrieren eines Clients verwendet hatten, bestimmen Sie die Optionswerte in der Clientoptionsdatei, die während dieses Prozesses abgerufen wurden. Sie können die Werte zur Angabe von Ports verwenden.

### Informationen zu diesem Vorgang

---

Achtung: Konfigurieren Sie eine Firewall nicht derart, dass dies eine Beendigung der Sitzungen zur Folge hätte, die von einem Server oder Speicheragenten verwendet werden. Die Beendigung einer gültigen Sitzung kann zu unvorhersehbaren Ergebnissen führen. Prozesse und Sitzungen scheinen unter Umständen aufgrund von Ein-/Ausgabebefehlen gestoppt zu werden. Um das Ausschließen von Sitzungen von Zeitlimitbeschränkungen zu erleichtern, konfigurieren Sie bekannte Ports für IBM Spectrum Protect-Komponenten. Stellen Sie sicher, dass die Serveroption KEEPALIVE auf den Standardwert YES gesetzt bleibt. Auf diese Art und Weise kann sichergestellt werden, dass die Client/Server-Kommunikation unterbrechungsfrei erfolgt. Anweisungen zum Definieren der Serveroption KEEPALIVE finden Sie in KEEPALIVE.

### Vorgehensweise

---

Öffnen Sie die folgenden Ports, um Zugriff durch die Firewall zu ermöglichen:

TCP/IP-Port für den Client für Sichern/Archivieren, den Verwaltungsbefehlszeilenclient und den Client-Scheduler

Geben Sie den Port über die Option tcpport in der Clientoptionsdatei an. Die Option tcpport in der Clientoptionsdatei muss mit der Option TCPPORT in der Serveroptionsdatei übereinstimmen. Der Standardwert ist 1500. Wenn ein anderer Wert als der Standardwert verwendet werden soll, geben Sie eine Zahl zwischen 1024 und 32767 an.

HTTP-Port, um die Kommunikation zwischen dem Web-Client und fernen Workstations zu ermöglichen

Geben Sie den Port für die ferne Workstation an, indem Sie die Option httpport in der Clientoptionsdatei der fernen Workstation festlegen. Der Standardwert ist 1581.

TCP/IP-Ports für die ferne Workstation

Der Standardwert von 0 (null) hat zur Folge, dass zwei freie Portnummern der fernen Workstation nach dem Zufallsprinzip zugeordnet werden. Wenn die Portnummern nicht nach dem Zufallsprinzip zugeordnet werden sollen, geben Sie über die Option webports in der Clientoptionsdatei der fernen Workstation Werte an.

TCP/IP-Port für Verwaltungssitzungen

Geben Sie den Port an, an dem der Server auf Anforderungen von Verwaltungsclientsitzungen wartet. Der Wert der Clientoption tcpadminport muss mit dem Wert der Serveroption TCPADMINPORT übereinstimmen. Auf diese Art und Weise können Sie sichere Verwaltungssitzungen in einem privaten Netz gewährleisten.

## Clientoperationen verwalten

---

Sie können Fehler, die einen Client für Sichern/Archivieren betreffen, mithilfe des Operations Center, das Vorschläge zur Behebung von Fehlern bereitstellt, auswerten und beheben. Bei Fehlern für andere Typen von Clients müssen Sie die Fehlerprotokolle auf dem Client überprüfen und in der Produktdokumentation nachlesen.

### Informationen zu diesem Vorgang

---

In einigen Fällen können Clientfehler behoben werden, indem der Clientakzeptor gestoppt und gestartet wird. Wenn Clientknoten oder Administrator-IDs gesperrt sind, können Sie das Problem beheben, indem Sie den Clientknoten bzw. die Administrator-ID entsperren und dann das Kennwort zurücksetzen.

Ausführliche Anweisungen zum Identifizieren und Beheben von Clientfehlern finden Sie in [Clientprobleme lösen](#).

- Fehler in Clientfehlerprotokollen auswerten  
Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.
- Clientakzeptor stoppen und erneut starten  
Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.
- Kennwörter zurücksetzen  
Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.
- Bereich einer Clientsicherung ändern  
Wenn Sie Clientsicherungsoperationen konfigurieren, ist das bevorzugte Verfahren das Ausschließen von Objekten, die nicht erforderlich sind. Angenommen, Sie möchten normalerweise temporäre Dateien von einer Sicherungsoperation ausschließen.

## Fehler in Clientfehlerprotokollen auswerten

---

Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.

### Vorbereitende Schritte

---

Um Fehler in einem Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem zu beheben, stellen Sie sicher, dass der Clientverwaltungsservice installiert und gestartet wurde. Installationsanweisungen finden Sie in [Clientverwaltungsservice installieren](#). Anweisungen zur Überprüfung der Installation finden Sie in [Ordnungsgemäße Installation des Clientverwaltungsservice](#) überprüfen.

### Vorgehensweise

---

Um Clientfehler zu diagnostizieren und zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn der Clientverwaltungsservice auf dem Clientknoten installiert ist, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Details.
  3. Klicken Sie auf der Seite 'Zusammenfassung' auf die Registerkarte Diagnose.
  4. Überprüfen Sie die abgerufenen Protokollnachrichten.  
Tipps:
    - Um das Fenster 'Clientprotokolle' ein- oder auszublenden, doppelklicken Sie auf den Rahmen des Fensters 'Clientprotokolle'.
    - Um die Größe des Fensters 'Clientprotokolle' zu ändern, klicken Sie auf den Rahmen des Fensters 'Clientprotokolle' und ziehen Sie den Rahmen.

Wenn auf der Seite 'Diagnose' Vorschläge angezeigt werden, wählen Sie einen Vorschlag aus. Im Fenster 'Clientprotokolle' sind die Clientprotokollnachrichten, auf die sich der Vorschlag bezieht, hervorgehoben.
- 5. Lösen Sie die in den Fehlernachrichten angegebenen Probleme mithilfe der Vorschläge.  
Tipp: Vorschläge werden nur für einen Teil der Clientnachrichten bereitgestellt.
- Wenn der Clientverwaltungsservice nicht auf dem Clientknoten installiert ist, überprüfen Sie die Fehlerprotokolle für den installierten Client.

## Clientakzeptor stoppen und erneut starten

---

Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.

### Informationen zu diesem Vorgang

---

In einigen Fällen können Clientzeitplanungsprobleme behoben werden, indem der Clientakzeptor gestoppt und erneut gestartet wird. Der Clientakzeptor muss aktiv sein, um sicherzustellen, dass geplante Operationen auf dem Client ausgeführt werden können. Wenn Sie beispielsweise die IP-Adresse oder den Domännennamen des Servers ändern, müssen Sie den Clientakzeptor erneut starten.

## Vorgehensweise

---

Führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

AIX und Oracle Solaris

- Um den Clientakzeptor zu stoppen, führen Sie die folgenden Schritte aus:
  - a. Bestimmen Sie die Prozess-ID für den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

```
ps -ef | grep dsmcad
```

Überprüfen Sie die Ausgabe. In der folgenden Beispielausgabe lautet die Prozess-ID für den Clientakzeptor 6764:

```
root 6764 1 0 16:26:35 ? 0:00 /usr/bin/dsmcad
```

- b. Geben Sie in der Befehlszeile den folgenden Befehl aus:

```
kill -9 PID
```

Dabei gibt *PID* die Prozess-ID für den Clientakzeptor an.

- Um den Clientakzeptor zu starten, geben Sie in der Befehlszeile den folgenden Befehl aus:

```
/usr/bin/dsmcad
```

Linux

- Um den Clientakzeptor zu stoppen, ohne ihn erneut zu starten, geben Sie den folgenden Befehl aus:

```
# service dsmcad stop
```

- Um den Clientakzeptor zu stoppen und erneut zu starten, geben Sie den folgenden Befehl aus:

```
# service dsmcad restart
```

MAC OS X

Klicken Sie auf Applications > Utilities > Terminal.

- Um den Clientakzeptor zu stoppen, geben Sie den folgenden Befehl aus:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Um den Clientakzeptor zu starten, geben Sie den folgenden Befehl aus:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

Windows

- Um den Clientakzeptorservice zu stoppen, führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf Start > Verwaltung > Dienste.
  - b. Doppelklicken Sie auf den Clientakzeptorservice.
  - c. Klicken Sie auf Beenden und OK.
- Um den Clientakzeptorservice erneut zu starten, führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf Start > Verwaltung > Dienste.
  - b. Doppelklicken Sie auf den Clientakzeptorservice.
  - c. Klicken Sie auf Starten und OK.

### Zugehörige Verweise:

 Fehler für Clientzeitplanung beheben

## Kennwörter zurücksetzen

---

Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.

## Vorgehensweise

---

Um Kennwortprobleme zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn ein Client für Sichern/Archivieren auf einem Clientknoten installiert ist und das Kennwort verloren gegangen ist oder Sie das Kennwort vergessen haben, führen Sie die folgenden Schritte aus:
  1. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

```
update node Knotenname neues_Kennwort forcepwreset=yes
```

Dabei gibt *Knotenname* den Clientknoten und *neues\_Kennwort* das Kennwort an, das Sie zuordnen.

2. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.  
Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf generate gesetzt haben.
- Wenn ein Administrator aufgrund von Kennwortproblemen ausgesperrt ist, führen Sie die folgenden Schritte aus:
    1. Um dem Administrator den Zugriff auf den Server zu ermöglichen, geben Sie den Befehl UNLOCK ADMIN aus. Anweisungen finden Sie in UNLOCK ADMIN (Administrator entsperren).
    2. Legen Sie mit dem Befehl UPDATE ADMIN ein neues Kennwort fest:

```
update admin Administratorname neues_Kennwort forcepwreset=yes
```

Dabei gibt *Administratorname* den Namen des Administrators und *neues\_Kennwort* das Kennwort an, das Sie zuordnen.

- Wenn ein Clientknoten gesperrt ist, führen Sie die folgenden Schritte aus:
  1. Bestimmen Sie, warum der Clientknoten gesperrt ist und ob er entsperrt werden muss. Wenn beispielsweise der Clientknoten stillgelegt ist, wird der Clientknoten aus der Produktionsumgebung entfernt. Sie können die Stilllegungsoperation nicht zurücknehmen und der Clientknoten bleibt gesperrt. Ein Clientknoten kann auch gesperrt sein, wenn die Clientdaten Gegenstand einer rechtlichen Untersuchung sind.
  2. Verwenden Sie zum Entsperren eines Clientknotens den Befehl UNLOCK NODE. Anweisungen finden Sie in UNLOCK NODE (Clientknoten entsperren).
  3. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

```
update node Knotenname neues_Kennwort forcepwreset=yes
```

Dabei gibt *Knotenname* den Namen des Knotens und *neues\_Kennwort* das Kennwort an, das Sie zuordnen.

4. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.  
Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf generate gesetzt haben.

## Bereich einer Clientsicherung ändern

---

Wenn Sie Clientsicherungsoperationen konfigurieren, ist das bevorzugte Verfahren das Ausschließen von Objekten, die nicht erforderlich sind. Angenommen, Sie möchten normalerweise temporäre Dateien von einer Sicherungsoperation ausschließen.

### Informationen zu diesem Vorgang

---

Indem Sie nicht benötigte Objekte von Sicherungsoperationen ausschließen, können Sie die Größe des Speicherbereichs, der für Sicherungsoperationen erforderlich ist, und die Speicherkosten besser steuern. Abhängig von Ihrem Lizenzpaket ist es unter Umständen auch möglich, die Lizenzierungskosten zu begrenzen.

## Vorgehensweise

---

Die Vorgehensweise beim Ändern des Bereichs von Sicherungsoperationen ist von dem Produkt abhängig, das auf dem Clientknoten installiert ist:

- Bei einem Client für Sichern/Archivieren können Sie eine Einschluss-/Ausschlussliste erstellen, um eine Datei, Dateigruppen oder Verzeichnisse in Sicherungsoperationen einzuschließen oder von Sicherungsoperationen auszuschließen. Um eine Einschluss-/Ausschlussliste zu erstellen, führen Sie die Anweisungen in Einschluss-/Ausschlussliste erstellen aus.

Um die konsistente Verwendung einer Einschluss-/Ausschlussliste für alle Clients eines bestimmten Typs zu gewährleisten, können Sie auf dem Server eine Clientoptionsgruppe erstellen, die die erforderlichen Optionen enthält. Anschließend ordnen Sie die Clientoptionsgruppe jedem Client desselben Typs zu. Ausführliche Informationen finden Sie in Clientoperationen über Clientoptionsgruppen steuern.



- Für einen Client für Sichern/Archivieren können Sie die Objekte, die in eine Teilsicherungsoperation eingeschlossen werden sollen, mithilfe der Option domain angeben. Führen Sie die Anweisungen in Clientoption 'domain' aus.
- Führen Sie für andere Produkte die Anweisungen in der Produktdokumentation aus, um zu definieren, welche Objekte in Sicherungsoperationen eingeschlossen und von Sicherungsoperationen ausgeschlossen werden sollen.

## Client-Upgrades verwalten

Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.

### Vorbereitende Schritte

1. Überprüfen Sie die Voraussetzungen für die Client/Server-Kompatibilität in Technote 1053218. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden.
2. Überprüfen Sie die Systemvoraussetzungen für den Client in IBM Spectrum Protect Supported Operating Systems.
3. Wenn die Lösung Speicheragenten oder Speicherarchivclients umfasst, überprüfen Sie die Informationen zur Kompatibilität von Speicheragenten bzw. Speicherarchivclients mit Servern, die als Speicherarchivmanager konfiguriert sind. Siehe Technote 1302789.

Wenn Sie planen, ein Upgrade für einen Speicherarchivmanager und einen Speicherarchivclient durchzuführen, müssen Sie zuerst das Upgrade für den Speicherarchivmanager durchführen.

### Vorgehensweise

Um ein Software-Upgrade durchzuführen, führen Sie die in der folgenden Tabelle aufgelisteten Anweisungen aus.

| Software  | Link zu Anweisungen   |
|---|---|
| IBM Spectrum Protect-Client für Sichern/Archivieren   | <ul style="list-style-type: none"> <li>• Clientaktualisierungen planen</li> </ul>   |
| IBM Spectrum Protect Snapshot                         | <ul style="list-style-type: none"> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen</li> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen</li> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen</li> </ul>  |
| IBM Spectrum Protect for Databases                    | <ul style="list-style-type: none"> <li>• Upgrade für Data Protection for SQL Server durchführen</li> <li>• Installation von Data Protection for Oracle</li> <li>• Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li> </ul>   |
| IBM Spectrum Protect for Enterprise Resource Planning | <ul style="list-style-type: none"> <li>• Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 durchführen</li> <li>• Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle durchführen</li> </ul>   |
| IBM Spectrum Protect for Mail                         | <ul style="list-style-type: none"> <li>• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0)</li> <li>• Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0)</li> <li>• Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li> </ul> |
| IBM Spectrum Protect for Virtual Environments         | <ul style="list-style-type: none"> <li>• Installation und Upgrade für Data Protection for VMware durchführen</li> <li>• Data Protection for Microsoft Hyper-V installieren</li> </ul>   |

## Clientknoten stilllegen

Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.

## Informationen zu diesem Vorgang

---

Wenn Sie den Stilllegungsprozess starten, sperrt der Server den Clientknoten, um zu verhindern, dass dieser auf den Server zugreift. Dateien, die zu dem Clientknoten gehören, werden nacheinander gelöscht; anschließend wird der Clientknoten gelöscht. Sie können die folgenden Typen von Clientknoten stilllegen:

### Anwendungsclientknoten

Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

### Systemclientknoten

Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

### VM-Clientknoten

Clientknoten virtueller Maschinen bestehen aus einem einzelnen Gasthost in einem Hypervisor. Jede virtuelle Maschine wird als ein Dateibereich dargestellt.

Die einfachste Methode zur Stilllegung eines Clientknotens ist die Verwendung des Operations Center. Der Stilllegungsprozess wird im Hintergrund ausgeführt. Wenn der Client für die Replikation von Clientdaten konfiguriert ist, entfernt das Operations Center den Client automatisch aus der Replikation auf dem Quellen- und dem Zielreplikationsserver, bevor es den Client stilllegt.

Tipp: Sie können einen Clientknoten auch stilllegen, indem Sie den Befehl `DECOMMISSION NODE` oder `DECOMMISSION VM` ausgeben. Diese Methode kann beispielsweise in den folgenden Fällen verwendet werden:

- Um den Stilllegungsprozess für einen späteren Zeitpunkt zu planen oder eine Serie von Befehlen unter Verwendung eines Scripts auszuführen, geben Sie die Ausführung des Stilllegungsprozesses im Hintergrund an.
- Um den Stilllegungsprozess zu Zwecken der Fehlerbehebung zu überwachen, geben Sie die Ausführung des Stilllegungsprozesses im Vordergrund an. Wenn Sie den Prozess im Vordergrund ausführen, müssen Sie warten, bis der Prozess abgeschlossen ist, bevor Sie die Arbeit mit anderen Tasks fortsetzen können.

## Vorgehensweise

---

Führen Sie eine der folgenden Aktionen aus:

- Um einen Client mithilfe des Operations Center im Hintergrund stillzulegen, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Weitere > Stilllegen.
- Um einen Clientknoten mithilfe eines Verwaltungsbefehls stillzulegen, führen Sie eine der folgenden Aktionen aus:
  - Um einen Anwendungs- oder Systemclientknoten im Hintergrund stillzulegen, geben Sie den Befehl `DECOMMISSION NODE` aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

```
decommission node austin
```

- Um einen Anwendungs- oder Systemclientknoten im Vordergrund stillzulegen, geben Sie den Befehl `DECOMMISSION NODE` unter Angabe des Parameters `wait=yes` aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

```
decommission node austin wait=yes
```

- Um eine virtuelle Maschine im Hintergrund stillzulegen, geben Sie den Befehl `DECOMMISSION VM` aus. Wenn beispielsweise die virtuelle Maschine den Namen AUSTIN hat, der Dateibereich 7 ist und der Dateibereichsname über die Dateibereichs-ID angegeben wird, geben Sie den folgenden Befehl aus:

```
decommission vm austin 7 nametype=fsid
```

Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Um eine virtuelle Maschine im Vordergrund stillzulegen, geben Sie den Befehl DECOMMISSION VM unter Angabe des Parameters `wait=yes` aus. Geben Sie beispielsweise den folgenden Befehl aus:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

## Nächste Schritte

Achten Sie auf Fehlermeldungen, die unter Umständen in der Benutzerschnittstelle oder in der Befehlsausgabe unmittelbar nach der Ausführung des Prozesses angezeigt werden.

Um zu überprüfen, ob der Clientknoten stillgelegt wurde, gehen Sie wie folgt vor:

- Klicken Sie auf der Seite Übersicht im Operations Center auf Clients.
- Überprüfen Sie in der Tabelle 'Clients' in der Spalte 'Gefährdet' den Status:
  - Der Status 'Stillgelegt' (DECOMMISSIONED) gibt an, dass der Knoten stillgelegt wurde.
  - Ein Nullwert gibt an, dass der Knoten nicht stillgelegt wurde.
  - Der Status 'Anstehend' (PENDING) gibt an, dass der Knoten gerade stillgelegt wird oder der Stilllegungsprozess fehlgeschlagen ist.

Tipp: Wenn der Status eines anstehenden Stilllegungsprozesses bestimmt werden soll, geben Sie den folgenden Befehl aus:

```
query process
```

- Überprüfen Sie die Befehlsausgabe:
  - Wenn für den Stilllegungsprozess ein Status angegeben ist, ist der Prozess in Bearbeitung. Beispiel:

```
query process
Prozess-      Prozessbeschreibung      Prozessstatus
nummer
-----
          3      DECOMMISSION NODE      Anzahl der für Knoten NODE1 inaktivierten
                               Sicherungsobjekte: 8 Objekte inaktiviert.
```

- Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie keine Fehlermeldung empfangen haben, ist der Prozess unvollständig. Ein Prozess kann unvollständig sein, wenn Dateien, die dem Knoten zugeordnet sind, noch nicht inaktiviert wurden. Führen Sie nach der Inaktivierung der Dateien den Stilllegungsprozess erneut aus.
- Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie eine Fehlermeldung empfangen, ist der Prozess fehlgeschlagen. Führen Sie den Stilllegungsprozess erneut aus.

### Zugehörige Verweise:

- [DECOMMISSION NODE \(Clientknoten stilllegen\)](#)
- [DECOMMISSION VM \(Virtuelle Maschine stilllegen\)](#)

## Daten zum Freigeben von Speicherbereich inaktivieren

In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegebenen Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

### Informationen zu diesem Vorgang

Einige Anwendungsclients sichern Daten immer als aktive Sicherungsdaten auf dem Server. Da aktive Sicherungsdaten nicht durch die Bestandsverfallsmaßnahmen verwaltet werden, werden die Daten nicht automatisch gelöscht und belegen unbegrenzt Serverspeicher. Um den Speicherbereich freizugeben, der von veralteten Daten belegt wird, können Sie die Daten inaktivieren.

Wenn Sie den Inaktivierungsprozess ausführen, werden alle aktiven Sicherungsdaten, die vor dem angegebenen Datum gespeichert wurden, inaktiv. Die Daten werden gelöscht, sobald sie verfallen, und können nicht zurückgeschrieben werden. Die Inaktivierungsfunktion gilt nur für Anwendungsclients, die Oracle-Datenbanken schützen.

### Vorgehensweise

- Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients.
- Wählen Sie in der Tabelle 'Clients' einen oder mehrere Clients aus und klicken Sie auf Weitere > Bereinigen.

Befehlszeilenmethode: Inaktivieren Sie Daten mit dem Befehl DEACTIVATE DATA.

**Zugehörige Verweise:**

➔ DEACTIVATE DATA (Daten für einen Clientknoten inaktivieren)

## Datenspeicher verwalten

---

Verwalten Sie Ihre Daten effizient und fügen Sie dem Server unterstützte Einheiten und Datenträger zum Speichern von Clientdaten hinzu.

- **Speicherpoolcontainer prüfen**  
Mit der Prüfung eines Speicherpoolcontainers wird auf Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Speicherpool geprüft.
- **Bestandskapazität verwalten**  
Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.
- **Speichernutzung und Prozessorauslastung verwalten**  
Der Speicherbedarf und die Prozessorauslastung müssen verwaltet werden, um sicherzustellen, dass der Server Datenprozesse wie Sicherung und Datenduplizierung ausführen kann. Berücksichtigen Sie die Auswirkung auf die Leistung, wenn Sie bestimmte Prozesse ausführen.
- **Geplante Aktivitäten optimieren**  
Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

**Zugehörige Verweise:**

➔ Speicherpooltypen

## Speicherpoolcontainer prüfen

---

Mit der Prüfung eines Speicherpoolcontainers wird auf Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Speicherpool geprüft.

### Informationen zu diesem Vorgang

---

Sie prüfen einen Speicherpoolcontainer in den folgenden Situationen:

- Sie geben den Befehl QUERY DAMAGED aus und es wird ein Problem erkannt.
- Der Server zeigt Nachrichten zu beschädigten Datenbereichen an.
- Ihre Hardware meldet ein Problem und es werden Fehlernachrichten angezeigt, die sich auf den Speicherpoolcontainer beziehen.

### Vorgehensweise

---

1. Um einen Speicherpoolcontainer zu prüfen, geben Sie den Befehl AUDIT CONTAINER aus. Geben Sie beispielsweise den folgenden Befehl aus, um den Container 000000000000076c.dcf zu prüfen:

```
audit container c:\tsm-storage\07\000000000000076c.dcf
```

2. Überprüfen Sie die Ausgabe der Nachricht ANR4891I auf Informationen zu allen beschädigten Datenbereichen.

### Nächste Schritte

---

Wenn Sie Probleme mit dem Speicherpoolcontainer erkennen, können Sie Daten auf der Basis Ihrer Konfiguration zurückschreiben. Geben Sie den Befehl AUDIT CONTAINER aus und geben Sie den Containernamen an.

**Zugehörige Verweise:**

➔ AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)

➔ QUERY DAMAGED (Beschädigte Daten in einem Verzeichniscontainer- oder Cloud-Containerspeicherpool abfragen)

## Bestandskapazität verwalten

---

Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.

## Vorbereitende Schritte

---

Die aktive Protokolldatei und das Archivprotokoll haben die folgenden Merkmale:

- Die Größe der aktiven Protokolldatei kann maximal 512 GB betragen. Weitere Informationen zum Festlegen der Größe der aktiven Protokolldatei für Ihr System finden Sie in Planung der Speicherarrays.
- Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist. Die Größe des Archivprotokolls ist im Gegensatz zur Größe der aktiven Protokolldatei nicht auf eine vordefinierte Größe festgelegt. Archivprotokolldateien werden automatisch gelöscht, wenn sie nicht mehr benötigt werden.

Als Best Practice können Sie wahlweise ein Archivübernahmeprotokoll erstellen, in dem Archivprotokolldateien gespeichert werden, wenn das Archivprotokollverzeichnis voll ist.

Bestimmen Sie über das Operations Center, welche Komponente des Bestands voll ist. Stellen Sie sicher, dass der Server gestoppt wird, bevor Sie eine der Bestandskomponenten vergrößern.

## Vorgehensweise

---

- Um die Datenbank zu vergrößern, führen Sie die folgenden Schritte aus:
  - Erstellen Sie in unterschiedlichen Laufwerken oder Dateisystemen ein oder mehrere Verzeichnisse für die Datenbank.
  - Geben Sie den Befehl `EXTEND DBSPACE` aus, um der Datenbank das Verzeichnis oder die Verzeichnisse hinzuzufügen. Die Instanzbenutzer-ID des Datenbankmanagers muss Zugriff auf die Verzeichnisse haben. Standardmäßig erfolgt eine Neuverteilung der Daten auf alle Datenbankverzeichnisse und eine Konsolidierung des Speicherbereichs.  
Tipps:
    - Die Zeit, die für die vollständige Neuverteilung von Daten und die Konsolidierung von Speicherbereich erforderlich ist, variiert abhängig von der Größe Ihrer Datenbank. Stellen Sie sicher, dass Sie dies bei der Planung berücksichtigen.
    - Stellen Sie sicher, dass die Verzeichnisse, die Sie angeben, dieselbe Größe wie vorhandene Verzeichnisse haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorabesezugriff und zur Verteilung der Datenbank verringert.
  - Stoppen Sie den Server und starten Sie ihn erneut, um die neuen Verzeichnisse vollständig nutzen zu können.
  - Reorganisieren Sie die Datenbank, falls erforderlich. Die Index- und Tabellenreorganisation für die Serverdatenbank kann dazu beitragen, unerwartetes Datenbankwachstum und Leistungsprobleme zu verhindern. Weitere Informationen zur Reorganisation der Datenbank finden Sie in Technote 1683633.
- Um die Datenbank für Server der Version 7.1 und höher zu verkleinern, geben Sie im Serverinstanzverzeichnis die folgenden DB2-Befehle aus:  
Einschränkung: Die Befehle können die E/A-Aktivität erhöhen und sich unter Umständen auf die Serverleistung auswirken. Um Leistungsprobleme auf ein Mindestmaß zu reduzieren, warten Sie, bis ein Befehl abgeschlossen ist, bevor Sie den nächsten Befehl ausgeben. Die DB2-Befehle können ausgegeben werden, wenn der Server aktiv ist.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE5 REDUCE MAX
```

- Um die aktive Protokolldatei zu vergrößern oder zu verkleinern, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass die Position für die aktive Protokolldatei über genügend Speicherbereich für die erhöhte Protokollgröße verfügt. Wenn ein Protokollspiegel vorhanden ist, muss auch die Position für den Spiegel über genügend Speicherbereich für die erhöhte Protokollgröße verfügen.
2. Stoppen Sie den Server.
3. Aktualisieren Sie in der Datei dmserv.opt die Option ACTIVELOGSIZE mit der neuen Größe der aktiven Protokolldatei (angegeben in Megabyte).  
Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option ACTIVELOGSIZE. Die folgende Tabelle enthält Richtlinien für den Speicherbedarf:

Tabelle 1. Schätzen des Speicherbedarfs für Datenträger und Dateibereiche

| Wert für die Option ACTIVELOGSIZE | Größe des im Verzeichnis für aktive Protokolldateien zu reservierender freier Speicherbereich zusätzlich zum Speicherbereich für ACTIVELOGSIZE |
|-----------------------------------|--|
| 16 GB bis 128 GB                  | 5120 MB  |
| 129 GB bis 256 GB                 | 10240 MB   |
| 257 GB bis 512 GB                 | 20480 MB   |

Um die Größe der aktiven Protokolldatei in die maximale Größe von 512 GB zu ändern, geben Sie die folgende Serveroption ein:

```
activeologsize 524288
```

4. Wenn Sie planen, ein neues Verzeichnis für aktive Protokolldateien zu verwenden, aktualisieren Sie den in der Serveroption ACTIVELOGDIRECTORY angegebenen Verzeichnisnamen. Das neue Verzeichnis muss leer sein und die Benutzer-ID des Datenbankmanagers muss Zugriff auf dieses Verzeichnis haben.
  5. Starten Sie den Server erneut.
- Komprimieren Sie die Archivprotokolle, um die Größe des Speicherbereichs, der zum Speichern benötigt wird, zu reduzieren. Aktivieren Sie die dynamische Komprimierung für das Archivprotokoll, indem Sie den folgenden Befehl ausgeben:

```
setopt archlogcompress yes
```

Einschränkung: Gehen Sie mit Vorsicht vor, wenn Sie die Serveroption ARCHLOGCOMPRESS auf Systemen mit kontinuierlich hoher Datenträgerverwendung und hohen Workloads aktivieren. Ein Aktivieren dieser Option in dieser Systemumgebung kann Verzögerungen beim Archivieren von Protokolldateien aus dem Dateisystem für aktive Protokolldateien in das Dateisystem für Archivprotokolle haben. Diese Verzögerung kann zur Folge haben, dass der Speicherbereich im Dateisystem für aktive Protokolldateien knapp wird. Sie müssen den verfügbaren Speicherbereich im Dateisystem für aktive Protokolldateien überwachen, nachdem die Komprimierung für das Archivprotokoll aktiviert wurde. Wenn für das Dateisystem für das Verzeichnis für aktive Protokolldateien fast kein Speicherbereich mehr verfügbar ist, muss die Serveroption ARCHLOGCOMPRESS inaktiviert werden. Mit dem Befehl SETOPT können Sie die Komprimierung für das Archivprotokoll sofort inaktivieren, ohne den Server stoppen zu müssen.

#### Zugehörige Verweise:

- ➔ Serveroption ACTIVELOGSIZE
- ➔ EXTEND DBSPACE (Speicherbereich für die Datenbank vergrößern)
- ➔ SETOPT (Serveroption für dynamische Aktualisierung definieren)

## Speichernutzung und Prozessorauslastung verwalten

Der Speicherbedarf und die Prozessorauslastung müssen verwaltet werden, um sicherzustellen, dass der Server Datenprozesse wie Sicherung und Datenduplizierung ausführen kann. Berücksichtigen Sie die Auswirkung auf die Leistung, wenn Sie bestimmte Prozesse ausführen.

### Vorbereitende Schritte

- Stellen Sie sicher, dass Ihre Konfiguration die erforderliche Hardware und Software verwendet. Weitere Informationen finden Sie in IBM Spectrum Protect Supported Operating Systems.
- Weitere Informationen zur Verwaltung von Ressourcen, wie beispielsweise Datenbank und Wiederherstellungsprotokoll, finden Sie in Planung der Speicherarrays.
- Fügen Sie zusätzlichen Systemspeicher hinzu, um festzustellen, ob sich die Leistung verbessert. Überwachen Sie die Speichernutzung regelmäßig, um zu bestimmen, ob weiterer Speicher erforderlich ist.

### Vorgehensweise

1. Geben Sie, falls möglich, Speicherbereich aus dem Dateisystemcache frei.
2. Verwenden Sie zur Verwaltung des Systemspeichers, den jeder Server auf einem System verwendet, die Serveroption DBMEMPERCENT. Begrenzen Sie den Prozentsatz des Systemspeichers, der vom Datenbankmanager jedes Servers verwendet

werden kann. Wenn alle Server gleich wichtig sind, verwenden Sie denselben Wert für jeden Server. Wenn ein Server der Produktionsserver ist und die anderen Server Testserver sind, definieren Sie für den Produktionsserver einen höheren Wert als für die Testserver.

3. Definieren Sie den Benutzerdatengrenzwert und den privaten Speicher für die Datenbank, um sicherzustellen, dass immer genügend privater Speicher verfügbar ist. Wenn der private Speicher knapp wird, kann dies Fehler, eine nicht optimale Leistung und Instabilität zur Folge haben.

## Geplante Aktivitäten optimieren

---

Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

### Vorgehensweise


---

1. Überwachen Sie die Systemleistung regelmäßig, um sicherzustellen, dass Sicherungs- und Verwaltungstasks erfolgreich ausgeführt werden. Weitere Informationen zur Überwachung finden Sie in Plattenspeicherlösung für einen einzelnen Standort überwachen.
2. Wenn die Überwachungsdaten anzeigen, dass sich die Server-Workload erhöht hat, müssen Sie die Planungsinformationen gegebenenfalls überprüfen. Überprüfen Sie, ob die Kapazität des Systems in den folgenden Fällen ausreichend ist:
  - o Erhöhung der Anzahl Clients
  - o Zunahme des Datenvolumens, das gesichert wird
  - o Änderung des Zeitraums, der für Sicherungen verfügbar ist
3. Bestimmen Sie, ob für Ihre Lösung Leistungsprobleme vorliegen. Überprüfen Sie die Clientzeitpläne dahingehend, ob Tasks innerhalb des geplanten Zeitrahmens ausgeführt werden:
  - a. Wählen Sie auf der Seite Clients im Operations Center den Client aus.
  - b. Klicken Sie auf Details.
  - c. Überprüfen Sie auf der Seite Zusammenfassung des Clients die für Gesichert und Repliziert angegebene Aktivität, um alle Risiken zu ermitteln.  
Passen Sie, falls erforderlich, den Zeitpunkt und die Häufigkeit für die Ausführung von Clientsicherungsoperationen an.
4. Planen Sie ausreichend Zeit ein, um die folgenden Verwaltungstasks innerhalb von 24 Stunden erfolgreich ausführen zu können:
  - a. Sichern der Datenbank
  - b. Ausführen der Verfallsverarbeitung, um Clientsicherungen und Archivierungsdateikopien aus dem Serverspeicher zu entfernen

#### Zugehörige Konzepte:

 Leistung

#### Zugehörige Tasks:

 Daten deduplizieren (Version 7.1.1)

## IBM Spectrum Protect-Server schützen

---

Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.

- Sicherheitskonzepte  
Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.
- Administratoren verwalten  
Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.
- Kennwortanforderungen ändern  
Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.
- Server auf dem System schützen  
Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

### Sicherheitskonzepte

---

Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.

## Transport Layer Security

Mithilfe des Protokolls Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) können Sie Transportschichtsicherheit für eine sichere Verbindung zwischen Servern, Clients und Speicheragenten bereitstellen. Wenn Sie Daten zwischen dem Server, dem Client und dem Speicheragenten austauschen, verwenden Sie SSL oder TLS zum Verschlüsseln der Daten.

**Tipp:** In der gesamten IBM Spectrum Protect-Dokumentation gilt jede Angabe von "SSL" oder zum "Auswählen von SSL" für TLS.

SSL wird von Global Security Kit (GSKit) bereitgestellt, das zusammen mit dem IBM Spectrum Protect-Server installiert wird, der vom Server, vom Client und vom Speicheragenten verwendet wird.

**Einschränkung:** Sie dürfen die SSL- oder TLS-Protokolle nicht für die Kommunikation mit einer DB2-Datenbankinstanz verwenden, die von IBM Spectrum Protect-Servern verwendet wird.

Jeder Server, Client oder Speicheragent, der SSL ermöglicht, muss ein vertrauenswürdigen selbst signiertes Zertifikat verwenden oder ein eindeutiges Zertifikat anfordern, das von einer Zertifizierungsstelle (CA) signiert ist. Sie können Ihre eigenen Zertifikate verwenden oder Zertifikate bei einer Zertifizierungsstelle (CA) kaufen. Jedes der Zertifikate muss installiert und der Schlüsseldatenbank auf dem IBM Spectrum Protect-Server, -Client oder -Speicheragenten hinzugefügt werden. Das Zertifikat wird von dem SSL-Client oder -Server geprüft, der die SSL-Kommunikation anfordert oder einleitet. Einige CA-Zertifikate sind in der Schlüsseldatenbank standardmäßig vorinstalliert.

SSL wird auf dem IBM Spectrum Protect-Server, -Client und -Speicheragenten unabhängig voneinander konfiguriert.

## Berechtigungsstufen

Für jeden IBM Spectrum Protect-Server sind verschiedene Administratorberechtigungsstufen verfügbar, die die Tasks festlegen, die ein Administrator ausführen kann.

Nach der Registrierung muss einem Administrator Berechtigung erteilt werden, indem ihm eine oder mehrere Administratorberechtigungsstufen zugeordnet werden. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen und anderen Administratoren über den Befehl GRANT AUTHORITY Berechtigungsstufen zuordnen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

Ein Administrator kann andere Administrator-IDs registrieren, den IDs Berechtigungsstufen zuordnen, IDs umbenennen, IDs entfernen und IDs für den Server sperren oder entsperren.

Ein Administrator kann den Zugriff auf bestimmte Clientknoten für Rootbenutzer-IDs und Nicht-Rootbenutzer-IDs steuern. Standardmäßig kann eine Nicht-Rootbenutzer-ID keine Daten auf dem Knoten sichern. Ändern Sie mit dem Befehl UPDATE NODE die Knoteneinstellungen, um Sicherungen zu ermöglichen.

## Kennwörter

Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer beim Zugriff auf den Server ein Kennwort eingeben.

Verwenden Sie LDAP (Lightweight Directory Access Protocol), um striktere Anforderungen für Kennwörter anzuwenden. Weitere Informationen finden Sie in Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1).

Tabelle 1. Merkmale der Kennwortauthentifizierung

| Merkmale                                   | Weitere Informationen  |
|--|--|
| Abhängigkeit von der Groß-/Kleinschreibung | Nicht von der Groß-/Kleinschreibung abhängig.  |
| Standardwert für Kennwortablauf            | 90 Tage.<br>Der Ablaufzeitraum beginnt mit der ersten Registrierung einer Administrator-ID oder eines Clientknotens beim Server. Wenn das Kennwort innerhalb dieses Zeitraums nicht geändert wird, muss das Kennwort beim nächsten Zugriff des Benutzers auf den Server geändert werden. |
| Ungültige Kennworteingabeversuche          | Sie können einen Grenzwert für aufeinanderfolgende ungültige Kennworteingabeversuche für alle Clientknoten definieren. Wenn der Grenzwert überschritten wird, sperrt der Server den Knoten.  |
| Kennwortlänge                              | Der Administrator kann eine Mindestlänge angeben.  |

## Sitzungssicherheit



Die Sitzungssicherheit ist die Sicherheitsstufe, die für die Kommunikation zwischen IBM Spectrum Protect-Clientknoten, -Verwaltungsclients und -Servern verwendet wird und mit dem Parameter SESSIONSECURITY festgelegt wird.

Der Parameter SESSIONSECURITY kann auf einen der folgenden Werte gesetzt werden:

- Mit dem Wert STRICT wird die höchste Sicherheitsstufe für die Kommunikation zwischen IBM Spectrum Protect-Servern, -Knoten und -Administratoren durchgesetzt.
- Der Wert TRANSITIONAL gibt an, dass das vorhandene Kommunikationsprotokoll verwendet wird, wenn Sie Ihre IBM Spectrum Protect-Software auf Version 8.1.2 oder höher aktualisieren. Dies ist der Standardwert. Wenn SESSIONSECURITY=TRANSITIONAL angegeben ist, werden strengere Sicherheitseinstellungen automatisch durchgesetzt, da höhere Versionen des TLS-Protokolls verwendet werden, wenn die Software auf Version 8.1.2 oder höher aktualisiert wird. Nachdem ein Knoten, Administrator oder Server die Anforderungen für den Wert STRICT erfüllt, wird die Sitzungssicherheit automatisch in den Wert STRICT geändert und die Entität kann sich nicht mehr unter Verwendung einer Vorgängerversion des Clients oder unter Verwendung früherer TLS-Protokolle authentifizieren.

Weitere Informationen zu den Werten für den Parameter SESSIONSECURITY enthalten die Beschreibungen der folgenden Befehle.

Tabelle 2. Befehle zum Festlegen des Parameters SESSIONSECURITY

| Entität         | Befehl   |
|-----------------|--|
| Clientknoten    | <ul style="list-style-type: none"> <li>• REGISTER NODE</li> <li>• UPDATE NODE</li> </ul>   |
| Administratoren | <ul style="list-style-type: none"> <li>• REGISTER ADMIN</li> <li>• UPDATE ADMIN</li> </ul> |
| Server          | <ul style="list-style-type: none"> <li>• DEFINE SERVER</li> <li>• UPDATE SERVER</li> </ul> |

Administratoren, die sich unter Verwendung des Befehls DSMADMC, des Befehls DSMC oder des Programms dsm authentifizieren, können sich nach der Authentifizierung unter Verwendung von Version 8.1.2 oder höher nicht unter Verwendung einer früheren Version authentifizieren. Die folgenden Tipps liefern Informationen zur Behebung von Authentifizierungsproblemen für Administratoren:

Tipps:

- Stellen Sie sicher, dass für die gesamte IBM Spectrum Protect-Software, die das Administratorkonto für die Anmeldung verwendet, ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird. Wenn sich ein Administratorkonto über mehrere Systeme anmeldet, stellen Sie sicher, dass das Zertifikat des Servers auf jedem System installiert ist.
- Nachdem sich ein Administrator bei einem Server der Version 8.1.2 oder höher unter Verwendung eines Clients der Version 8.1.2 oder höher authentifiziert hat, kann sich der Administrator nur auf Clients oder Servern authentifizieren, die Version 8.1.2 oder höher verwenden. Ein Administratorbefehl kann von jedem beliebigen System ausgegeben werden.
- Erstellen Sie, falls erforderlich, ein separates Administratorkonto, das nur mit Clients und Servern verwendet wird, die Software der Version 8.1.1 oder früher verwenden.

Setzen Sie die höchste Sicherheitsstufe für die Kommunikation mit dem IBM Spectrum Protect-Server durch, indem Sie sicherstellen, dass alle Knoten, Administratoren und Server die Sitzungssicherheit STRICT verwenden. Mithilfe des Befehls SELECT können Sie feststellen, welche Server, Knoten und Administratoren die Sitzungssicherheit TRANSITIONAL verwenden und für die Verwendung der Sitzungssicherheit STRICT aktualisiert werden sollten.

**Zugehörige Tasks:**

 Kommunikation schützen

## Administratoren verwalten

Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.

### Vorgehensweise

Führen Sie die folgenden Tasks aus, um Administratoreinstellungen zu ändern.

| Task | Prozedur |
|------|----------|
|------|----------|

| Task  | Prozedur  |
|---|---|
| Administrator hinzufügen                        | <p>Um einen Administrator, ADMIN1, mit Systemberechtigung hinzuzufügen und ein Kennwort anzugeben, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>Registrieren Sie den Administrator und geben Sie Pa\$#\$twO als Kennwort an, indem Sie den folgenden Befehl ausgeben: <pre>register admin admin1 Pa\$#\$twO</pre> </li> <li>Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben: <pre>grant authority admin1 classes=system</pre> </li> </ol> |
| Administratorberechtigung ändern                | <p>Ändern Sie die Berechtigungsstufe für einen Administrator, ADMIN1.</p> <ul style="list-style-type: none"> <li>Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben: <pre>grant authority admin1 classes=system</pre> </li> <li>Entziehen Sie dem Administrator die Systemberechtigung, indem Sie den folgenden Befehl ausgeben: <pre>revoke authority admin1 classes=system</pre> </li> </ul>  |
| Administratoren entfernen                       | <p>Entfernen Sie einen Administrator, ADMIN1, sodass er nicht mehr auf den IBM Spectrum Protect-Server zugreifen kann, indem Sie den folgenden Befehl ausgeben:</p> <pre>remove admin admin1</pre>  |
| Zugriff auf den Server vorübergehend verhindern | <p>Sperrern oder entsperren Sie einen Administrator, indem Sie den Befehl LOCK ADMIN bzw. UNLOCK ADMIN verwenden.</p>   |

## Kennwortanforderungen ändern

Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.

## Informationen zu diesem Vorgang

Indem Sie die Kennwortauthentifizierung durchsetzen und Kennworteinschränkungen verwalten, können Sie Ihre Daten und Ihre Server vor möglichen Sicherheitsrisiken schützen.

## Vorgehensweise



Führen Sie die folgenden Tasks aus, um Kennwortanforderungen für IBM Spectrum Protect-Server zu ändern.

Tabelle 1. Authentifizierungstasks für IBM Spectrum Protect-Server

| Task  | Prozedur   |
|---|--|
| Grenzwert für ungültige Kennworteingabeversuche festlegen | <ol style="list-style-type: none"> <li>Wählen Sie auf der Seite Server im Operations Center den Server aus.</li> <li>Klicken Sie auf Details und dann auf die Registerkarte Merkmale.</li> <li>Geben Sie die Anzahl ungültiger Versuche im Feld Grenzwert für ungültige Anmeldeversuche an.</li> </ol> <p>Der Standardwert bei der Installation ist 0.</p> |

| Task  | Prozedur   |
|---|--|
| Mindestlänge für Kennwörter festlegen       | <ol style="list-style-type: none"> <li>Wählen Sie auf der Seite Server im Operations Center den Server aus.</li> <li>Klicken Sie auf Details und dann auf die Registerkarte Merkmale.</li> <li>Geben Sie die Anzahl Zeichen im Feld Mindestlänge für Kennwort an.</li> </ol>   |
| Ablaufzeitraum für Kennwörter festlegen     | <ol style="list-style-type: none"> <li>Wählen Sie auf der Seite Server im Operations Center den Server aus.</li> <li>Klicken Sie auf Details und dann auf die Registerkarte Merkmale.</li> <li>Geben Sie die Anzahl Tage im Feld Allgemeine Kennwortablaufdauer an.</li> </ol>   |
| Kennwortauthentifizierung inaktivieren      | <p>Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer ein Kennwort eingeben, um auf den Server zugreifen zu können.</p> <p>Sie können die Kennwortauthentifizierung nur für Kennwörter inaktivieren, die mit dem Server (LOCAL) authentifiziert werden. Durch das Inaktivieren der Kennwortauthentifizierung erhöht sich das Sicherheitsrisiko für den Server.</p> |
| Standardauthentifizierungsmethode festlegen | <p>Geben Sie den Befehl SET DEFAULTAUTHENTICATION aus. Um beispielsweise den Server als die Standardauthentifizierungsmethode zu verwenden, geben Sie den folgenden Befehl aus:</p> <pre>set defaultauthentication local</pre> <p>Um einen Clientknoten für die Authentifizierung mit dem Server zu aktualisieren, schließen Sie AUTHENTICATION=LOCAL in den Befehl UPDATE NODE ein:</p> <pre>update node authentication=local</pre>                 |

#### Zugehörige Konzepte:

-  IBM Spectrum Protect-Benutzer mithilfe eines LDAP-Servers authentifizieren
-  Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1)

## Server auf dem System schützen

Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

### Vorgehensweise

Stellen Sie sicher, dass nicht berechtigte Benutzer nicht auf die Verzeichnisse für die Serverdatenbank und die Serverinstanz zugreifen können. Behalten Sie die Zugriffseinstellungen für diese Verzeichnisse bei, die Sie während der Implementierung konfiguriert haben.

- Benutzerzugriff auf den Server einschränken  
Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.
- Zugriff über Porteinschränkungen einschränken  
Schränken Sie den Zugriff auf den Server ein, indem Sie Porteinschränkungen anwenden.

## Benutzerzugriff auf den Server einschränken

Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

## Vorgehensweise

1. Nachdem Sie einen Administrator mit dem Befehl REGISTER ADMIN registriert haben, legen Sie die Berechtigungsstufe des Administrators mithilfe des Befehls GRANT AUTHORITY fest. Ausführliche Informationen zum Festlegen und Ändern der Berechtigung finden Sie in Administratoren verwalten.
2. Um die Berechtigung eines Administrators zur Ausführung bestimmter Tasks zu steuern, verwenden Sie die beiden folgenden Serveroptionen:
  - a. Über die Serveroption QUERYAUTH können Sie die Berechtigungsstufe auswählen, die ein Administrator haben muss, um Befehle QUERY und SELECT ausgeben zu können. Standardmäßig ist keine Berechtigungsstufe erforderlich. Sie können die Anforderung in eine der Berechtigungsstufen, einschließlich Systemberechtigung, ändern.
  - b. Über die Serveroption REQSYSAUTHOUTFILE können Sie angeben, dass Systemberechtigung für Befehle erforderlich ist, die zur Folge haben, dass der Server Daten in eine externe Datei schreibt. Standardmäßig ist für diese Befehle Systemberechtigung erforderlich.
3. Sie können die Datensicherung auf einem Clientknoten ausschließlich auf Rootbenutzer-IDs oder berechtigte Benutzer beschränken. Um beispielsweise Sicherungen auf die Rootbenutzer-ID zu beschränken, geben Sie den Befehl REGISTER NODE oder UPDATE NODE unter Angabe des Parameters BACKUPINITIATION=root aus:

```
update node backupinitiation=root
```

## Zugriff über Porteinschränkungen einschränken

Schränken Sie den Zugriff auf den Server ein, indem Sie Porteinschränkungen anwenden.

### Informationen zu diesem Vorgang

Gegebenenfalls müssen Sie abhängig von Ihren Sicherheitsanforderungen den Zugriff auf bestimmte Server einschränken. Der IBM Spectrum Protect-Server kann so konfiguriert werden, dass er an vier TCP/IP-Ports empfangsbereit ist: zwei Ports, die für reguläre TCP/IP-Protokolle oder SSL-/TLS-Protokolle verwendet werden können, und zwei Ports, die nur für das SSL-/TLS-Protokoll verwendet werden können.

## Vorgehensweise

Sie können die Serveroptionen wie in Tabelle 1 aufgeführt zur Angabe des erforderlichen Ports festlegen.

Tabelle 1. Serveroptionen und Portzugriff

| Serveroption    | Portzugriff  |
|-----------------|--|
| TCPPORT         | Gibt die Nummer des Ports an, dem der TCP/IP-DFV-Treiber des Servers auf Anforderungen von Clientsitzungen warten soll. Dieser Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen empfangsbereit. Der Standardwert ist 1500.  |
| TCPADMINPORT    | Gibt die Nummer des Ports an, an dem der TCP/IP-DFV-Treiber des Servers auf Anforderungen von anderen Sitzungen als Clientsitzungen warten soll. Dieser Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen empfangsbereit. Der Standardwert ist der Wert für TCPPORT.<br><br>Verwenden Sie diese Option, um den Datenverkehr des Verwaltungsclients vom Datenverkehr des regulären Clients, der die Optionen TCPPORT und SSLTCPSPORT verwendet, zu trennen. |
| SSLTCPSPORT     | Gibt die SSL-TCP/-IP-Portadresse für einen Server an. Dieser Port ist nur für SSL-fähige Sitzungen empfangsbereit. Ein Standardwert für den Port ist nicht verfügbar.  |
| SSLTCPADMINPORT | Gibt die Portadresse an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen von SSL-fähigen Sitzungen wartet. Ein Standardwert für den Port ist nicht verfügbar.<br><br>Verwenden Sie diese Option, um den Datenverkehr des Verwaltungsclients vom Datenverkehr des regulären Clients, der die Optionen TCPPORT und SSLTCPSPORT verwendet, zu trennen.  |

Einschränkungen:

Wenn Sie die Server-Ports, die nur für SSL gelten, (SSLTCPSPORT und SSLTCPADMINPORT) angeben, gelten die folgenden Einschränkungen:

- Wenn Sie den Server-Port, der nur für SSL gilt, für den Parameter LLADDRESS im Befehl DEFINE SERVER oder im Befehl UPDATE SERVER angeben, müssen Sie auch den Parameter SSL=YES angeben.
- Wenn Sie den Server-Port, der nur für SSL gilt, für die Clientoption TCPSPORT angeben, müssen Sie auch YES für die SSL-Clientoption angeben.

### Zugehörige Verweise:

Planung des Firewallzugriffs

# Server stoppen und starten

---

Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.

## Vorbereitende Schritte

---

Um den IBM Spectrum Protect-Server stoppen und starten zu können, müssen Sie über System- oder Bedienerberechtigung verfügen.

- **Server stoppen**  
Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.
- **Server für Verwaltungs- oder Rekonfigurationstasks starten**  
Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

## Server stoppen

---

Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.

## Informationen zu diesem Vorgang

---

Wenn Sie den Befehl HALT zum Stoppen des Servers ausgeben, werden die folgenden Aktionen ausgeführt:

- Alle Prozesse und Clientknotensitzungen werden abgebrochen.
- Alle aktuellen Transaktionen werden gestoppt. (Die Transaktionen werden rückgängig gemacht, wenn der Server erneut gestartet wird.)

## Vorgehensweise

---

Um das System vorzubereiten und den Server zu stoppen, führen Sie die folgenden Schritte aus:

1. Verhindern Sie, dass neue Clientknotensitzungen gestartet werden, indem Sie den Befehl DISABLE SESSIONS ausgeben:

```
disable sessions all
```

2. Bestimmen Sie, ob Clientknotensitzungen oder -prozesse aktiv sind, indem Sie die folgenden Schritte ausführen:
  - a. Rufen Sie die Seite Übersicht im Operations Center auf, auf der im Bereich Aktivität die Gesamtzahl Prozesse und Sitzungen angezeigt wird, die derzeit aktiv sind. Wenn die Zahlen erheblich von den Zahlen abweichen, die normalerweise während Ihrer täglichen Speicherverwaltungsroutine angezeigt werden, überprüfen Sie mithilfe weiterer Statusanzeiger im Operations Center, ob ein Problem vorliegt.
  - b. Zeigen Sie das Diagramm im Bereich Aktivität an, um den Umfang des Datenaustauschs im Netz für die folgenden Perioden zu vergleichen:
    - Die laufende Periode, d. h. die letzte 24-Stunden-Periode
    - Die vorherige Periode, d. h. die 24 Stunden vor der laufenden PeriodeWenn das Diagramm für die vorherige Periode den erwarteten Umfang des Datenaustauschs darstellt, können deutliche Abweichungen in dem Diagramm für die laufende Periode auf ein Problem hindeuten.
  - c. Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details. Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, rufen Sie mithilfe von Verwaltungsbefehlen Informationen zu Prozessen ab. Geben Sie den Befehl QUERY PROCESS aus, um Prozesse abzufragen; geben Sie den Befehl QUERY SESSION aus, um Informationen zu Sitzungen abzurufen.
3. Warten Sie, bis die Clientknotensitzungen abgeschlossen sind oder brechen Sie diese ab. Um Prozesse und Sitzungen abzubrechen, führen Sie die folgenden Schritte aus:
  - Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details.
  - Klicken Sie auf die Registerkarte Aktive Tasks und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
  - Klicken Sie auf Abbrechen.

- Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, brechen Sie Sitzungen mithilfe von Verwaltungsbefehlen ab. Geben Sie den Befehl CANCEL SESSION aus, um eine Sitzung abubrechen; geben Sie den Befehl CANCEL PROCESS aus, um Prozesse abubrechen.  
Tipp: Wenn der Prozess, der abgebrochen werden soll, auf die Bereitstellung eines Banddatenträgers wartet, wird die Mountainforderung abgebrochen. Wenn Sie beispielsweise einen Befehl EXPORT, IMPORT oder MOVE DATA ausgeben, leitet der Befehl möglicherweise einen Prozess ein, der die Bereitstellung eines Banddatenträgers erfordert. Wenn jedoch ein Banddatenträger durch ein automatisiertes Speicherarchiv bereitgestellt wird, wird die Abbruchoperation unter Umständen erst wirksam, wenn der Bereitstellungsprozess abgeschlossen ist. Abhängig von Ihrer Systemumgebung kann dies mehrere Minuten dauern.

4. Stoppen Sie den Server, indem Sie den Befehl HALT ausgeben:

```
halt
```

## Server für Verwaltungs- oder Rekonfigurationstasks starten

---

Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

### Informationen zu diesem Vorgang

---

Starten Sie den Server im Verwaltungsmodus, indem Sie das Dienstprogramm DSMSERV mit dem Parameter MAINTENANCE ausführen.

Im Verwaltungsmodus sind die folgenden Operationen inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Konsolidierung von Speicherbereich auf dem Server
- Bestandsverfall
- Umlagerung von Speicherpools

Darüber hinaus wird verhindert, dass Clients Sitzungen mit dem Server starten können.

Tipps:

- Sie müssen die Serveroptionsdatei, dmserv.opt, nicht editieren, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Speicherbereichskonsolidierung, den Bestandsverfall und Umlagerungsprozesse für Speicherpools manuell starten.

### Vorgehensweise

---

Um den Server im Verwaltungsmodus zu starten, geben Sie den folgenden Befehl aus:

```
dmserv maintenance
```

Tipp: Informationen zum Anzeigen eines Ein Video zum Starten des Servers im Verwaltungsmodus kann über Server im Verwaltungsmodus starten angezeigt werden.




### Nächste Schritte

---

Um Serveroperationen im Produktionsmodus wiederaufzunehmen, führen Sie die folgenden Schritte aus:

1. Fahren Sie den Server herunter, indem Sie den Befehl HALT ausgeben:

```
halt
```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden. Führen Sie die Anweisungen für Ihr Betriebssystem aus:
  -  AIX-BetriebssystemeServerinstanz starten
  -  Linux-BetriebssystemeServerinstanz starten
  -  Windows-BetriebssystemeServerinstanz starten

Operationen, die im Verwaltungsmodus inaktiviert waren, werden wieder aktiviert.

## Durchführung eines Upgrades für den Server planen

---

Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.

## Informationen zu diesem Vorgang

---

Beachten Sie diese Richtlinien:

- Bei der bevorzugten Methode erfolgt das Upgrade für den Server mithilfe des Installationsassistenten. Nachdem Sie den Assistenten gestartet haben, klicken Sie im Fenster IBM Installation Manager auf das Symbol zum Aktualisieren; klicken Sie nicht auf das Symbol zum Installieren oder Ändern!
- Wenn sowohl für die Serverkomponente als auch für die Operations Center-Komponente Upgrades verfügbar sind, wählen Sie die Kontrollkästchen aus, um das Upgrade für beide Komponenten durchzuführen.

## Vorgehensweise




---

1. Überprüfen Sie die Liste der Fixpacks und vorläufigen Fixes. Siehe Technote 1239415.
2. Studieren Sie die Produktverbesserungen, die in der Readme-Datei beschrieben sind.  
Tipp: Wenn Sie die Installationspaketdatei von der IBM Spectrum Protect-Unterstützungssite abrufen, können Sie auch auf die Readme-Datei zugreifen.
3. Stellen Sie sicher, dass die Version, auf die das Upgrade für Ihren Server durchgeführt wird, mit anderen Komponenten, wie beispielsweise Speicheragenten und Speicherarchivclients, kompatibel ist. Siehe Technote 1302789.
4. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden. Siehe Technote 1053218.
5. Lesen Sie die Upgradeanweisungen. Stellen Sie sicher, dass Sie die Serverdatenbank, die Einheitenkonfigurationsinformationen und die Protokolldatei für Datenträger sichern.

## Nächste Schritte

---

Um ein Fixpack oder einen vorläufigen Fix zu installieren, führen Sie die Anweisungen für Ihr Betriebssystem aus:

-  AIX-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
-  Linux-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
-  Windows-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren

### Zugehörige Informationen:

 Upgrade- und Umlagerungsprozess - Häufig gestellte Fragen

## Vorbereitungen für einen Ausfall oder eine Systemaktualisierung

---

Treffen Sie Vorbereitungen in IBM Spectrum Protect, damit Ihr System während eines geplanten Stromausfalls oder einer geplanten Systemaktualisierung in einem konsistenten Zustand verbleibt.

## Informationen zu diesem Vorgang

---

Stellen Sie sicher, dass Sie die regelmäßige Ausführung von Aktivitäten planen, um den Server zu verwalten und zu schützen.

## Vorgehensweise

---

1. Brechen Sie Prozesse und Sitzungen, die aktiv sind, ab, indem Sie die folgenden Schritte ausführen:
  - a. Wählen Sie im Operations Center auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details.
  - b. Klicken Sie auf die Registerkarte Aktive Tasks und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
  - c. Klicken Sie auf Abbrechen.
2. Stoppen Sie den Server, indem Sie den Befehl HALT ausgeben:

```
halt
```

Tipp: Sie können den Befehl HALT im Operations Center ausgeben, indem Sie den Mauszeiger über das Symbol für Einstellungen bewegen und auf Command Builder klicken. Wählen Sie dann den Server aus, geben Sie `halt` ein und drücken Sie die Eingabetaste.

## Plan zur Wiederherstellung nach einem Katastrophenfall implementieren

---

Implementieren Sie eine Strategie zur Wiederherstellung nach einem Katastrophenfall, um Ihre Anwendungen in einem Katastrophenfall wiederherstellen und hohe Serververfügbarkeit sicherstellen zu können.

## Informationen zu diesem Vorgang

Bestimmen Sie Ihre Anforderungen für die Wiederherstellung nach einem Katastrophenfall, indem Sie die Geschäftsprioritäten für die Clientknotenwiederherstellung und die Systeme, die zum Wiederherstellen von Daten verwendet werden, angeben und prüfen, ob Clientknoten über eine Verbindung zu einem Wiederherstellungsserver verfügen. Verwenden Sie zum Schützen von Daten Replikation und Speicherpoolschutz. Außerdem müssen Sie bestimmen, wie oft Verzeichniscontainerspeicherpools geschützt werden.

- **Wiederherstellungsdrilloperationen ausführen**  
Planen Sie Drilloperationen für die Wiederherstellung nach einem Katastrophenfall als Vorbereitung für Prüfungen, mit denen die Wiederherstellbarkeit des IBM Spectrum Protect-Servers bestätigt wird, und um sicherzustellen, dass nach einem Ausfall Daten zurückgeschrieben und Operationen wiederaufgenommen werden können. Mithilfe einer Drilloperation können Sie außerdem vor dem Eintreten einer kritischen Situation sicherstellen, dass alle Daten zurückgeschrieben und Operationen wiederaufgenommen werden können.

## Wiederherstellung nach einem Systemausfall

Bei IBM Spectrum Protect-Plattenspeicherlösungen für einen einzelnen Standort können Sie den Bestand nur lokal wiederherstellen und die Datenbank zum Schutz Ihrer Daten zurückschreiben.

### Vorgehensweise

Verwenden Sie abhängig vom Typ der gesicherten Informationen eine der folgenden Methoden, um den Bestand an einem lokalen Standort wiederherzustellen.

Einschränkung: Da bei Plattenspeicherlösungen für einen einzelnen Standort keine zweite Kopie des Speicherpools vorhanden ist, können Speicherpools nicht zurückgeschrieben werden. Informationen zur Architektur von Plattenspeicherlösungen finden Sie in IBM Spectrum Protect-Lösung auswählen.

Tabelle 1. Szenarios für die Wiederherstellung nach einem Katastrophenfall

| Szenario   | Prozedur   |
|--|--|
| Der Zugriff auf Ihr System ist nicht möglich und das System soll mithilfe von Systemtools lokal mit dem Stand einer früheren Version zurückgeschrieben werden. | <ul style="list-style-type: none"> <li>• Verwenden Sie IBM Spectrum Protect, um den Server auf einem anderen Server zu sichern.</li> <li>• Verwenden Sie Betriebssystemtools, um Ihr System zu sichern und mit dem Stand einer früheren Version zurückzuschreiben.</li> </ul>  |
| Bei einem Ausfall oder einer Katastrophe sollen Ihre Daten aus gesicherten Versionen der Daten zurückgeschrieben werden.                                       | <ul style="list-style-type: none"> <li>• Um einen Client zu sichern, wählen Sie auf der Seite TSM-Clients im Operations Center die Clients aus, die gesichert werden sollen, und klicken Sie auf Sichern.</li> <li>• Wählen Sie auf der Seite TSM-Server im Operations Center den Server aus, dessen Datenbank gesichert werden soll. Klicken Sie auf Sichern und führen Sie die Anweisungen im Fenster Serverdatenbank sichern aus.</li> </ul> <p>Um einen Speicherpool aus einer gesicherten Version des Speicherpools zurückzuschreiben, müssen Sie die Datenbank zurückschreiben. Geben Sie den Befehl <code>DSMSERV RESTORE DB</code> aus, um die Datenbank und zugehörige Speicherpools mit dem Stand einer gesicherten Version zurückzuschreiben.</p> |

- **Datenbank zurückschreiben**  
Unter Umständen müssen Sie die IBM Spectrum Protect-Datenbank nach einem Katastrophenfall zurückschreiben. Sie können die Datenbank mit dem neuesten Stand oder mit dem Stand eines angegebenen Zeitpunkts zurückschreiben. Zum Zurückschreiben der Datenbank benötigen Sie Datenträger mit einer Datenbankgesamt-, -teil- oder -momentaufnahmesicherung.

#### Zugehörige Verweise:

- ➔ [AUDIT CONTAINER](#) (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)
- ➔ [DSMSERV RESTORE DB](#) (Datenbank zurückschreiben)



## Plattenspeicherlösung für mehrere Standorte

---

Diese Datenschutzlösung stellt Replikation an mehreren Standorten bereit, sodass jeder Server Daten für den jeweils anderen Standort schützt.

- Planung für eine Plattenspeicherdatenschutzlösung für mehrere Standorte  
Planung für eine Plattenspeicherdatenschutzlösung für mehrere Standorte mit Servern an zwei Standorten, die Datendeduplizierung und Replikation verwenden.
- Implementierung einer Plattenspeicherdatenschutzlösung für mehrere Standorte  
Die Plattenspeicherlösung für mehrere Standorte wird an zwei Standorten konfiguriert und verwendet Datendeduplizierung und Replikation.
- Plattenspeicherlösung für mehrere Standorte überwachen  
Überwachen Sie nach der Implementierung einer Plattenspeicherlösung für mehrere Standorte mit IBM Spectrum Protect die Lösung, um ihre korrekte Funktionsweise sicherzustellen. Indem die Lösung täglich und regelmäßig überwacht wird, können Sie bestehende und potenzielle Probleme erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden.
- Operationen für eine Plattenspeicherlösung für mehrere Standorte verwalten  
Verwenden Sie diese Informationen, um Operationen für eine Plattenspeicherlösung für mehrere Standorte mit IBM Spectrum Protect zu verwalten, die einen Server umfasst und Datendeduplizierung für mehrere Standorte verwendet.

## Planung für eine Plattenspeicherdatenschutzlösung für mehrere Standorte

---

Planung für eine Plattenspeicherdatenschutzlösung für mehrere Standorte mit Servern an zwei Standorten, die Datendeduplizierung und Replikation verwenden.

### Implementierungsmethoden

---

Sie können Server für eine Plattenspeicherlösung für mehrere Standorte wie folgt konfigurieren:

Server unter Verwendung des Operations Center und von Verwaltungsbefehlen konfigurieren

Sie können eine Reihe von Speichersystemen und die Server-Software für Ihre Lösung konfigurieren. Konfigurationstasks werden mithilfe von Assistenten und Optionen im Operations Center und mithilfe von IBM Spectrum Protect-Befehlen ausgeführt. Informationen zu ersten Schritten finden Sie in Planungsroadmap.

Server mithilfe automatisierter Scripts konfigurieren

Eine ausführliche Anleitung zur Konfiguration mit bestimmten IBM® Storwize-Speichersystemen sowie zur Verwendung automatisierter Scripts zur Konfiguration jedes Servers finden Sie in den IBM Spectrum Protect-Blueprints. Die Dokumentation und Scripts sind unter IBM developerWorks verfügbar: IBM Spectrum Protect Blueprints.

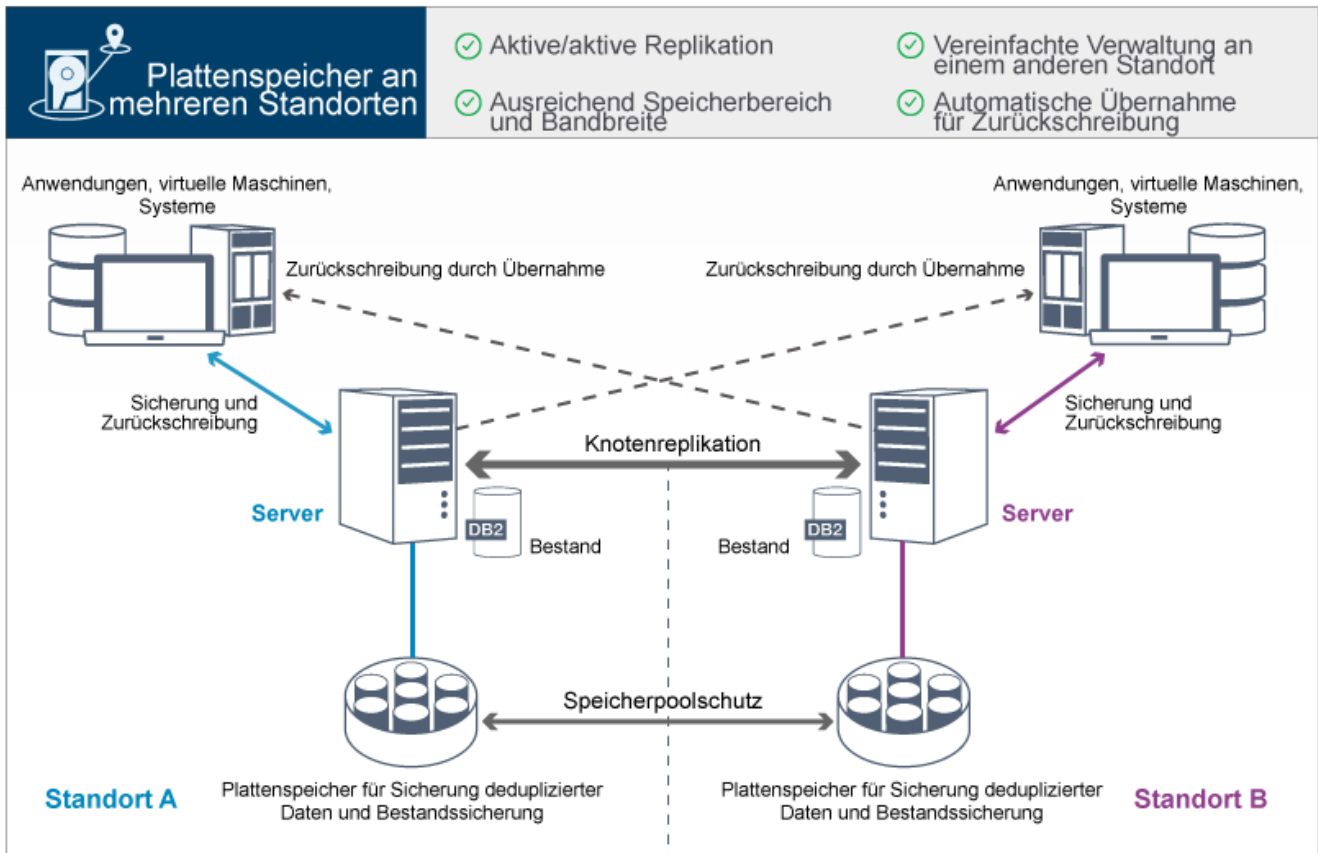
Die Blueprint-Dokumentation umfasst keine Schritte zum Installieren und Konfigurieren des Operations Center oder zum Konfigurieren der sicheren Kommunikation mithilfe von Transport Security Layer (TLS). Die Replikation wird unter Verwendung von Befehlen im Anschluss an die Konfiguration des Servers konfiguriert. Eine Option zur Verwendung von Elastic Storage Server-Speicher auf der Basis der Technologie von IBM Spectrum Scale ist eingeschlossen.

### Planungsroadmap

---

Planen Sie eine Plattenspeicherlösung für mehrere Standorte, indem Sie das Architekturlayout in der folgenden Abbildung überprüfen und dann die Roadmap-Tasks ausführen, die auf die Abbildung folgen.

Abbildung 1. Plattenspeicherlösung für mehrere Standorte



Die folgenden Schritte sind für die korrekte Planung für eine Plattenspeicherumgebung an mehreren Standorten erforderlich.

1. Wählen Sie Ihre Systemgröße aus.
2. Führen Sie die Planung für die Standorte aus.
3. Erfüllen Sie die Systemvoraussetzungen für Hardware und Software.
4. Notieren Sie die Werte für Ihre Systemkonfiguration in den Arbeitsblättern zur Planung.
5. Führen Sie die Planung für den Speicher durch.
6. Führen Sie die Planung für die Sicherheit durch.
  - a. Führen Sie die Planung für Administratorrollen durch.
  - b. Führen Sie die Planung für die sichere Kommunikation durch.
  - c. Führen Sie die Planung für verschlüsselte Daten durch.
  - d. Führen Sie die Planung für den Firewallzugriff durch.

## Systemgröße auswählen

Wählen Sie die Größe des IBM Spectrum Protect-Servers auf der Basis des verwalteten Datenvolumens und der Systeme, die geschützt werden müssen, aus.

### Informationen zu diesem Vorgang

Mithilfe der Informationen in der Tabelle können Sie auf der Basis des verwalteten Datenvolumens die erforderliche Größe des Servers bestimmen.

In der folgenden Tabelle ist das Datenvolumen aufgeführt, das von einem Server verwaltet wird. Dieses Volumen umfasst alle Versionen. Das tägliche Datenvolumen gibt an, wie viele neue Daten täglich gesichert werden. Sowohl das Gesamtvolumen der verwalteten Daten als auch das tägliche Volumen an neuen Daten wird als Größe vor jeglicher Datenreduktion gemessen.

Tabelle 1. Größe des Servers bestimmen

| Gesamtvolumen der verwalteten Daten | Volumen an täglich zu sichernden neuen Daten | Erforderliche Servergröße |
|-------------------------------------|--|---------------------------|
| 60 TB bis 240 TB                    | Bis zu 10 TB pro Tag                         | Klein                     |
| 196 TB bis 784 TB                   | 10 bis 20 TB pro Tag                         | Mittelgroß                |
| 1000 TB bis 4000 TB                 | 20 bis 100 TB pro Tag                        | Groß                      |

Die Werte für die tägliche Sicherung in der Tabelle basieren auf Testergebnissen für Objekte mit einer Größe von 128 MB, die von IBM Spectrum Protect for Virtual Environments verwendet werden. Bei Workloads, die aus Objekten bestehen, die kleiner als 128 KB sind, werden diese Grenzwerte für tägliche Sicherungen möglicherweise nicht erreicht.

## Planung der Standorte

---

Überprüfen Sie Anwendungsfälle und bewerten Sie die Faktoren, um den effizientesten Datenschutz für die Plattenspeicherlösung für mehrere Standorte in IBM Spectrum Protect bereitzustellen.

### Anwendungsfälle

---

Bei der Plattenspeicherlösung für mehrere Standorte wird mindestens eine Kopie gesicherter Daten erstellt. Wenn sich die IBM Spectrum Protect-Server an unterschiedlichen Standorten befinden, werden die gesicherten Replikate an einem anderen Standort aufbewahrt.

Tipp: Verhindern Sie Konflikte bei der Verwaltung von Verwaltungs-IDs und Clientoptionsgruppen, indem Sie die IDs und Optionsgruppen, die auf dem Zielsystem repliziert werden, und die IDs und Optionsgruppen, die in einer unternehmensweiten Konfiguration verwaltet werden, identifizieren. Es ist nicht möglich, eine Benutzer-ID mit Administratorberechtigung für einen registrierten Knoten zu definieren, wenn für denselben Knoten eine Verwaltungs-ID vorhanden ist.

Ihr Unternehmen könnte aus verschiedenen Gründen von einer Plattenspeicherlösung für mehrere Standorte profitieren, die häufigsten Gründe für die Verwendung einer Plattenspeicherlösung für mehrere Standorte umfassen jedoch die folgenden Replikationsszenarios:

Replikation vom primären Standort zum Standort für die Wiederherstellung nach einem Katastrophenfall

In diesem Szenario werden Daten, die am primären Standort (Standort A) gesichert werden, auf einen Server am sekundären Standort (Standort B), dem Standort für die Wiederherstellung nach einem Katastrophenfall, repliziert. Bei einer Katastrophe an Standort A, beispielsweise dem Ausfall des Servers, können Sie Systeme mithilfe des Servers an Standort B wiederherstellen. Sie können auch stattdessen mithilfe des Servers an Standort A Daten in primären Speicherpools an Standort B zurückschreiben, beispielsweise nach einem Plattenspeicherfehler an Standort B.

Gegenseitige Replikation an zwei aktiven Standorten

In diesem Szenario werden lokale Daten an jedem Standort von den Servern an beiden Standorten, Standort A und Standort B, gesichert. Daten, die an Standort A gesichert werden, werden an Standort B repliziert und Daten, die an Standort B gesichert werden, werden an Standort A repliziert. Wenn Daten, die gesichert wurden, an Standort A verloren gehen, können Sie Speicherpooldaten mithilfe des Servers an Standort B auf dem Server an Standort A wiederherstellen. Wenn Standort A nicht mehr verfügbar ist, können Sie die replizierten Daten für Standort A auf einem neuen System an Standort B wiederherstellen. Sie müssen die Größe der Serverressourcen ändern, um sicherzustellen, dass beide Server über ausreichend Kapazität zum Sichern und Zurückschreiben aller Clientknoten im Rahmen Ihres Plans zur Wiederherstellung nach einem Katastrophenfall verfügen.

Schutz ferner Server am primären Standort

In diesem Szenario konfigurieren Sie ferne Server, die relativ klein sind, für die Replikation von Daten, die auf einem größeren Server am primären Standort gesichert werden. Wenn die Bandbreite begrenzt ist, ist die Zurückschreibung von Systemen an die fernen Standorte unter Umständen nicht praktikabel. In diesem Fall können Sie Systeme, falls gewünscht, am primären Standort wiederherstellen, bevor die gesicherten Daten auf die fernen Server repliziert werden.

## Zu bewertende Faktoren

---

Bewerten Sie vor der Implementierung einer Plattenspeicherlösung für mehrere Standorte die folgenden Faktoren:

Netzbandbreite

Das Netz muss über genügend Bandbreite für die erwarteten Datenübertragungen zwischen Knoten, für die Replikation und für die standortübergreifenden Zurückschreibungsoperationen verfügen, die für die Wiederherstellung nach einem Katastrophenfall erforderlich sind. Bevor Sie mit dem Testen des Replikationsdurchsatzes fortfahren, müssen Sie sicherstellen, dass Ihr Netz den Replikationsdatenverkehr handhaben kann. Berechnen Sie die für den stabilen Zustand erforderliche Netzbandbreite, indem Sie die Richtlinien in Für die Replikation erforderliche Netzbandbreite schätzen (Version 7.1.1) anwenden.

Die Netzverbindung ist häufig eine gemeinsam genutzte Ressource. Planen Sie die Uhrzeit, zu der die Knotenreplikation ausgeführt werden soll, um einen Konflikt mit anderen Ressourcennutzern zu verhindern. Gegebenenfalls kann die Aktivität mithilfe von Netzsteuerelementen auch auf einen Teil der Bandbreite beschränkt werden. In IBM Spectrum Protect sind keine Steuerelemente zur Beschränkung der Netzauslastung verfügbar.

Ressourcen für die Erstreplikation

Um eine Datenschutzlösung für zwei Standorte zu konfigurieren, müssen Sie Daten zunächst von Standort A auf den Zielsystem an Standort B replizieren. Um sicherzustellen, dass die Erstreplikation erfolgreich ist, müssen Sie bestimmen, ob die zum Replizieren

der Daten erforderliche Netzbandbreite, Prozessorressourcen und Zeit verfügbar sind. Unter Umständen müssen Sie die Replikation der ersten Gesamtsicherungen für mehrere Tage planen. Wenn der Zeitplan für die Erstsicherungen nicht erweitert werden kann, können Sie Daten von Standort A an Standort B replizieren, ohne das Netz zu verwenden. Sie können beispielsweise die gesicherten Daten mithilfe von Datenträgern exportieren und importieren oder den Quellen- und Zielsever vorübergehend an denselben Standort verlegen.

#### Tägliche Datenaufnahme

Bei der Plattenspeicherlösung für mehrere Standorte muss die tägliche Datenaufnahme und die Aufbewahrung aller Daten innerhalb der Kapazität der Konfigurationen liegen. Beispielsweise liegt bei einer großen Konfiguration die Kapazität der Datenaufnahme bei bis zu 100 TB pro Tag einschließlich Knotenreplikation. In Fällen, in denen die Sicherungsanforderungen die Kapazität eines einzelnen Servers überschreiten, können Sie eine Lösung konfigurieren, die mehrere Server zum Erreichen der erforderlichen Kapazität verwendet.

#### Serverkonfiguration

Die Serverkonfiguration muss die Anforderungen der Plattenspeicherlösung für mehrere Standorte erfüllen oder überschreiten.

#### Einzelnes Replikat gesicherter Daten

Die Plattenspeicherlösung für mehrere Standorte ist am effizientesten, wenn eine einzelne ausgelagerte Kopie der gesicherten Daten Ihre Anforderungen in Bezug auf Datenschutz und Risikominderung erfüllt. In diesem Fall wird die einzelne ausgelagerte Kopie der Daten am Standort eines Replikationsservers aufbewahrt.

#### Zugehörige Verweise:

Systemvoraussetzungen für eine Plattenspeicherlösung für mehrere Standorte

## Systemvoraussetzungen für eine Plattenspeicherlösung für mehrere Standorte

Überprüfen Sie nach der Auswahl der besten IBM Spectrum Protect-Lösung für Ihre Datenschutzerfordernungen die Systemvoraussetzungen, um die Planung für die Implementierung der Datenschutzlösung auszuführen.

Stellen Sie sicher, dass Ihr System die Hardware- und Softwarevoraussetzungen für die geplante Größe des Servers erfüllt.

- **Hardwarevoraussetzungen**  
Hardwarevoraussetzungen für Ihre IBM Spectrum Protect-Lösung basieren auf der Systemgröße. Wählen Sie funktional entsprechende oder bessere Komponenten als die aufgelisteten aus, um optimale Leistung für Ihre Umgebung zu gewährleisten.
- **Softwarevoraussetzungen**  
Die Dokumentation für die IBM Spectrum Protect-Plattenspeicherlösung für mehrere Standorte umfasst Installations- und Konfigurationstasks für die folgenden Betriebssysteme. Die aufgelisteten Softwaremindestvoraussetzungen müssen erfüllt sein.

#### Zugehörige Informationen:










 [IBM Spectrum Protect Supported Operating Systems](#)

## Hardwarevoraussetzungen

Hardwarevoraussetzungen für Ihre IBM Spectrum Protect-Lösung basieren auf der Systemgröße. Wählen Sie funktional entsprechende oder bessere Komponenten als die aufgelisteten aus, um optimale Leistung für Ihre Umgebung zu gewährleisten.

Eine Definition der Systemgrößen finden Sie in Systemgröße auswählen.

In der folgenden Tabelle sind die Hardwaremindestvoraussetzungen für den Server und Speicher auf der Basis der Größe Servers aufgelistet, der erstellt werden soll. Wenn Sie logische Partitionen (LPARs) oder Arbeitspartitionen (WPARs) verwenden, passen Sie die Netzvoraussetzungen an, um den Partitionsgrößen Rechnung zu tragen.

| Hardwarekomponente | Kleines System  | Mittelgroßes System   | Großes System   |
|--------------------|---|---|---|
| Serverprozessor    |  AIX-Betriebssysteme6<br>Prozessorkerne, 3,42 GHz oder schneller<br><br> Linux-Betriebssysteme<br> Windows-Betriebssysteme12<br>Prozessorkerne, 1,9 GHz oder schneller |  AIX-Betriebssysteme8<br>Prozessorkerne, 3,42 GHz oder schneller<br><br> Linux-Betriebssysteme<br> Windows-Betriebssysteme16<br>Prozessorkerne, 2,0 GHz oder schneller |  AIX-Betriebssysteme20<br>Prozessorkerne, 3,42 GHz<br><br> Linux-Betriebssysteme<br> Windows-Betriebssysteme32<br>Prozessorkerne, 2,0 GHz oder schneller |

| Hardwarekomponente | Kleines System  | Mittelgroßes System  | Großes System   |
|--------------------|---|--|---|
| Serverspeicher     | 64 GB RAM   | 128 GB RAM   | 192 GB RAM  |
| Netz               | <ul style="list-style-type: none"> <li>• 10 GB Ethernet (1 Port)</li> <li>• 8 GB Fibre Channel-Adapter (2 Ports)</li> </ul>   | <ul style="list-style-type: none"> <li>• 10 GB Ethernet (2 Ports)</li> <li>• 8 GB Fibre Channel-Adapter (2 Ports)</li> </ul>   | <ul style="list-style-type: none"> <li>• 10 GB Ethernet (4 Ports)</li> <li>• 8 GB Fibre Channel-Adapter (4 Ports)</li> </ul>  |
| Speicher           | <ul style="list-style-type: none"> <li>• 1,3 TB Bestand plus Speicherbereich für Operations Center-Datensätze</li> <li>• 46 TB deduplizierter Verzeichniscontainerspeicherpool</li> </ul> | <ul style="list-style-type: none"> <li>• 2 TB Bestand plus Speicherbereich für Operations Center-Datensätze</li> <li>• 200 TB deduplizierter Verzeichniscontainerspeicherpool</li> </ul> | <ul style="list-style-type: none"> <li>• 6 TB Bestand plus Speicherbereich für Operations Center-Datensätze</li> <li>• 1000 TB deduplizierter Verzeichniscontainerspeicherpool</li> </ul> |

## Speicherbedarf für die Datenbank für das Operations Center schätzen

Hardwarevoraussetzungen für das Operations Center sind mit Ausnahme des Speicherbereichs für die Datenbank und das Archivprotokoll (Bestand), den das Operations Center zum Aufnehmen von Datensätzen für verwaltete Clients verwendet, in die vorherige Tabelle eingeschlossen.

Wenn Sie nicht planen, das Operations Center auf demselben System wie den Server zu installieren, können Sie die Systemanforderungen separat schätzen. Informationen zum Berechnen der Systemanforderungen für das Operations Center enthält die Technote 1641684 für die Berechnungsfunktion der Systemanforderungen.

Die Verwaltung des Operations Center auf dem Server stellt eine Workload dar, die zusätzlichen Speicherbereich für Datenbankoperationen erfordert. Wie viel Speicherbereich erforderlich ist, ist von der Anzahl Clients abhängig, die auf einem Server überwacht werden. Lesen Sie die folgenden Richtlinien, um schätzen zu können, wie viel Speicherbereich Ihr Server erfordert.

### Speicherbereich in der Datenbank

Das Operations Center benötigt ungefähr 1,2 GB Speicherbereich in der Datenbank pro 1000 Clients, die auf einem Server überwacht werden. Angenommen, ein Hub-Server überwacht 2000 Clients und verwaltet außerdem drei Peripherieserver mit jeweils 1500 Clients. Bei dieser Konfiguration sind insgesamt 6500 Clients auf den vier Servern vorhanden und ungefähr 8,4 GB Speicherbereich in der Datenbank erforderlich. Bei der Berechnung dieses Werts werden die 6500 Clients auf den nächsthöheren Tausenderwert aufgerundet, d. h. auf 7000:

$$7 \times 1,2 \text{ GB} = 8,4 \text{ GB}$$

### Speicherbereich für das Archivprotokoll

Das Operations Center verwendet alle 24 Stunden ungefähr 8 GB Speicherbereich für das Archivprotokoll pro 1000 Clients. In dem Beispiel mit den 6500 Clients auf dem Hub-Server und den Peripherieservern werden in einem Zeitraum von 24 Stunden für den Hub-Server 56 GB Speicherbereich für das Archivprotokoll verwendet.

Für jeden Peripherieserver in dem Beispiel werden im Verlauf von 24 Stunden etwa 16 GB Speicherbereich für das Archivprotokoll verwendet. Diese Schätzungen basieren auf dem Standardintervall von 5 Minuten zur Erfassung von Statusdaten. Wenn Sie das Erfassungsintervall von einmal alle 5 Minuten auf einmal alle 3 Minuten reduzieren, erhöht sich der Speicherbedarf. Das folgende Beispiel zeigt die ungefähre Erhöhung des Protokollspeicherbedarfs bei einem Erfassungsintervall von einmal alle 3 Minuten:

- Hub-Server: von 56 GB auf ungefähr 94 GB
- Jeder Peripherieserver: von 16 GB auf ungefähr 28 GB

Vergrößern Sie den Speicherbereich für das Archivprotokoll, sodass genügend Speicherbereich zur Unterstützung des Operations Center ohne Auswirkungen auf die vorhandenen Serveroperationen verfügbar ist.

## Hardwarevoraussetzungen für den zweiten Server

Wenn Sie planen, Ihre Standorte so zu konfigurieren, dass alle Daten am ersten Standort an den zweiten Standort repliziert werden, sind die Hardwarevoraussetzungen an beiden Standorten identisch. Soll nur ein Teil der Daten an Ihren zweiten Standort repliziert werden, können die Speicher- und Netzvoraussetzungen geringer ausfallen.

## Softwarevoraussetzungen

Die Dokumentation für die IBM Spectrum Protect-Plattenspeicherlösung für mehrere Standorte umfasst Installations- und Konfigurationstasks für die folgenden Betriebssysteme. Die aufgelisteten Softwaremindestvoraussetzungen müssen erfüllt sein.

Informationen zu den Softwarevoraussetzungen für IBM® lin\_tape-Einheitentreiber finden Sie in der Veröffentlichung IBM Tape Device Drivers Installation and User's Guide.

## AIX-Systeme

| Softwaretyp           | Softwaremindestvoraussetzungen   |
|-----------------------|--|
| Betriebssystem        | IBM AIX 7.1<br><br>Weitere Informationen zu Betriebssystemvoraussetzungen finden Sie in AIX: Systemmindestvoraussetzungen für AIX-Systeme.   |
| Dienstprogramm gunzip | Das Dienstprogramm gunzip muss auf Ihrem System verfügbar sein, bevor Sie die Installation oder das Upgrade für den IBM Spectrum Protect-Server ausführen. Stellen Sie sicher, dass das Dienstprogramm gunzip installiert ist und der Pfad zu diesem Dienstprogramm in der Umgebungsvariablen PATH definiert ist.  |
| Dateisystemtyp        | JFS2-Dateisysteme<br><br>AIX-Systeme können ein großes Volumen an Dateisystemdaten zwischenspeichern, wodurch der Speicherplatz, der für Server- und IBM DB2-Prozesse erforderlich ist, reduziert werden kann. Um beim AIX-Server eine Auslagerung zu verhindern, verwenden Sie die Mountoption rbrw für das JFS2-Dateisystem. Für den Dateisystemcache wird weniger Speicher verwendet und für IBM Spectrum Protect ist mehr Speicher verfügbar.<br><br>Verwenden Sie nicht die Mountoptionen für Dateisysteme, gleichzeitige E/A (CIO = Concurrent I/O) und direkte E/A (DIO = Direct I/O) für Dateisysteme, die die IBM Spectrum Protect-Datenbank, Protokolle oder Speicherpooldatenträger enthalten. Diese Optionen können eine Leistungsverschlechterung vieler Serveroperationen zur Folge haben. IBM Spectrum Protect und DB2 können, wenn dies von Vorteil ist, weiterhin DIO verwenden, IBM Spectrum Protect erfordert die Mountoptionen jedoch nicht, um die Vorteile dieser Verfahren selektiv nutzen zu können. |
| Andere Software       | Korn-Shell (ksh)   |

## Linux-Systeme

| Softwaretyp     | Softwaremindestvoraussetzungen   |
|-----------------|--|
| Betriebssystem  | Red Hat Enterprise Linux 7 (x86_64)  |
| Bibliotheken    | GNU C-Bibliotheken, Version 2.3.3-98.38 oder höher, die auf dem IBM Spectrum Protect-System installiert sind.<br>Red Hat Enterprise Linux-Server: <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 (32-Bit- und 64-Bit-Pakete sind erforderlich)</li> <li>• numactl.x86_64</li> </ul> |
| Dateisystemtyp  | Formatieren Sie datenbankbezogene Dateisysteme mit ext3 oder ext4.<br><br>Verwenden Sie für speicherpoolbezogene Dateisysteme XFS.   |
| Andere Software | Korn-Shell (ksh)   |

## Windows-Systeme

| Softwaretyp    | Softwaremindestvoraussetzungen                                     |
|----------------|--|
| Betriebssystem | Microsoft Windows Server 2012 R2 (64-Bit) oder Windows Server 2016 |
| Dateisystemtyp | NTFS   |

| Softwaretyp     | Softwaremindestvoraussetzungen  |
|-----------------|---|
| Andere Software | <p>Windows 2012 R2 oder Windows 2016 mit .NET Framework 3.5 ist installiert und aktiviert.</p> <p>Die folgenden Benutzerkontensteuerungsrichtlinien müssen inaktiviert sein:</p> <ul style="list-style-type: none"> <li>• Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto</li> <li>• Benutzerkontensteuerung: Alle Administratoren im Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen</li> </ul> |

**Zugehörige Tasks:**

- ➔ AIX-Netzoptionen definieren

## Arbeitsblätter zur Planung

Verwenden Sie die Arbeitsblätter zur Planung für die Aufzeichnung von Werten, die Sie bei der Konfiguration Ihres Systems und bei der Konfiguration des IBM Spectrum Protect-Servers verwenden. Verwenden Sie die Best-Practice-Standardwerte, die in den Arbeitsblättern aufgeführt sind.

Jedes Arbeitsblatt unterstützt Sie bei den Vorbereitungen für unterschiedliche Teile der Systemkonfiguration mithilfe der Best-Practice-Werte:

**Vorkonfiguration des Serversystems**

Führen Sie mithilfe der Arbeitsblätter zur Vorkonfiguration die Planung für die Dateisysteme und Verzeichnisse aus, die erstellt werden sollen, wenn Sie während der Systemkonfiguration Dateisysteme für IBM Spectrum Protect konfigurieren. Alle Verzeichnisse, die Sie für den Server erstellen, müssen leer sein.

**Serverkonfiguration**

Verwenden Sie die Arbeitsblätter zur Konfiguration, wenn Sie den Server konfigurieren. Für die meisten Elemente werden Standardwerte vorgeschlagen; andernfalls ist ein entsprechender Hinweis vorhanden.

## AIX

Tabelle 1. Arbeitsblatt für die Vorkonfiguration eines AIX-Serversystems

| Element   | Standardwert            | Eigener Wert | Minimale Verzeichnisgröße  | Anmerkungen  |
|---|-------------------------|--------------|--|--|
| TCP/IP-Portadresse für die Kommunikation mit dem Server | 1500                    |              | Nicht zutreffend   | Stellen Sie sicher, dass dieser Port verfügbar ist, wenn Sie das Betriebssystem installieren und konfigurieren.<br><br>Die Portnummer kann eine Zahl zwischen 1024 und 32767 sein. |
| Verzeichnis für die Serverinstanz                       | /home/tsminst1/tsminst1 |              | 50 GB  | Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den DB2-Instanzeigner in Tabelle 2.                          |
| Verzeichnis für Serverinstallation                      | /                       |              | Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist:<br>5 GB |  |
| Verzeichnis für Serverinstallation                      | /usr                    |              | Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist:<br>5 GB |  |

| Element                                   | Standardwert  | Eigener Wert | Minimale Verzeichnisgröße  | Anmerkungen   |
|---|---|--------------|--|---|
| Verzeichnis für Serverinstallation        | /var  |              | Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist:<br>5 GB   |   |
| Verzeichnis für Serverinstallation        | /tmp  |              | Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist:<br>5 GB   |   |
| Verzeichnis für Serverinstallation        | /opt  |              | Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist:<br>10 GB  |   |
| Verzeichnis für die aktive Protokolldatei | /tsminst1/TSMalog   |              | <ul style="list-style-type: none"> <li>• Klein und mittel: 140 GB</li> <li>• Groß: 300 GB</li> </ul>   | Wenn Sie die aktive Protokolldatei während der Erstkonfiguration des Servers erstellen, setzen Sie die Größe auf 128 GB.  |
| Verzeichnis für das Archivprotokoll       | /tsminst1/TSMarchlog  |              | <ul style="list-style-type: none"> <li>• Klein: 1 TB</li> <li>• Mittel: 2 TB</li> <li>• Groß: 4 TB</li> </ul>  |   |
| Verzeichnisse für die Datenbank           | /tsminst1/TSMdbspace00<br>/tsminst1/TSMdbspace01<br>/tsminst1/TSMdbspace02<br>/tsminst1/TSMdbspace03<br>... |              | <p>Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 1 TB</li> <li>• Mittel: Mindestens 2 TB</li> <li>• Groß: Mindestens 4 TB</li> </ul>      | <p>Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 4 Dateisysteme</li> <li>• Mittel: Mindestens 4 Dateisysteme</li> <li>• Groß: Mindestens 8 Dateisysteme</li> </ul>   |
| Verzeichnisse für Speicher                | /tsminst1/TSMfile00<br>/tsminst1/TSMfile01<br>/tsminst1/TSMfile02<br>/tsminst1/TSMfile03<br>...             |              | <p>Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 38 TB</li> <li>• Mittel: Mindestens 180 TB</li> <li>• Groß: Mindestens 500 TB</li> </ul> | <p>Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 10 Dateisysteme</li> <li>• Mittel: Mindestens 20 Dateisysteme</li> <li>• Groß: Mindestens 40 Dateisysteme</li> </ul> |



| Element                              | Standardwert   | Eigener Wert | Minimale Verzeichnisgröße  | Anmerkungen   |
|--------------------------------------|--|--------------|--|---|
| Verzeichnisse für Datenbanksicherung | /tsminst1/TSMbkup00<br>/tsminst1/TSMbkup01<br>/tsminst1/TSMbkup02<br>/tsminst1/TSMbkup03 |              | Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: <ul style="list-style-type: none"> <li>• Klein: Mindestens 3 TB</li> <li>• Mittel: Mindestens 10 TB</li> <li>• Groß: Mindestens 16 TB</li> </ul> | Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank: <ul style="list-style-type: none"> <li>• Klein: Mindestens 2 Dateisysteme</li> <li>• Mittel: Mindestens 4 Dateisysteme</li> <li>• Groß: Mindestens 4 Dateisysteme, vorzugsweise jedoch 6</li> </ul> Das erste Datenbanksicherungsverzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfigurationsdatei verwendet. |

Tabelle 2. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

| Element                                | Standardwert   | Eigener Wert | Anmerkungen   |
|--|--|--------------|---|
| DB2-Instanzeigner                      | tsminst1   |              | Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 1 in einen anderen Wert geändert haben, ändern Sie auch den Wert für den DB2-Instanzeigner. |
| Kennwort des DB2-Instanzeigners        | passw0rd   |              | Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.             |
| Primärgruppe für den DB2-Instanzeigner | tsmsrvrs   |              |   |
| Servername                             | Der Standardwert für den Servernamen ist der Systemhostname. |              |   |
| Serverkennwort                         | passw0rd   |              | Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.                          |

| Element   | Standardwert | Eigener Wert | Anmerkungen  |
|---|--------------|--------------|--|
| Administrator-ID:<br>Benutzer-ID für die<br>Serverinstanz | admin        |              |  |
| Kennwort für die<br>Administrator-ID                      | passw0rd     |              | Wählen Sie für das<br>Administratorkennwort einen<br>anderen Wert als den<br>Standardwert aus. Sie müssen<br>diesen Wert an einem sicheren<br>Ort aufbewahren.   |
| Startzeit des Zeitplans                                   | 22:00        |              | Die standardmäßige Startzeit<br>des Zeitplans gibt den Anfang<br>der Client-Workload-Phase an,<br>die sich in erster Linie auf die<br>Clientsicherungs- und -<br>archivierungsaktivitäten bezieht.<br>Während der Client-Workload-<br>Phase werden Clientoperationen<br>durch Serverressourcen<br>unterstützt. Normalerweise<br>werden diese Operationen<br>während des nächtlichen<br>Zeitplanfensters ausgeführt.<br><br>Zeitpläne für<br>Serververwaltungsoperationen<br>beginnen gemäß Definition 10<br>Stunden nach dem Start des<br>Fensters zum Durchführen von<br>Clientsicherungen. |

## Linux

Tabelle 3. Arbeitsblatt für die Vorkonfiguration eines Linux-Serversystems

| Element  | Standardwert            | Eigener Wert | Minimale<br>Verzeichnisgröße   | Anmerkungen   |
|--|-------------------------|--------------|--|---|
| TCP/IP-Portadresse<br>für die<br>Kommunikation mit<br>dem Server | 1500                    |              | Nicht zutreffend   | Stellen Sie sicher, dass<br>dieser Port verfügbar<br>ist, wenn Sie das<br>Betriebssystem<br>installieren und<br>konfigurieren.<br><br>Die Portnummer kann<br>eine Zahl zwischen<br>1024 und 32767 sein. |
| Verzeichnis für die<br>Serverinstanz                             | /home/tsminst1/tsminst1 |              | 25 GB  | Wenn Sie den<br>Standardwert für das<br>Serverinstanzverzeichnis<br>in einen anderen<br>Wert ändern, ändern<br>Sie auch den Wert für<br>den DB2-Instanzeigner<br>in Tabelle 4.                          |
| Verzeichnis für die<br>aktive Protokolldatei                     | /tsminst1/TSMalog       |              | <ul style="list-style-type: none"> <li>• Klein und mittel: 140 GB</li> <li>• Groß: 300 GB</li> </ul> |   |

| Element                             | Standardwert  | Eigener Wert | Minimale Verzeichnisgröße  | Anmerkungen   |
|-------------------------------------|---|--------------|--|---|
| Verzeichnis für das Archivprotokoll | /tsminst1/TSMarchlog  |              | <ul style="list-style-type: none"> <li>• Klein: 1 TB</li> <li>• Mittel: 2 TB</li> <li>• Groß: 4 TB</li> </ul>  |   |
| Verzeichnisse für die Datenbank     | /tsminst1/TSMdbspace00<br>/tsminst1/TSMdbspace01<br>/tsminst1/TSMdbspace02<br>/tsminst1/TSMdbspace03<br>... |              | <p>Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 1 TB</li> <li>• Mittel: Mindestens 2 TB</li> <li>• Groß: Mindestens 4 TB</li> </ul>      | <p>Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 4 Dateisysteme</li> <li>• Mittel: Mindestens 4 Dateisysteme</li> <li>• Groß: Mindestens 8 Dateisysteme</li> </ul>   |
| Verzeichnisse für Speicher          | /tsminst1/TSMfile00<br>/tsminst1/TSMfile01<br>/tsminst1/TSMfile02<br>/tsminst1/TSMfile03<br>...             |              | <p>Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 38 TB</li> <li>• Mittel: Mindestens 180 TB</li> <li>• Groß: Mindestens 500 TB</li> </ul> | <p>Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 10 Dateisysteme</li> <li>• Mittel: Mindestens 20 Dateisysteme</li> <li>• Groß: Mindestens 40 Dateisysteme</li> </ul> |

| Element                              | Standardwert   | Eigener Wert | Minimale Verzeichnisgröße   | Anmerkungen   |
|--------------------------------------|--|--------------|---|---|
| Verzeichnisse für Datenbanksicherung | /tsminst1/TSMbkup00<br>/tsminst1/TSMbkup01<br>/tsminst1/TSMbkup02<br>/tsminst1/TSMbkup03 |              | <p>Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 3 TB</li> <li>• Mittel: Mindestens 10 TB</li> <li>• Groß: Mindestens 16 TB</li> </ul> | <p>Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 2 Dateisysteme</li> <li>• Mittel: Mindestens 4 Dateisysteme</li> <li>• Groß: Mindestens 4 Dateisysteme, vorzugsweise jedoch 6</li> </ul> <p>Das erste Datenbanksicherungsv erzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfiguration sdatei verwendet.</p> |

Tabelle 4. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

| Element   | Standardwert   | Eigener Wert | Anmerkungen   |
|---|--|--------------|---|
| DB2-Instanzeigner                                   | tsminst1   |              | Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 3 in einen anderen Wert geändert haben, ändern Sie auch den Wert für den DB2-Instanzeigner. |
| Kennwort des DB2-Instanzeigners                     | passw0rd   |              | Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.             |
| Primärgruppe für den DB2-Instanzeigner              | tsmsrvrs   |              |   |
| Servername  | Der Standardwert für den Servernamen ist der Systemhostname. |              |   |
| Serverkennwort                                      | passw0rd   |              | Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.                          |
| Administrator-ID: Benutzer-ID für die Serverinstanz | admin  |              |   |

| Element                           | Standardwert | Eigener Wert | Anmerkungen   |
|-----------------------------------|--------------|--------------|---|
| Kennwort für die Administrator-ID | passw0rd     |              | Wählen Sie für das Administratorkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.   |
| Startzeit des Zeitplans           | 22:00        |              | Die standardmäßige Startzeit des Zeitplans gibt den Anfang der Client-Workload-Phase an, die sich in erster Linie auf die Clientsicherungs- und -archivierungsaktivitäten bezieht. Während der Client-Workload-Phase werden Clientoperationen durch Serverressourcen unterstützt. Normalerweise werden diese Operationen während des nächtlichen Zeitplanfensters ausgeführt.<br><br>Zeitpläne für Serververwaltungsoperationen beginnen gemäß Definition 10 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen. |

## Windows

Da für den Server viele Datenträger erstellt werden, konfigurieren Sie den Server mithilfe der Windows-Funktion zum Zuordnen von Plattendatenträgern zu Verzeichnissen (statt der Funktion zum Zuordnen von Plattendatenträgern zu Laufwerkbuchstaben).

Beispielsweise ist C:\tsminst1\TSMdbpsace00 ein Mountpunkt für einen Datenträger mit eigenem Speicherbereich. Der Datenträger wird einem Verzeichnis unter dem Laufwerk C: zugeordnet, nimmt aber keinen Speicherbereich auf Laufwerk C: in Anspruch. Einzige Ausnahme ist das Serverinstanzverzeichnis, C:\tsminst1, das ein Mountpunkt oder ein normales Verzeichnis sein kann.

Tabelle 5. Arbeitsblatt für die Vorkonfiguration eines Windows-Serversystems

| Element   | Standardwert        | Eigener Wert | Minimale Verzeichnisgröße  | Anmerkungen  |
|---|---------------------|--------------|--|--|
| TCP/IP-Portadresse für die Kommunikation mit dem Server | 1500                |              | Nicht zutreffend   | Stellen Sie sicher, dass dieser Port verfügbar ist, wenn Sie das Betriebssystem installieren und konfigurieren.<br><br>Die Portnummer kann eine Zahl zwischen 1024 und 32767 sein. |
| Verzeichnis für die Serverinstanz                       | C:\tsminst1         |              | 25 GB  | Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den DB2-Instanzeigner in Tabelle 6.                          |
| Verzeichnis für die aktive Protokolldatei               | C:\tsminst1\TSMalog |              | <ul style="list-style-type: none"> <li>• Klein und mittel: 140 GB</li> <li>• Groß: 300 GB</li> </ul> |  |

| Element                             | Standardwert  | Eigener Wert | Minimale Verzeichnisgröße  | Anmerkungen   |
|-------------------------------------|---|--------------|--|---|
| Verzeichnis für das Archivprotokoll | C:\tsminst1\TSMarchlog  |              | <ul style="list-style-type: none"> <li>• Klein: 1 TB</li> <li>• Mittel: 2 TB</li> <li>• Groß: 4 TB</li> </ul>  |   |
| Verzeichnisse für die Datenbank     | C:\tsminst1\TSMdbspace00<br>C:\tsminst1\TSMdbspace01<br>C:\tsminst1\TSMdbspace02<br>C:\tsminst1\TSMdbspace03<br>... |              | <p>Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 1 TB</li> <li>• Mittel: Mindestens 2 TB</li> <li>• Groß: Mindestens 4 TB</li> </ul>      | <p>Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 4 Dateisysteme</li> <li>• Mittel: Mindestens 4 Dateisysteme</li> <li>• Groß: Mindestens 8 Dateisysteme</li> </ul>   |
| Verzeichnisse für Speicher          | C:\tsminst1\TSMfile00<br>C:\tsminst1\TSMfile01<br>C:\tsminst1\TSMfile02<br>C:\tsminst1\TSMfile03<br>...             |              | <p>Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 38 TB</li> <li>• Mittel: Mindestens 180 TB</li> <li>• Groß: Mindestens 500 TB</li> </ul> | <p>Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher:</p> <ul style="list-style-type: none"> <li>• Klein: Mindestens 10 Dateisysteme</li> <li>• Mittel: Mindestens 20 Dateisysteme</li> <li>• Groß: Mindestens 40 Dateisysteme</li> </ul> |

| Element                              | Standardwert   | Eigener Wert | Minimale Verzeichnisgröße  | Anmerkungen   |
|--------------------------------------|--|--------------|--|---|
| Verzeichnisse für Datenbanksicherung | C:\tsminst1\TSMbkup00<br>C:\tsminst1\TSMbkup01<br>C:\tsminst1\TSMbkup02<br>C:\tsminst1\TSMbkup03 |              | Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: <ul style="list-style-type: none"> <li>• Klein: Mindestens 3 TB</li> <li>• Mittel: Mindestens 10 TB</li> <li>• Groß: Mindestens 16 TB</li> </ul> | Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank: <ul style="list-style-type: none"> <li>• Klein: Mindestens 2 Dateisysteme</li> <li>• Mittel: Mindestens 4 Dateisysteme</li> <li>• Groß: Mindestens 4 Dateisysteme, vorzugsweise jedoch 6</li> </ul> Das erste Datenbanksicherungsv erzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfiguration sdatei verwendet. |

Tabelle 6. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

| Element   | Standardwert   | Eigener Wert | Anmerkungen   |
|---|--|--------------|---|
| DB2-Instanzeigner                                   | tsminst1   |              | Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 5 in einen anderen Wert geändert haben, ändern Sie auch den Wert für den DB2-Instanzeigner. |
| Kennwort des DB2-Instanzeigners                     | pAssW0rd   |              | Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.             |
| Servername  | Der Standardwert für den Servernamen ist der Systemhostname. |              |   |
| Serverkennwort                                      | passw0rd   |              | Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.                          |
| Administrator-ID: Benutzer-ID für die Serverinstanz | admin  |              |   |

| Element                           | Standardwert | Eigener Wert | Anmerkungen   |
|-----------------------------------|--------------|--------------|---|
| Kennwort für die Administrator-ID | passw0rd     |              | Wählen Sie für das Administratorkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.   |
| Startzeit des Zeitplans           | 22:00        |              | Die standardmäßige Startzeit des Zeitplans gibt den Anfang der Client-Workload-Phase an, die sich in erster Linie auf die Clientsicherungs- und -archivierungsaktivitäten bezieht. Während der Client-Workload-Phase werden Clientoperationen durch Serverressourcen unterstützt. Normalerweise werden diese Operationen während des nächtlichen Zeitplanfensters ausgeführt.<br><br>Zeitpläne für Serververwaltungsoperationen beginnen gemäß Definition 10 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen. |

## Planung für Speicher

Wählen Sie die effektivste Speichertechnologie für IBM Spectrum Protect-Komponenten aus, um effiziente Serverleistung und Serveroperationen zu gewährleisten.

Speicherhardwareeinheiten haben unterschiedliche Kapazitäts- und Leistungsmerkmale, die festlegen, wie die Einheiten effizient mit IBM Spectrum Protect verwendet werden können. Die folgenden Richtlinien stellen eine allgemeine Anleitung zur Auswahl der für Ihre Lösung geeigneten Speicherhardware und Konfiguration dar.

### Datenbank und aktive Protokolldatei

- Verwenden Sie eine schnelle Platte für die IBM Spectrum Protect-Datenbank und die aktive Protokolldatei, die beispielsweise die folgenden Merkmale hat:
  - Hochleistungsplatte mit 15.000 Umdrehungen pro Minute mit Fibre Channel- oder SAS-Schnittstelle
  - Solid-State-Platte (SSD)
- Trennen Sie die aktive Protokolldatei von der Datenbank, es sei denn, Sie verwenden SSD oder Flash-Hardware.
- Verwenden Sie beim Erstellen von Arrays für die Datenbank RAID-Stufe 5.

### Speicherpool

- Sie können kostengünstigere und langsamere Platten für den Speicherpool verwenden.
- Der Speicherpool kann Platten für den Speicher für das Archivprotokoll und die Datenbanksicherung gemeinsam nutzen.
- Verwenden Sie RAID-Stufe 6 für Speicherpoolarrays, um bei Verwendung von Typen großer Platten Schutz vor Laufwerkdoppelfehlern hinzuzufügen.
- Planung der Speicherarrays  
Bereiten Sie die Konfiguration des Plattenspeichers vor, indem Sie die Planung für RAID-Arrays und Datenträger gemäß der Größe Ihres IBM Spectrum Protect-Systems ausführen.

### Zugehörige Verweise:

 Speichersystemvoraussetzungen und Reduzierung des Risikos fehlerhafter Daten

## Planung für Sicherheit

Planen Sie den Schutz der Sicherheit von Systemen in der IBM Spectrum Protect-Lösung mithilfe von Steuerelementen für Zugriff und Authentifizierung und ziehen Sie das Verschlüsseln von Daten und der Übertragung von Kennwörtern in Erwägung.



Richtlinien zum Schutz Ihrer Speicherumgebung vor Ransomware-Attacken und zur Wiederherstellung Ihrer Speicherumgebung nach einer Attacke finden Sie in Speicherumgebung vor Ransomware-Attacken schützen.

- **Planung für Administratorrollen**  
Definieren Sie die Berechtigungsstufen, die Administratoren zugeordnet werden sollen, die Zugriff auf die IBM Spectrum Protect-Lösung haben.
- **Planung für sichere Kommunikation**  
Planen Sie den Schutz der Kommunikation zwischen den IBM Spectrum Protect-Lösungskomponenten.
- **Planung für die Speicherung verschlüsselter Daten**  
Bestimmen Sie, ob Ihr Unternehmen die Verschlüsselung gespeicherter Daten erfordert, und wählen Sie für Ihre Anforderungen am besten geeignete Option aus.
- **Planung des Firewallzugriffs**  
Bestimmen Sie die definierten Firewalls und die Ports, die offen sein müssen, damit die IBM Spectrum Protect-Lösung funktionsfähig ist.

## Planung für Administratorrollen

Definieren Sie die Berechtigungsstufen, die Administratoren zugeordnet werden sollen, die Zugriff auf die IBM Spectrum Protect-Lösung haben.

Sie können Administratoren eine der folgenden Berechtigungsstufen zuordnen:

### Systemberechtigung

Administratoren mit Systemberechtigung verfügen über die höchste Berechtigungsstufe. Administratoren mit dieser Berechtigungsstufe können jede Task ausführen. Sie können alle Maßnahmendomänen und Speicherpools verwalten und anderen Administratoren Berechtigung erteilen.

### Maßnahmenberechtigung

Administratoren mit Maßnahmenberechtigung können alle Tasks verwalten, die sich auf die Maßnahmenverwaltung beziehen. Diese Berechtigung kann uneingeschränkt sein oder auf bestimmte Maßnahmendomänen eingeschränkt werden.

### Speicherberechtigung

Administratoren mit Speicherberechtigung können Speicherressourcen für den Server zuordnen und steuern.

### Bedienerberechtigung

Administratoren mit Bedienerberechtigung können den sofortigen Betrieb des Servers und die Verfügbarkeit von Speichermedien wie beispielsweise Bandarchiven und -laufwerken steuern.

Die Szenarios in Tabelle 1 enthalten Beispiele, die zeigen, warum es sinnvoll ist, Administratoren für die Ausführung von Tasks unterschiedliche Berechtigungsstufen zuzuordnen:

Tabelle 1. Szenarios für Administratorrollen

| Szenario  | Typ der zu konfigurierenden Administrator-ID  |
|---|---|
| Ein Administrator in einem kleinen Unternehmen verwaltet den Server und ist für alle Serveraktivitäten verantwortlich.  | <ul style="list-style-type: none"> <li>• Systemberechtigung: 1 Administrator-ID</li> </ul>  |
| Ein Administrator für mehrere Server verwaltet auch das gesamte System. Mehrere andere Administratoren verwalten ihre eigenen Speicherpools.  | <ul style="list-style-type: none"> <li>• Systemberechtigung auf allen Servern: 1 Administrator-ID für den Administrator des gesamten Systems</li> <li>• Speicherberechtigung für bestimmte Speicherpools: 1 Administrator-ID für jeden der anderen Administratoren</li> </ul> |
| Ein Administrator verwaltet 2 Server. Eine andere Person unterstützt ihn bei den Verwaltungstasks. Zwei Assistenten müssen sicherstellen, dass wichtige Systeme gesichert werden. Jeder Assistent ist für die Überwachung der geplanten Sicherungen auf einem der IBM Spectrum Protect-Server verantwortlich. | <ul style="list-style-type: none"> <li>• Systemberechtigung auf beiden Servern: 2 Administrator-IDs</li> <li>• Bedienerberechtigung: 2 Administrator-IDs für die Assistenten mit Zugriff auf den Server, für den die jeweilige Person verantwortlich ist.</li> </ul>          |

## Planung für sichere Kommunikation

Planen Sie den Schutz der Kommunikation zwischen den IBM Spectrum Protect-Lösungskomponenten.

Bestimmen Sie auf der Basis der Regelungen und Geschäftsanforderungen für Ihr Unternehmen, welche Stufe des Schutzes für Ihre Daten erforderlich ist.

Wenn Ihr Unternehmen ein hohes Maß an Sicherheit für Kennwörter und die Datenübertragung erfordert, planen Sie die Implementierung der sicheren Kommunikation mit dem Protokoll Transport Layer Security (TLS) oder Secure Sockets Layer (SSL).

TLS und SSL stellen sichere Kommunikation zwischen dem Server und dem Client bereit, können sich jedoch auf die Systemleistung auswirken. Um die Systemleistung zu verbessern, verwenden Sie TLS für die Authentifizierung, ohne Objektdaten zu verschlüsseln. Informationen zur Angabe, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, finden Sie in der Beschreibung der Clientoption SSL für die Client/Server-Kommunikation und der Beschreibung des Parameters UPDATE SERVER=SSL für die Kommunikation zwischen Servern. Ab Version 8.1.2 wird TLS standardmäßig für die Authentifizierung verwendet. Wenn Sie sich für die Verwendung von TLS entscheiden, um vollständige Sitzungen zu verschlüsseln, verwenden Sie das Protokoll nur für Sitzungen, für die es erforderlich ist; fügen Sie außerdem auf dem Server Prozessorressourcen hinzu, um den wachsenden Datenaustausch im Netz handhaben zu können. Sie können auch versuchsweise andere Optionen verwenden. Beispielsweise stellen einige Netzeinheiten wie Router und Switches die TLS- oder SSL-Funktion bereit.

Mithilfe von TLS und SSL können Sie einige oder alle der unterschiedlichen möglichen Kommunikationspfade schützen, beispielsweise:

- Operations Center: vom Browser zum Hub-Server; vom Hub-Server zum Peripherieserver
- Vom Client zum Server
- Vom Server zum Server: Knotenreplikation

**Zugehörige Tasks:**

 Kommunikation schützen


## Planung für die Speicherung verschlüsselter Daten

Bestimmen Sie, ob Ihr Unternehmen die Verschlüsselung gespeicherter Daten erfordert, und wählen Sie für Ihre Anforderungen am besten geeignete Option aus.

Wenn Ihr Unternehmen die Verschlüsselung der Daten in Speicherpools erfordert, können Sie entweder die IBM Spectrum Protect-Verschlüsselung oder eine externe Einheit wie beispielsweise ein Band für die Verschlüsselung verwenden.

Wenn Sie IBM Spectrum Protect zum Verschlüsseln der Daten auswählen, sind zusätzliche IT-Ressourcen auf dem Client erforderlich, die sich auf die Leistung von Sicherungs- und Zurückschreibungsprozessen auswirken können.

**Zugehörige Informationen:**

 [Technote 1963635](#)

## Planung des Firewallzugriffs

Bestimmen Sie die definierten Firewalls und die Ports, die offen sein müssen, damit die IBM Spectrum Protect-Lösung funktionsfähig ist.

In Tabelle 1 sind die Ports beschrieben, die vom Server, vom Client und vom Operations Center verwendet werden.

Tabelle 1. Vom Server, Client und Operations Center verwendete Ports

| Element                                   | Standardwert      | Richtung           | Beschreibung   |
|---|-------------------|--------------------|--|
| Basisport (TCPPOINT)                      | 1500              | Abgehend/Eingehend | Jede Serverinstanz erfordert einen eindeutigen Port. Sie können eine alternative Portnummer angeben, anstatt den Standardwert zu verwenden. Der mit der Option TCPPOINT angegebene Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen vom Client empfangsbereit. Für den Datenverkehr des Verwaltungsclients können Sie zum Festlegen von Portwerten die Optionen TCPADMINPORT und ADMINONCLIENTPORT verwenden. |
| Port ausschließlich für SSL (SSLTCPPOINT) | Kein Standardwert | Abgehend/Eingehend | Dieser Port wird verwendet, wenn die Kommunikation am Port auf ausschließlich SSL-fähige Sitzungen beschränkt werden soll. Um sowohl die SSL-Kommunikation als auch die Nicht-SSL-Kommunikation zu unterstützen, verwenden Sie die Option TCPPOINT oder TCPADMINPORT.  |
| SMB                                       | 45                | Eingehend/Abgehend | Dieser Port wird von Konfigurationsassistenten verwendet, die unter Verwendung nativer Protokolle mit mehreren Hosts kommunizieren.  |
| SSH                                       | 22                | Eingehend/Abgehend | Dieser Port wird von Konfigurationsassistenten verwendet, die unter Verwendung nativer Protokolle mit mehreren Hosts kommunizieren.  |
| SMTP                                      | 25                | Abgehend           | Dieser Port wird zum Senden von E-Mail-Alerts vom Server verwendet.  |

| Element                               | Standardwert                   | Richtung           | Beschreibung   |
|---------------------------------------|--------------------------------|--------------------|--|
| NDMP                                  | Kein Standardwert              | Eingehend/Abgehend | <p>Der Server muss eine abgehende NDMP-Steuerportverbindung zu der NAS-Einheit öffnen können. Der abgehende Steuerport ist die Adresse der unteren Ebene in der Definition der Einheit zum Versetzen von Daten für die NAS-Einheit.</p> <p>Während einer NDMP-Zurückschreibung vom Dateiserver auf den Server muss der Server eine abgehende NDMP-Datenverbindung zu der NAS-Einheit öffnen können. Der Datenverbindungsport, der während einer Zurückschreibung verwendet wird, kann auf der NAS-Einheit konfiguriert werden.</p> <p>Während NDMP-Sicherungen vom Dateiserver auf den Server muss die NAS-Einheit abgehende Datenverbindungen zum Server öffnen können und der Server muss eingehende NDMP-Datenverbindungen akzeptieren können. Mithilfe der Serveroption NDMPORTRANGE können Sie die für die Verwendung als NDMP-Datenverbindungen verfügbare Gruppe von Ports einschränken. Sie können eine Firewall für Verbindungen zu diesen Ports konfigurieren.</p> |
| Replikation                           | Kein Standardwert              | Abgehend/Eingehend | <p>Der Port und das Protokoll für den Port für abgehende Daten für die Replikation werden mit dem Befehl DEFINE SERVER festgelegt, der zum Konfigurieren der Replikation verwendet wird.</p> <p>Bei den Ports für eingehende Daten für die Replikation handelt es sich um die TCP-Ports und SSL-Ports, die für den Quellenserver im Befehl DEFINE SERVER angegeben werden.</p>   |
| Port für Clientzeitplan               | Client-Port: 1501              | Abgehend           | Der Client ist an dem angegebenen Port empfangsbereit und teilt die Portnummer dem Server mit. Der Server kontaktiert den Client, wenn die servergesteuerte Zeitplanung verwendet wird. Sie können eine alternative Portnummer in der Clientoptionsdatei angeben.  |
| Lange laufende Sitzungen              | Einstellung für KEEPALIVE: YES | Abgehend           | Wenn die Option KEEPALIVE aktiviert ist, werden während Client/Server-Sitzungen Keepalive-Pakete gesendet, um zu verhindern, dass die Firewall-Software lange laufende inaktive Verbindungen schließt.   |
| Operations Center                     | HTTPS: 11090                   | Eingehend          | Diese Ports werden für den Web-Browser des Operations Center verwendet. Sie können eine alternative Portnummer angeben.  |
| Port für den Clientverwaltungsservice | Client-Port: 9028              | Eingehend          | Der Zugriff auf den Port für den Clientverwaltungsservice muss über das Operations Center möglich sein. Stellen Sie sicher, dass Verbindungen nicht durch Firewalls verhindert werden können. Der Clientverwaltungsservice verwendet den TCP-Port des Servers für den Clientknoten für die Authentifizierung unter Verwendung einer Verwaltungssitzung.  |

## Implementierung einer Plattenspeicherdatenschutzlösung für mehrere Standorte

Die Plattenspeicherlösung für mehrere Standorte wird an zwei Standorten konfiguriert und verwendet Datenduplizierung und Replikation.

### Implementierungsroadmap

Die folgenden Schritte sind zum Konfigurieren einer Plattenspeicherumgebung an mehreren Standorten erforderlich.

1. Konfigurieren Sie das System.
  - a. Konfigurieren Sie die Speicherhardware und Speicherarrays für Ihre Umgebungsgröße.
  - b. Installieren Sie das Serverbetriebssystem.
  - c. Konfigurieren Sie Multipath I/O.
  - d. Erstellen Sie die Benutzer-ID für die Serverinstanz.
  - e. Bereiten Sie Dateisysteme für IBM Spectrum Protect vor.
2. Installieren Sie den Server und das Operations Center.

3. Konfigurieren Sie den Server und das Operations Center.
  - a. Führen Sie die Erstkonfiguration des Servers aus.
  - b. Legen Sie Serveroptionen fest.
  - c. Konfigurieren Sie Secure Sockets Layer für den Server und den Client.
  - d. Konfigurieren Sie das Operations Center.
  - e. Registrieren Sie Ihre IBM Spectrum Protect-Lizenz.
  - f. Konfigurieren Sie die Datenduplizierung.
  - g. Definieren Sie Datenaufbewahrungsregeln für Ihr Unternehmen.
  - h. Definieren Sie Zeitpläne für die Serververwaltung.
  - i. Definieren Sie Clientzeitpläne.
4. Installieren und konfigurieren Sie Clients.
  - a. Registrieren Sie Clients und ordnen Sie Clients Zeitplänen zu.  
Tipp: Verhindern Sie Konflikte bei der Verwaltung von Verwaltungs-IDs und Clientoptionsgruppen, indem Sie die IDs und Optionsgruppen, die auf dem Zielsystem repliziert werden, und die IDs und Optionsgruppen, die in einer unternehmensweiten Konfiguration verwaltet werden, identifizieren. Es ist nicht möglich, eine Benutzer-ID mit Administratorberechtigung für einen registrierten Knoten zu definieren, wenn für denselben Knoten eine Verwaltungs-ID vorhanden ist.
  - b. Installieren und überprüfen Sie den Clientverwaltungsservice.
  - c. Konfigurieren Sie das Operations Center für die Verwendung des Clientverwaltungsservice.
5. Konfigurieren Sie den zweiten Server.
  - a. Konfigurieren Sie die SSL-Kommunikation zwischen dem Hub-Server und dem Peripherieserver.
  - b. Fügen Sie den zweiten Server als Peripherieserver hinzu.
  - c. Aktivieren Sie die Replikation.
6. Schließen Sie die Implementierung ab.

## System konfigurieren

---

Um das System konfigurieren zu können, müssen Sie zunächst Ihre Plattenspeicherhardware und das Serversystem für IBM Spectrum Protect konfigurieren.

- Speicherhardware konfigurieren  
Um Ihre Speicherhardware zu konfigurieren, lesen Sie die allgemeine Anleitung für Plattensysteme und IBM Spectrum Protect.
- Serverbetriebssystem installieren  
Installieren Sie das Betriebssystem auf dem Serversystem und stellen Sie sicher, dass die Voraussetzungen für den IBM Spectrum Protect-Server erfüllt sind. Passen Sie Betriebssystemeinstellungen gemäß Anweisung an.
- Multipath I/O konfigurieren  
Sie können Multipathing für Plattenspeicher aktivieren und konfigurieren. Die mit Ihrer Hardware zur Verfügung gestellte Dokumentation enthält ausführliche Anweisungen.
- Benutzer-ID für den Server erstellen  
Erstellen Sie die Benutzer-ID, die Eigner der IBM Spectrum Protect-Serverinstanz ist. Sie geben diese Benutzer-ID an, wenn Sie die Serverinstanz im Rahmen der Erstkonfiguration des Servers erstellen.
- Dateisysteme für den Server vorbereiten  
Sie müssen die Dateisystemkonfiguration ausführen, damit der Plattenspeicher vom Server verwendet werden kann.

## Speicherhardware konfigurieren

---

Um Ihre Speicherhardware zu konfigurieren, lesen Sie die allgemeine Anleitung für Plattensysteme und IBM Spectrum Protect.

### Vorgehensweise

---

1. Stellen Sie unter Berücksichtigung der folgenden Richtlinien eine Verbindung zwischen dem Server und den Speichereinheiten her:
  - Verwenden Sie einen Switch oder eine Direktverbindung für Fibre Channel-Verbindungen.
  - Berücksichtigen Sie die Anzahl Ports, die verbunden sind, und die erforderliche Bandbreite.
  - Berücksichtigen Sie die Anzahl Ports auf dem Server und die Anzahl Host-Ports auf dem Plattensystem, die verbunden sind.
2. Stellen Sie sicher, dass die Einheitentreiber und die Firmware für das Serversystem, die Adapter und das Betriebssystem aktuell sind und die empfohlenen Versionen haben.
3. Konfigurieren Sie Speicherarrays. Stellen Sie sicher, dass Sie entsprechend geplant haben, um die optimale Leistung zu gewährleisten. Weitere Informationen finden Sie in Planung für Speicher.
4. Stellen Sie sicher, dass das Serversystem Zugriff auf Plattendatenträger hat, die erstellt werden. Führen Sie die folgenden Schritte aus:
  - a. Wenn das System mit einem Fibre Channel-Switch verbunden ist, verzonieren Sie den Server, um die Platten anzuzeigen.

- b. Ordnen Sie alle Datenträger zu, um dem Plattensystem mitzuteilen, dass diesem spezifischen Server die Anzeige jeder Platte ermöglicht werden soll.

#### Zugehörige Tasks:

📁 Speicher konfigurieren

## Serverbetriebssystem installieren

---

Installieren Sie das Betriebssystem auf dem Serversystem und stellen Sie sicher, dass die Voraussetzungen für den IBM Spectrum Protect-Server erfüllt sind. Passen Sie Betriebssystemeinstellungen gemäß Anweisung an.

- Installation auf AIX-Systemen  
Führen Sie die folgenden Schritte aus, um AIX auf dem Serversystem zu installieren.
- Installation auf Linux-Systemen  
Führen Sie die folgenden Schritte aus, um Linux x86\_64 auf dem Serversystem zu installieren.
- Installation auf Windows-Systemen  
Installieren Sie Microsoft Windows Server 2012 Standard Edition auf dem Serversystem und bereiten Sie das System für die Installation und Konfiguration des IBM Spectrum Protect-Servers vor.

## Installation auf AIX-Systemen

---

Führen Sie die folgenden Schritte aus, um AIX auf dem Serversystem zu installieren.

### Vorgehensweise

---

1. Installieren Sie AIX Version 7.1, TL4, SP2 oder höher gemäß den Anweisungen des Herstellers.
2. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Anweisungen zur Installation des Betriebssystems.
3. Öffnen Sie die Datei /etc/hosts und führen Sie die folgenden Aktionen aus:

- Aktualisieren Sie die Datei, um die IP-Adresse und den Hostnamen des Servers einzuschließen. Beispiel:

```
192.0.2.7 server.yourdomain.com server
```

- Überprüfen Sie, ob die Datei einen Eintrag für localhost mit der Adresse 127.0.0.1 enthält. Beispiel:

```
127.0.0.1 localhost
```

4. Aktivieren Sie die AIX-I/O Completion Ports (IOCP), indem Sie den folgenden Befehl eingeben:

```
chdev -l iocp0 -P
```

Die Olson-Zeitzonendefinition kann sich auf die Serverleistung auswirken.

5. Um die Leistung zu optimieren, ändern Sie Ihr Systemzeitonenformat von Olson in POSIX. Verwenden Sie das folgende Befehlsformat zum Aktualisieren der Zeitzoneneinstellung:

```
chtz=Ortszeitzone,Datum/Uhrzeit,Datum/Uhrzeit
```

Beispielsweise würden Sie in Tucson, Arizona, wo die Mountain Standard Time gilt, den folgenden Befehl ausgeben, um das Format in das POSIX-Format zu ändern:

```
chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
```

6. Fügen Sie in .profile des Instanzbenutzers einen Eintrag hinzu, um die folgende Umgebung festzulegen:

```
export MALLOCOPTIONS=multiheap:16
```

7. Legen Sie fest, dass das System vollständige Anwendungskerndateien erstellen soll. Geben Sie den folgenden Befehl aus:

```
chdev -l sys0 -a fullcore=true -P
```

8. Stellen Sie für die Kommunikation mit dem Server und dem Operations Center sicher, dass die folgenden Ports für alle Firewalls, die gegebenenfalls vorhanden sind, offen sind:

- Öffnen Sie für die Kommunikation mit dem Server Port 1500.
- Öffnen Sie für die sichere Kommunikation mit dem Operations Center Port 11090 auf dem Hub-Server.

Wenn Sie nicht die Standardwerte für Ports verwenden, stellen Sie sicher, dass die verwendeten Ports offen sind.

9. Aktivieren Sie TCP-Hochleistungsverbesserungen. Geben Sie den folgenden Befehl aus:

```
no -p -o rfc1323=1
```

10. Um optimalen Durchsatz und optimale Zuverlässigkeit zu gewährleisten, kombinieren Sie vier 10-Gb-Ethernet-Ports durch Bonding miteinander. Verwenden Sie das System Management Interface Tool (SMIT), um die Ports durch Bonding unter Verwendung von Etherchannel zu kombinieren. Beim Testen wurden die folgenden Einstellungen verwendet:

```

mode          8023ad
auto_recovery yes          Automatische Wiederherstellung nach
                          Übernahme aktivieren
backup_adapter NONE       Adapter, der beim Fehlschlagen des
                          gesamten Kanals verwendet wird
hash_mode     src_dst_port Legt fest, wie der abgehende Adapter
                          ausgewählt wird
interval      long        Legt den Intervallwert für den IEEE-Modus
                          802.3ad fest
mode          8023ad      EtherChannel-Betriebsart
netaddr       0           Mit Ping zu überprüfende Adresse
no_loss_failover yes      Verlustfreie Übernahme nach dem Fehl-
                          schlagen des Pingbefehls aktivieren
num_retries   3           Anzahl Wiederholungen für Pingbefehl vor
                          dem Fehlschlagen
retry_time    1           Wartezeit (in Sekunden) zwischen
                          Pingbefehlen
use_alt_addr  no          Alternative EtherChannel-Adresse
                          aktivieren
use_jumbo_frame no       Jumbo-Frames für Gigabit Ethernet
                          aktivieren

```

11. Überprüfen Sie, ob Benutzerprozessressourcengrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, gemäß den Richtlinien in Tabelle 1 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

Tabelle 1. Benutzerbegrenzwerte (ulimit-Werte)

| Typ des Benutzerbegrenzwerts                         | Einstellung | Wert      | Befehl zum Abfragen des Werts |
|--|-------------|-----------|-------------------------------|
| Maximale Größe der erstellten Kerndateien            | core        | Unlimited | ulimit -Hc                    |
| Maximale Größe eines Datensegments für einen Prozess | data        | Unlimited | ulimit -Hd                    |
| Maximale Dateigröße                                  | fsize       | Unlimited | ulimit -Hf                    |
| Maximale Anzahl offener Dateien                      | nofile      | 65536     | ulimit -Hn                    |
| Maximale Prozessorzeit in Sekunden                   | cpu         | Unlimited | ulimit -Ht                    |
| Maximale Anzahl Benutzerprozesse                     | nproc       | 16384     | ulimit -Hu                    |

Wenn einer der Benutzerbegrenzwerte geändert werden muss, führen Sie die Anweisungen in der Dokumentation für Ihr Betriebssystem aus.

## Installation auf Linux-Systemen

Führen Sie die folgenden Schritte aus, um Linux x86\_64 auf dem Serversystem zu installieren.

### Vorbereitende Schritte

Das Betriebssystem wird auf den internen Festplatten installiert. Konfigurieren Sie die internen Festplatten für die Verwendung eines RAID 1-Hardware-Arrays. Wenn Sie beispielsweise ein kleines System konfigurieren, werden die beiden internen 300-GB-Platten in RAID 1 gespiegelt, sodass es aussieht, als würde dem Installationsprogramm des Betriebssystems eine einzelne 300-GB-Platte zur Verfügung stehen.

### Vorgehensweise

1. Installieren Sie Red Hat Enterprise Linux Version 7.1 oder höher gemäß den Anweisungen des Herstellers. Fordern Sie eine bootfähige DVD an, die Red Hat Enterprise Linux Version 7.1 enthält, und starten Sie Ihr System von dieser DVD. Für Installationsoptionen siehe die folgende Anleitung. Wenn ein Element in der folgenden Liste nicht aufgeführt ist, übernehmen Sie die Standardauswahl unverändert.

- a. Wählen Sie nach dem Starten der DVD im Menü Install or upgrade an existing system (Installation oder Aktualisierung eines bestehenden Systems) aus.
- b. Wählen Sie in der Eingangsanzeige Test this media & install Red Hat Enterprise Linux 7.1 (Diese Medien überprüfen & Red Hat Enterprise Linux 7.1 installieren) aus.
- c. Wählen Sie Ihre Sprache und Tastaturbelegung aus.
- d. Wählen Sie Ihren Standort aus, um die korrekte Zeitzone festzulegen.
- e. Wählen Sie Software Selection (Softwareauswahl) und in der nächsten Anzeige Server with GUI (Server mit GUI) aus.
- f. Klicken Sie auf der Installationszusammenfassungsseite auf Installation Destination (Installationsziel) und überprüfen Sie die folgenden Einträge:
  - Die lokale 300-GB-Platte ist als Installationsziel ausgewählt.
  - Unter 'Other Storage Options' (Weitere Speicheroptionen) ist Automatically configure partitioning (Partitionierung automatisch konfigurieren) ausgewählt.
 Klicken Sie auf Done (Fertig).
- g. Klicken Sie auf Begin Installation (Installation starten). Legen Sie nach dem Start der Installation das Rootkennwort für Ihr Rootbenutzerkonto fest.

Führen Sie nach dem Abschluss der Installation einen Neustart für das System durch und melden Sie sich als Rootbenutzer an. Geben Sie den Befehl `df` aus, um die Basispartitionierung zu überprüfen. Auf einem Testsystem hatte die Erstpartitionierung beispielsweise das folgende Ergebnis zur Folge:

```
[root@tvapp02]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/mapper/rhel-root  50G  3.0G  48G   6% /
devtmpfs        32G   0    32G   0% /dev
tmpfs           32G   92K   32G   1% /dev/shm
tmpfs           32G   8.8M  32G   1% /run
tmpfs           32G   0    32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home 220G  37M  220G   1% /home
/dev/sda1       497M  124M  373M  25% /boot
```

2. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Anweisungen zur Installation des Betriebssystems. Um optimalen Durchsatz und optimale Zuverlässigkeit zu gewährleisten, sollten Sie das Bonding mehrerer Netzports in Erwägung ziehen. Erstellen Sie dazu eine LACP-Netzverbindung (LACP = Link Aggregation Control Protocol), bei der mehrere untergeordnete Ports in einer einzigen logischen Verbindung aggregiert werden. Die bevorzugte Methode ist die Verwendung des Bondmodus 802.3ad, des Werts 100 für die Einstellung `mimon` und der Angabe 'layer3+4' für die Einstellung `xmit_hash_policy`. Einschränkung: Um eine LACP-Netzverbindung verwenden zu können, muss ein Netzswitch vorhanden sein, der LACP unterstützt.

Weitere Anweisungen zur Konfiguration von Bonding-Netzverbindungen mit Red Hat Enterprise Linux Version 7 finden Sie unter [Create a Channel Bonding Interface](#).

3. Öffnen Sie die Datei `/etc/hosts` und führen Sie die folgenden Aktionen aus:
  - Aktualisieren Sie die Datei, um die IP-Adresse und den Hostnamen des Servers einzuschließen. Beispiel:

```
192.0.2.7  server.yourdomain.com  server
```

- Überprüfen Sie, ob die Datei einen Eintrag für localhost mit der Adresse 127.0.0.1 enthält. Beispiel:

```
127.0.0.1  localhost
```

4. Installieren Sie Komponenten, die für die Serverinstallation erforderlich sind. Führen Sie die folgenden Schritte aus, um ein YUM-Repository (YUM = Yellowdog Updater, Modified) zu erstellen und die vorausgesetzten Pakete zu installieren.
  - a. Stellen Sie die DVD für die Installation von Red Hat Enterprise Linux in einem Systemverzeichnis bereit. Um sie beispielsweise im Verzeichnis `/mnt` bereitzustellen, geben Sie den folgenden Befehl aus:

```
mount -t iso9660 -o ro /dev/cdrom /mnt
```

- b. Überprüfen Sie, ob die DVD bereitgestellt wurde, indem Sie den Befehl `mount` ausgeben. Es sollte eine ähnliche Ausgabe wie in dem folgenden Beispiel angezeigt werden:

```
/dev/sr0 on /mnt type iso9660
```

- c. Wechseln Sie in das YUM-Repository-Verzeichnis, indem Sie den folgenden Befehl ausgeben:

```
cd /etc/yum/repos.d
```

- Wenn das Verzeichnis `repos.d` nicht vorhanden ist, erstellen Sie es.

- d. Listen Sie den Verzeichnisisinhalt auf:

```
ls rhel-source.repo
```

- e. Benennen Sie die ursprüngliche repo-Datei um, indem Sie den Befehl `mv` ausgeben. Beispiel:

```
mv rhel-source.repo rhel-source.repo.orig
```

f. Erstellen Sie mithilfe eines Texteditors eine neue repo-Datei. Um beispielsweise den Editor vi zu verwenden, geben Sie den folgenden Befehl aus:

```
vi rhel71_dvd.repo
```

g. Fügen Sie der neuen repo-Datei die folgenden Zeilen hinzu. Der Parameter baseurl gibt den Verzeichnismountpunkt an:

```
[rhel71_dvd]
name=DVD Redhat Enterprise Linux 7.1
baseurl=file:///mnt
enabled=1
gpgcheck=0
```

h. Installieren Sie das vorausgesetzte Paket ksh.x86\_64, indem Sie den Befehl yum ausgeben. Beispiel:

```
yum install ksh.x86_64
```

Ausnahme: Sie müssen die Bibliotheken compat-libstdc++-33-3.2.3-69.el6.i686 und libstdc++.i686 für Red Hat Enterprise Linux Version 7.1 nicht installieren.

5. Wenn die Softwareinstallation abgeschlossen ist, können Sie die ursprünglichen YUM-Repository-Werte zurückschreiben, indem Sie die folgenden Schritte ausführen:

a. Heben Sie die Bereitstellung der DVD für die Installation von Red Hat Enterprise Linux auf, indem Sie den folgenden Befehl ausgeben:

```
umount /mnt
```

b. Wechseln Sie in das YUM-Repository-Verzeichnis, indem Sie den folgenden Befehl ausgeben:

```
cd /etc/yum/repos.d
```

c. Benennen Sie die von Ihnen erstellte repo-Datei um:

```
mv rhel71_dvd.repo rhel71_dvd.repo.orig
```

d. Benennen Sie die ursprüngliche Datei wieder in den ursprünglichen Namen um:

```
mv rhel-source.repo.orig rhel-source.repo
```

6. Bestimmen Sie, ob Änderungen an Kernelparametern erforderlich sind. Führen Sie die folgenden Schritte aus:

a. Listen Sie mithilfe des Befehls sysctl -a die Parameterwerte auf.

b. Analysieren Sie die Ergebnisse anhand der Richtlinien in Tabelle 1, um zu bestimmen, ob Änderungen erforderlich sind.

c. Wenn Änderungen erforderlich sind, definieren Sie die Parameter in der Datei /etc/sysctl.conf. Die Dateiänderungen werden angewendet, wenn das System gestartet wird.

Tipp: Passen Sie Kernelparametereinstellungen automatisch an und eliminieren Sie die Notwendigkeit manueller Aktualisierungen dieser Einstellungen. Unter Linux passt die DB2-Datenbanksoftware automatisch die Werte der Kernelparameter für die Interprozesskommunikation (IPC) an und setzt sie auf die bevorzugten Einstellungen. Weitere Informationen zu Kernelparametereinstellungen finden Sie bei Verwendung des Suchbegriffs Linux-Kernelparameter im Produktdokumentation zu IBM DB2 Version 11.1.

Tabelle 1. Optimale Einstellungen für Linux-Kernelparameter

| Parameter  | Beschreibung  |
|--|---|
| kernel.shmmni                                    | Die maximale Anzahl Segmente.   |
| kernel.shmmax                                    | Die maximale Größe eines gemeinsam genutzten Speichersegments (Byte).<br><br>Dieser Parameter muss definiert werden, bevor der IBM Spectrum Protect-Server beim Systemstart automatisch gestartet wird. |
| kernel.shmall                                    | Die maximale Zuordnung von Seiten im gemeinsam genutzten Speicher (Seiten).   |
| kernel.sem                                       | (SEMMSL)  |
| Für den Parameter kernel.sem gibt es vier Werte. | Die maximale Anzahl Semaphore pro Array.  |
|  | (SEMMNS)  |
|  | Die maximale Anzahl Semaphore pro System.   |
|  | (SEMOPM)  |
|  | Die maximale Anzahl Operationen pro Semaphoraufruf.   |



| Parameter                 | Beschreibung   |
|---------------------------|--|
|                           | (SEMMNI)<br>Die maximale Anzahl Arrays.  |
| kernel.msgmni             | Die maximale Anzahl systemweiter Nachrichtenwarteschlangen.  |
| kernel.msgmax             | Die maximale Größe von Nachrichten (Byte).   |
| kernel.msgmnb             | Die standardmäßige maximale Größe der Warteschlange (Byte).  |
| kernel.randomize_va_space | Mit dem Parameter kernel.randomize_va_space wird die Verwendung von Speicher-ASLR für den Kernel konfiguriert. Inaktivieren Sie ASLR, da ASLR Fehler der DB2-Software zur Folge haben kann. Weitere ausführliche Informationen zu Linux-ASLR und DB2 enthält die Technote 1365583. |
| vm.swappiness             | Der Parameter vm.swappiness definiert, ob der Kernel Anwendungsspeicher aus physischem Arbeitsspeicher (RAM) auslagern kann. Weitere Informationen zu Kernelparametern enthält die Produktinformation zu DB2.  |
| vm.overcommit_memory      | Der Parameter vm.overcommit_memory hat Auswirkungen darauf, wie viel virtueller Speicher gemäß dem Kernel zugeordnet werden kann. Weitere Informationen zu Kernelparametern enthält die Produktinformation zu DB2.   |

7. Öffnen Sie Firewall-Ports für die Kommunikation mit dem Server. Führen Sie die folgenden Schritte aus:

a. Legen Sie die von der Netzschnittstelle verwendete Zone fest. Die Zone ist standardmäßig 'public'.

Geben Sie den folgenden Befehl aus:

```
# firewall-cmd --get-active-zones
public
  interfaces: ens4f0
```

b. Um die Standardportadresse für die Kommunikation mit dem Server zu verwenden, öffnen Sie TCP/IP-Port 1500 in der Linux-Firewall.

Geben Sie den folgenden Befehl aus:

```
firewall-cmd --zone=public --add-port=1500/tcp --permanent
```

Wenn ein anderer Wert als der Standardwert verwendet werden soll, können Sie eine Zahl zwischen 1024 und 32767 angeben. Wenn ein anderer Port als der Standardport geöffnet wird, müssen Sie diesen Port bei der Ausführung des Konfigurationsscripts angeben.

c. Wenn Sie planen, dieses System als einen Hub zu verwenden, öffnen Sie Port 11090, den Standardport für die sichere Kommunikation (HTTPS).

Geben Sie den folgenden Befehl aus:

```
firewall-cmd --zone=public --add-port=11090/tcp --permanent
```

d. Laden Sie die Firewalldefinitionen erneut, damit die Änderungen wirksam werden.

Geben Sie den folgenden Befehl aus:

```
firewall-cmd --reload
```

8. Überprüfen Sie, ob Benutzerprozessressourcengrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, gemäß den Richtlinien in Tabelle 2 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

Tabelle 2. Benutzerbegrenzwerte (ulimit-Werte)

| Typ des Benutzerbegrenzwerts                         | Einstellung | Wert      | Befehl zum Abfragen des Werts |
|--|-------------|-----------|-------------------------------|
| Maximale Größe der erstellten Kerndateien            | core        | Unlimited | ulimit -Hc                    |
| Maximale Größe eines Datensegments für einen Prozess | data        | Unlimited | ulimit -Hd                    |
| Maximale Dateigröße                                  | fsize       | Unlimited | ulimit -Hf                    |

| Typ des Benutzergrenzwerts         | Einstellung | Wert      | Befehl zum Abfragen des Werts |
|------------------------------------|-------------|-----------|-------------------------------|
| Maximale Anzahl offener Dateien    | nofile      | 65536     | <code>ulimit -Hn</code>       |
| Maximale Prozessorzeit in Sekunden | cpu         | Unlimited | <code>ulimit -Ht</code>       |
| Maximale Anzahl Benutzerprozesse   | nproc       | 16384     | <code>ulimit -Hu</code>       |

Wenn einer der Benutzergrenzwerte geändert werden muss, führen Sie die Anweisungen in der Dokumentation für Ihr Betriebssystem aus.

## Installation auf Windows-Systemen

Installieren Sie Microsoft Windows Server 2012 Standard Edition auf dem Serversystem und bereiten Sie das System für die Installation und Konfiguration des IBM Spectrum Protect-Servers vor.

### Vorgehensweise

1. Installieren Sie Windows Server 2016 Standard Edition gemäß den Anweisungen des Herstellers.
2. Ändern Sie die Windows-Kostensteuerungsrichtlinien, indem Sie die folgenden Schritte ausführen.
  - a. Öffnen Sie den Editor für lokale Sicherheitsrichtlinien, indem Sie `secpol.msc` ausführen.
  - b. Klicken Sie auf Lokale Richtlinien > Sicherheitsoptionen und stellen Sie sicher, dass die folgenden Benutzerkostensteuerungsrichtlinien inaktiviert sind:
    - Administratorbestätigungsmodus für das integrierte Administratorkonto
    - Alle Administratoren im Administratorbestätigungsmodus ausführen
3. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Installationsanweisungen für das Betriebssystem.
4. Wenden Sie Windows-Updates an und aktivieren Sie Zusatzfunktionen (optionale Features), indem Sie die folgenden Schritte ausführen:
  - a. Wenden Sie die neuesten Windows Server 2016-Updates an.
  - b. Installieren und aktivieren Sie das Windows 2012 R2-Feature Microsoft .NET Framework 3.5 über den Windows Server-Manager.
  - c. Aktualisieren Sie, falls erforderlich, die FC- und Ethernet-HBA-Einheitentreiber mit neueren Versionen.
  - d. Installieren Sie den für das verwendete Plattensystem geeigneten Multipath I/O-Treiber.
5. Öffnen Sie den TCP/IP-Standardport (1500) für die Kommunikation mit dem IBM Spectrum Protect-Server. Geben Sie beispielsweise den folgenden Befehl aus:

```
netsh advfirewall firewall add rule name="Sicherungsserver-Port 1500"
dir=in action=allow protocol=TCP localport=1500
```

6. Öffnen Sie auf dem Operations Center-Hub-Server den Standardport für die sichere Kommunikation (HTTPS) mit dem Operations Center. Die Portnummer ist 11090. Geben Sie beispielsweise den folgenden Befehl aus:

```
netsh advfirewall firewall add rule name="Operations Center-Port 11090"
dir=in action=allow protocol=TCP localport=11090
```

## Multipath I/O konfigurieren

Sie können Multipathing für Plattenspeicher aktivieren und konfigurieren. Die mit Ihrer Hardware zur Verfügung gestellte Dokumentation enthält ausführliche Anweisungen.

- AIX-Systeme
- Linux-Systeme
- Windows-Systeme

## AIX-Systeme

### Vorgehensweise

1. Bestimmen Sie die Fibre Channel-Portadresse, die für die Hostdefinition auf dem Plattensubsystem verwendet werden muss. Geben Sie den Befehl `lscfg` für jeden Port aus.
  - Geben Sie auf kleinen und mittelgroßen Systemen die folgenden Befehle aus:

```
lscfg -vps -l fcs0 | grep "Netzadresse"
lscfg -vps -l fcs1 | grep "Netzadresse"
```

- o Geben Sie auf großen Systemen die folgenden Befehle aus:

```
lscfg -vps -l fcs0 | grep "Netzadresse"
lscfg -vps -l fcs1 | grep "Netzadresse"
lscfg -vps -l fcs2 | grep "Netzadresse"
lscfg -vps -l fcs3 | grep "Netzadresse"
```

2. Stellen Sie sicher, dass die folgenden AIX-Dateigruppen installiert sind:

- o devices.common.IBM.mpio.rte
- o devices.fcp.disk.array.rte
- o devices.fcp.disk.rte

3. Geben Sie den Befehl `cfgmgr` aus, damit AIX die Hardware erneut überprüft und verfügbare Platten erkennt. Beispiel:

```
cfgmgr
```

4. Um die verfügbaren Platten aufzulisten, geben Sie den folgenden Befehl aus:

```
lsdev -Ccdisk
```

Es sollte eine ähnliche Ausgabe wie die folgende angezeigt werden:

```
hdisk0 Available 00-00-00 SAS Disk Drive
hdisk1 Available 00-00-00 SAS Disk Drive
hdisk2 Available 01-00-00 SAS Disk Drive
hdisk3 Available 01-00-00 SAS Disk Drive
hdisk4 Available 06-01-02 MPIO IBM 2076 FC Disk
hdisk5 Available 07-01-02 MPIO IBM 2076 FC Disk
...
```

5. Verwenden Sie die Ausgabe des Befehls `lsdev`, um die Einheiten-IDs für jede Platteneinheit zu ermitteln und aufzulisten.

Beispielsweise könnte eine Einheiten-ID `hdisk4` lauten. Sichern Sie die Liste der Einheiten-IDs für die Verwendung bei der Erstellung von Dateisystemen für den IBM Spectrum Protect-Server.

6. Korrelieren Sie die SCSI-Einheiten-IDs zu bestimmten Platten-LUNs aus dem Plattensystem, indem Sie detaillierte Informationen zu allen physischen Datenträgern im System auflisten. Geben Sie den folgenden Befehl aus:

```
lspv -u
```

Auf einem IBM® Storwize-System werden beispielsweise die folgenden Informationen für jede Einheit angezeigt:

```
hdisk4 00f8cf083fd97327 None active
3321360050763008101057800000000000003004214503IBMfcp
```

In dem Beispiel ist `6005076300810105780000000000030` die UID für den Datenträger, die von der Storwize-Managementsschnittstelle zurückgemeldet wurde.

Um die Plattengröße in Megabyte zu überprüfen und den Wert mit dem für das System aufgelisteten Wert zu vergleichen, geben Sie den folgenden Befehl aus:

```
bootinfo -s hdisk4
```

## Linux-Systeme

---

### Vorgehensweise

---

1. Editieren Sie die Datei `/etc/multipath.conf`, um Multipathing für Linux-Hosts zu aktivieren. Wenn die Datei `multipath.conf` nicht vorhanden ist, können Sie die Datei erstellen, indem Sie den folgenden Befehl ausgeben:

```
multipathconf --enable
```

Die folgenden Parameter wurden in `multipath.conf` zu Testzwecken auf einem IBM Storwize-System festgelegt:

```
defaults {
    user_friendly_names no
}

devices {
    device {
        vendor "IBM "
        product "2145"
```

```

        path_grouping_policy group_by_prio
        user_friendly_names no
        path_selector "round-robin 0"
        prio "alua"
        path_checker "tur"
        failback "immediate"
        no_path_retry 5
        rr_weight uniform
        rr_min_io_rq "1"
        dev_loss_tmo 120
    }
}

```

2. Definieren Sie die Multipath-Option so, dass Multipath zusammen mit dem System gestartet wird. Geben Sie die folgenden Befehle aus:

```

systemctl enable multipathd.service
systemctl start multipathd.service

```

3. Um sicherzustellen, dass Platten für das Betriebssystem sichtbar sind und durch Multipath verwaltet werden, geben Sie den folgenden Befehl aus:

```

multipath -l

```

4. Stellen Sie sicher, dass jede Einheit aufgelistet ist und über so viele Pfade wie erwartet verfügt. Anhand der Größe und Einheiten-ID können Sie die aufgelisteten Platten identifizieren.

Beispielsweise zeigt die folgende Ausgabe, dass einer 2-TB-Platte zwei Pfadgruppen und vier aktive Pfade zugeordnet sind. Die Größe von 2 TB bestätigt, dass die Platte einem Pooldateisystem entspricht. Suchen Sie anhand eines Teils der langen Einheiten-ID-Nummer (in diesem Beispiel 12) in der Managementschnittstelle des Plattensystems nach dem Datenträger.

```

[root@tapsrv01 code]# multipath -l
36005076802810c509800000000000012 dm-43 IBM,2145
size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|+- policy='round-robin 0' prio=0 status=active
| |- 2:0:1:18 sdcw 70:64 active undef running
| `-- 4:0:0:18 sdgb 131:112 active undef running
`-+- policy='round-robin 0' prio=0 status=enabled
   |- 1:0:1:18 sdat 66:208 active undef running
   `-- 3:0:0:18 sddy 128:0 active undef running

```

- a. Korrigieren Sie, falls erforderlich, Platten-LUN/Host-Zuordnungen und erzwingen Sie eine erneute Busüberprüfung. Beispiel:

```

echo "-- --" > /sys/class/scsi_host/host0/scan
echo "-- --" > /sys/class/scsi_host/host1/scan
echo "-- --" > /sys/class/scsi_host/host2/scan

```

Sie können für eine erneute Überprüfung der Platten-LUN/Host-Zuordnungen auch das System erneut starten.

- b. Stellen Sie sicher, dass Platten jetzt für Multipath I/O verfügbar sind, indem Sie den Befehl `multipath -l` erneut ausgeben.

5. Verwenden Sie die Multipath-Ausgabe, um die Einheiten-IDs für jede Platteneinheit zu ermitteln und aufzulisten.

Beispielsweise ist die Einheiten-ID für Ihre 2-TB-Platte `36005076802810c509800000000000012`.

Sichern Sie die Liste der Einheiten-IDs für die Verwendung im nächsten Schritt.

## Windows-Systeme

### Vorgehensweise

1. Stellen Sie sicher, dass Multipath I/O installiert ist. Installieren Sie, falls erforderlich, weitere anbieterspezifische Multipath-Treiber.
2. Um sicherzustellen, dass Platten für das Betriebssystem sichtbar sind und durch Multipath I/O verwaltet werden, geben Sie den folgenden Befehl aus:

```

c:\Programme\IBM\SDDDSM\datapath.exe query device

```

3. Überprüfen Sie die Multipath-Ausgabe und stellen Sie sicher, dass jede Einheit aufgelistet ist und über so viele Pfade wie erwartet verfügt. Anhand der Größe und Einheitenseriennummer können Sie die aufgelisteten Platten identifizieren. Beispielsweise können Sie anhand eines Teils der langen Einheitenseriennummer (in diesem Beispiel 34) in der Managementschnittstelle des Plattensystems nach dem Datenträger suchen. Die Größe von 2 TB bestätigt, dass die Platte einem Speicherpooldateisystem entspricht.

```

DEV#: 4 DEVICE NAME: Disk5 Part0 TYPE: 2145 POLICY: OPTIMIZED
SERIAL: 60050763008101057800000000000034 LUN SIZE: 2.0TB
=====
Path# Adapter/Hard Disk State Mode Select Errors
0 Scsi Port2 Bus0/Disk5 Part0 OPEN NORMAL 0 0
1 Scsi Port2 Bus0/Disk5 Part0 OPEN NORMAL 27176 0
2 Scsi Port3 Bus0/Disk5 Part0 OPEN NORMAL 28494 0
3 Scsi Port3 Bus0/Disk5 Part0 OPEN NORMAL 0 0

```

- Erstellen Sie unter Verwendung der in der Multipath-Ausgabe im vorherigen Schritt zurückgegebenen Seriennummern eine Liste der Platteneinheiten-IDs.

Beispielsweise ist die Einheiten-ID für Ihre 2-TB-Platte 60050763008101057800000000000034.

Sichern Sie die Liste der Einheiten-IDs für die Verwendung im nächsten Schritt.

- Um neue Platten online zu schalten und das Lesezugriffsattribut zu löschen, führen Sie diskpart.exe mit den folgenden Befehlen aus. Wiederholen Sie diesen Schritt für jede der Platten:

```

diskpart
select Disk 1
online disk
attribute disk clear readonly
select Disk 2
online disk
attribute disk clear readonly
< ... >
select Disk 49
online disk
attribute disk clear readonly
exit

```

## Benutzer-ID für den Server erstellen



Erstellen Sie die Benutzer-ID, die Eigner der IBM Spectrum Protect-Serverinstanz ist. Sie geben diese Benutzer-ID an, wenn Sie die Serverinstanz im Rahmen der Erstkonfiguration des Servers erstellen.

### Informationen zu diesem Vorgang

Sie können nur Kleinbuchstaben (a-z), Ziffern (0-9) und das Unterstrichszeichen (\_) für die Benutzer-ID angeben. Die Benutzer-ID und der Gruppenname müssen den folgenden Regeln entsprechen:

- Die Länge darf 8 Zeichen nicht überschreiten.
- Die Benutzer-ID und der Gruppenname dürfen nicht mit *ibm*, *sql*, *sys* oder einer Ziffer beginnen.
- Die Benutzer-ID und der Gruppenname dürfen nicht *user*, *admin*, *guest*, *public*, *local* oder ein in SQL reserviertes Wortes sein.

### Vorgehensweise

- Erstellen Sie mithilfe von Betriebssystembefehlen eine Benutzer-ID.
  -   Erstellen Sie eine Gruppe und eine Benutzer-ID im Ausgangsverzeichnis des Benutzers, der Eigner der Serverinstanz ist.

Um beispielsweise die Benutzer-ID *tsminst1* in der Gruppe *tsmsrvrs* mit dem Kennwort *tsminst1* zu erstellen, geben Sie die folgenden Befehle mit einer ID für einen Benutzer mit Verwaltungsaufgaben aus:

#### AIX-Betriebssysteme

```

mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1

```


#### Linux-Betriebssysteme

```

groupadd tsmsrvrs
useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
passwd tsminst1

```

Melden Sie sich von Ihrem System ab und anschließend wieder an. Wechseln Sie zu dem von Ihnen erstellten Benutzerkonto. Verwenden Sie ein interaktives Anmeldeprogramm, wie beispielsweise Telnet, damit Sie zur Eingabe des Kennworts aufgefordert werden und es, falls erforderlich, ändern können.

- o  Windows-Betriebssysteme Erstellen Sie eine Benutzer-ID und fügen Sie dann die neue ID der Gruppe 'Administratoren' hinzu. Um beispielsweise die Benutzer-ID `tsminst1` zu erstellen, geben Sie den folgenden Befehl aus:

```
net user tsminst1 * /add
```

Fügen Sie, nachdem Sie für den neuen Benutzer ein Kennwort erstellt und bestätigt haben, die Benutzer-ID der Gruppe 'Administratoren' hinzu, indem Sie die folgenden Befehle ausgeben:

```
net localgroup Administratoren tsminst1 /add
net localgroup DB2ADMNS tsminst1 /add
```

2. Melden Sie die neue Benutzer-ID ab.

## Dateisysteme für den Server vorbereiten

---

Sie müssen die Dateisystemkonfiguration ausführen, damit der Plattenspeicher vom Server verwendet werden kann.

- Dateisysteme auf AIX-Systemen vorbereiten  
Sie müssen Datenträgergruppen, logische Datenträger und Dateisysteme für den Server mithilfe von AIX Logical Volume Manager erstellen.
- Dateisysteme auf Linux-Systemen vorbereiten  
Sie müssen ext4- oder xfs-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.
- Dateisysteme auf Windows-Systemen vorbereiten  
Sie müssen NTFS-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

## Dateisysteme auf AIX-Systemen vorbereiten

---

Sie müssen Datenträgergruppen, logische Datenträger und Dateisysteme für den Server mithilfe von AIX Logical Volume Manager erstellen.

### Vorgehensweise

---

1. Erhöhen Sie die Warteschlangenlänge und die maximale Übertragungsgröße für alle verfügbaren *hdiskX*-Platten. Geben Sie für jede Platte die folgenden Befehle aus:

```
chdev -l hdisk4 -a max_transfer=0x100000
chdev -l hdisk4 -a queue_depth=32
chdev -l hdisk4 -a reserve_policy=no_reserve
chdev -l hdisk4 -a algorithm=round_robin
```

Sie dürfen diese Befehle nicht für interne Betriebssystemplatten, beispielsweise *hdisk0*, ausführen.

2. Erstellen Sie Datenträgergruppen für die IBM Spectrum Protect-Datenbank, die aktive Protokolldatei, das Archivprotokoll, die Datenbanksicherung und den Speicherpool. Geben Sie den Befehl `mkvg` unter Angabe der Einheiten-IDs für die entsprechenden zuvor ermittelten Platten aus.

Wenn beispielsweise die Einheitennamen *hdisk4*, *hdisk5* und *hdisk6* Datenbankplatten entsprechen, schließen Sie diese in die Datenbankdatenträgergruppe ein.

Systemgröße: Die folgenden Befehle basieren auf einer Konfiguration für ein mittelgroßes System. Für kleine und große Systeme müssen Sie die Syntax wie erforderlich anpassen.

```
mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
mkvg -S -y tsmactlog hdisk5
mkvg -S -y tsmarchlog hdisk6
mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
```

3. Bestimmen Sie die Namen der physischen Datenträger und die Anzahl freier physischer Partitionen, die beim Erstellen logischer Datenträger verwendet werden sollen. Geben Sie den Befehl `lsvg` für jede Datenträgergruppe aus, die Sie im vorherigen Schritt erstellt haben.

Beispiel:

```
lsvg -p tsmdb
```

Die Ausgabe sieht ähnlich wie die folgende aus. Die Spalte *FREE PPs* gibt die freien physischen Partitionen an:

```
tsmdb:
PV_NAME  PV STATE  TOTAL PPs  FREE PPs  FREE DISTRIBUTION
```

```

hdisk4  active      1631      1631      327..326..326..326..326
hdisk5  active      1631      1631      327..326..326..326..326
hdisk6  active      1631      1631      327..326..326..326..326

```

- Erstellen Sie mit dem Befehl `mklv` logische Datenträger in jeder Datenträgergruppe. Die Datenträgergröße, die Datenträgergruppe und die Einheitenamen sind, abhängig von der Größe Ihres Systems und Variationen in Ihrer Plattenkonfiguration, unterschiedlich.

Um beispielsweise die Datenträger für die IBM Spectrum Protect-Datenbank auf einem mittelgroßen System zu erstellen, geben Sie die folgenden Befehle aus:

```

mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4

```

- Formatieren Sie Dateisysteme auf jedem logischen Datenträger mit dem Befehl `crfs`.

Um beispielsweise die Dateisysteme für die Datenbank auf einem mittelgroßen System zu formatieren, geben Sie die folgenden Befehle aus:

```

crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes

```

- Führen Sie für alle neu erstellten Dateisysteme einen Mount durch, indem Sie den folgenden Befehl eingeben:

```
mount -a
```

- Listen Sie alle Dateisysteme auf, indem Sie den Befehl `df` ausgeben. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Überprüfen Sie außerdem den verfügbaren Speicherbereich.

Das folgende Beispiel der Befehlsausgabe zeigt, dass der Umfang des belegten Speicherbereichs normalerweise 1 % beträgt:

```

tapsrv07> df -g /tsminst1/*
Filesystem      GB blocks  Free      %Used   Iused   %Iused   Mounted on
/dev/tsmact00   195.12    194.59    1%        4        1%      /tsminst1/TSMalog

```

- Überprüfen Sie, ob die in Benutzer-ID für den Server erstellen erstellte Benutzer-ID Schreib-/Lesezugriff auf die Verzeichnisse für den IBM Spectrum Protect-Server hat.

## Dateisysteme auf Linux-Systemen vorbereiten

Sie müssen ext4- oder xfs-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

### Vorgehensweise

- Verwenden Sie die zuvor generierte Liste der Einheiten-IDs und geben Sie den Befehl `mkfs` aus, um für jede LUN-Speichereinheit ein Dateisystem zu erstellen und zu formatieren. Geben Sie die Einheiten-ID im Befehl an. Siehe die folgenden Beispiele. Formatieren Sie für die Datenbank ext4-Dateisysteme:

```
mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c50980000000000012
```

Formatieren Sie für Speicherpool-LUNs xfs-Dateisysteme:

```
mkfs -t xfs /dev/mapper/3600507630081010578000000000002c3
```

Abhängig davon, wie viele verschiedene Einheiten vorhanden sind, können Sie den Befehl `mkfs` bis zu 50 Mal ausgeben.

- Erstellen Sie Mountpunktverzeichnisse für Dateisysteme.

Geben Sie den Befehl `mkdir` für jedes Verzeichnis aus, das erstellt werden muss. Verwenden Sie die in den Arbeitsblättern zur Planung verwendeten Verzeichniswerte.

Um beispielsweise das Serverinstanzverzeichnis unter Verwendung des Standardwerts zu erstellen, geben Sie den folgenden Befehl aus:

```
mkdir /tsminst1
```

Wiederholen Sie den Befehl `mkdir` für jedes Dateisystem.

- Fügen Sie in der Datei `/etc/fstab` für jedes Dateisystem einen Eintrag hinzu, damit für die Dateisysteme beim Serverstart automatisch ein Mount durchgeführt wird.

Beispiel:

```
/dev/mapper/36005076802810c50980000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
```

4. Führen Sie für die Dateisysteme, die der Datei `/etc/fstab` hinzugefügt wurden, einen Mount durch, indem Sie den Befehl `mount -a` ausgeben.
5. Listen Sie alle Dateisysteme auf, indem Sie den Befehl `df` ausgeben. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Überprüfen Sie außerdem den verfügbaren Speicherbereich. Das folgende Beispiel für ein IBM® Storwize-System zeigt, dass der Umfang des belegten Speicherbereichs normalerweise 1 % beträgt:

```
[root@tapsrv04 ~]# df -h /tsminst1/*
Filesystem                                Size  Used Avail Use% Mounted on
/dev/mapper/36005076300810105780000000000003 134G  188M 132G  1%  /tsminst1/TSMalog
```

6. Überprüfen Sie, ob die in Benutzer-ID für den Server erstellen erstellte Benutzer-ID Schreib-/Lesezugriff auf die Verzeichnisse für IBM Spectrum Protect hat.

## Dateisysteme auf Windows-Systemen vorbereiten

---

Sie müssen NTFS-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

### Vorgehensweise

---

1. Erstellen Sie Mountpunktverzeichnisse für Dateisysteme.  
Geben Sie den Befehl `md` für jedes Verzeichnis aus, das erstellt werden muss. Verwenden Sie die in den Arbeitsblättern zur Planung verwendeten Verzeichniswerte. Um beispielsweise das Serverinstanzverzeichnis unter Verwendung des Standardwerts zu erstellen, geben Sie den folgenden Befehl aus:

```
md c:\tsminst1
```

Wiederholen Sie den Befehl `md` für jedes Dateisystem.

2. Erstellen Sie für jede Platten-LUN, die einem Verzeichnis unter dem Serverinstanzverzeichnis zugeordnet ist, unter Verwendung des Windows-Datenträgermanagers (Volume-Manager) einen Datenträger.

Rufen Sie `Server-Manager > Datei- und Speicherdienste` auf und führen Sie die folgenden Schritte für jede Platte aus, die der im vorherigen Schritt erstellten LUN-Zuordnung entspricht:

- a. Schalten Sie die Platte online.
- b. Initialisieren Sie die Platte mit dem GPT-Basistyp, dem Standardwert.
- c. Erstellen Sie einen einfachen Datenträger, der den gesamten Speicherbereich auf der Platte belegt. Formatieren Sie das Dateisystem mit NTFS und ordnen Sie einen Kennsatz zu, der den Zweck des Datenträgers angibt, wie beispielsweise `TSMfile00`. Ordnen Sie den neuen Datenträger keinem Laufwerksbuchstaben zu. Ordnen Sie den Datenträger stattdessen einem Verzeichnis unter dem Instanzverzeichnis zu, wie beispielsweise `C:\tsminst1\TSMfile00`.  
Tipp: Legen Sie den Datenträgerkennsatz und die Bezeichnungen für Verzeichniszuordnungen auf der Basis der Größe der aufgelisteten Platte fest.

3. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Listen Sie alle Dateisysteme auf, indem Sie den Befehl `mountvol` ausgeben; überprüfen Sie dann die Ausgabe. Beispiel:

```
\\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
C:\tsminst1\TSMdbspace00\
```

4. Starten Sie nach dem Abschluss der Plattenkonfiguration das System erneut.

### Nächste Schritte

---

Mithilfe von Windows Explorer können Sie den Umfang des freien Speicherbereichs für jeden Datenträger prüfen.

## Server und das Operations Center installieren

---

Verwenden Sie den grafisch orientierten Assistenten von IBM® Installation Manager, um die Komponenten zu installieren.

- Installation auf AIX- und Linux-Systemen  
Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf dem ersten Serversystem.
- Installation auf Windows-Systemen  
Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf dem ersten Serversystem.



# Installation auf AIX- und Linux-Systemen

---

Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf dem ersten Serversystem.


## Vorbereitende Schritte

---

Überprüfen Sie, ob das Betriebssystem auf die erforderliche Sprache gesetzt ist. Standardmäßig entspricht die Sprache für das Betriebssystem der Sprache für den Installationsassistenten.

## Vorgehensweise

---

1.  Überprüfen Sie, ob die erforderlichen RPM-Dateien auf Ihrem System installiert sind.

Ausführliche Informationen finden Sie in Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren.


2. Überprüfen Sie vor dem Herunterladen des Installationspakets, ob genügend Speicherbereich zum Speichern der Installationsdateien vorhanden ist, wenn die Dateien aus dem Produktpaket extrahiert werden. Informationen zum Speicherbedarf enthält das Downloaddokument unter Technote 4042992.
3. Rufen Sie Passport Advantage auf und laden Sie die Paketdatei in ein leeres Verzeichnis Ihrer Wahl herunter.
4. Stellen Sie sicher, dass für das Paket die Berechtigung zur Ausführung festgelegt ist. Ändern Sie, falls erforderlich, die Dateiberechtigungen, indem Sie den folgenden Befehl ausgeben:

```
chmod a+x Paketname.bin
```

5. Extrahieren Sie das Paket, indem Sie den folgenden Befehl ausgeben:

```
./Paketname.bin
```

Dabei ist *Paketname* der Name der Downloaddatei.

6.  Stellen Sie sicher, dass der folgende Befehl aktiviert ist, damit die Assistenten korrekt ausgeführt werden:

```
lsuser
```

Standardmäßig ist der Befehl aktiviert.

7. Wechseln Sie in das Verzeichnis, in das die ausführbare Datei gestellt wurde.
8. Starten Sie den Installationsassistenten, indem Sie den folgenden Befehl ausgeben:

```
./install.sh
```

Wenn Sie die zu installierenden Pakete auswählen, wählen Sie sowohl den Server als auch das Operations Center aus.

## Nächste Schritte



---

- Wenn während des Installationsprozesses Fehler auftreten, werden die Fehler in Protokolldateien aufgezeichnet, die im Protokollverzeichnis von IBM Installation Manager gespeichert sind.

Um Installationsprotokolldateien in Installation Manager anzuzeigen, klicken Sie auf Datei > Protokoll anzeigen. Um diese Protokolldateien in Installation Manager zu erfassen, klicken Sie auf Hilfe > Daten zur Fehleranalyse exportieren.

- Rufen Sie nach der Installation des Servers, aber vor der Anpassung des Servers für Ihre Verwendung die IBM Spectrum Protect-Unterstützungssite auf. Klicken Sie auf Support und Downloads und wenden Sie alle zutreffenden Fixes an.
- Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren  
RPM-Dateien sind für den grafisch orientierten Assistenten von IBM Installation Manager erforderlich.

### Zugehörige Tasks:

-  Andere Methoden zum Installieren von IBM Spectrum Protect-Komponenten (AIX)
-  Andere Methoden zum Installieren von IBM Spectrum Protect-Komponenten (Linux)

# Installation auf Windows-Systemen

---

Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf dem ersten Serversystem.

## Vorbereitende Schritte

---

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Überprüfen Sie, ob das Betriebssystem auf die erforderliche Sprache gesetzt ist. Standardmäßig entspricht die Sprache für das Betriebssystem der Sprache für den Installationsassistenten.
- Stellen Sie sicher, dass die Benutzer-ID, die während der Installation verwendet werden soll, für einen Benutzer mit der Berechtigung eines lokalen Administrators gilt.

## Vorgehensweise

---

1. Überprüfen Sie vor dem Herunterladen des Installationspakets, ob genügend Speicherbereich zum Speichern der Installationsdateien vorhanden ist, wenn die Dateien aus dem Produktpaket extrahiert werden. Informationen zum Speicherbedarf enthält das Downloaddokument unter Technote 4042993.
2. Rufen Sie Passport Advantage auf und laden Sie die Paketdatei in ein leeres Verzeichnis Ihrer Wahl herunter.
3. Wechseln Sie in das Verzeichnis, in das die ausführbare Datei gestellt wurde.
4. Doppelklicken Sie auf die ausführbare Datei, um die Datei in das aktuelle Verzeichnis zu extrahieren.
5. Starten Sie in dem Verzeichnis, in das die Installationsdateien extrahiert wurden, den Installationsassistenten, indem Sie auf die Datei install.bat doppelklicken. Wenn Sie die zu installierenden Pakete auswählen, wählen Sie sowohl den Server als auch das Operations Center aus.

## Nächste Schritte

---

- Wenn während des Installationsprozesses Fehler auftreten, werden die Fehler in Protokolldateien aufgezeichnet, die im Protokollverzeichnis von IBM® Installation Manager gespeichert sind.

Um Installationsprotokolldateien in Installation Manager anzuzeigen, klicken Sie auf Datei > Protokoll anzeigen. Um diese Protokolldateien in Installation Manager zu erfassen, klicken Sie auf Hilfe > Daten zur Fehleranalyse exportieren.

- Rufen Sie nach der Installation des Servers, aber vor der Anpassung des Servers für Ihre Verwendung die IBM Spectrum Protect-Unterstützungssite auf. Klicken Sie auf Support und Downloads und wenden Sie alle zutreffenden Fixes an.

### Zugehörige Tasks:

- 🔗 Andere Methoden zum Installieren von IBM Spectrum Protect-Komponenten

## Server und das Operations Center konfigurieren

---

Nachdem Sie die Komponenten installiert haben, führen Sie die Konfiguration für den IBM Spectrum Protect-Server und das Operations Center aus.

- Serverinstanz konfigurieren  
Verwenden Sie den IBM Spectrum Protect-Assistenten für die Serverinstanzkonfiguration, um die Erstkonfiguration für den Server auszuführen.
- Client für Sichern/Archivieren installieren  
Installieren Sie als Best Practice den IBM Spectrum Protect-Client für Sichern/Archivieren auf dem Serversystem, sodass der Verwaltungsbefehlszeilenclient und der Scheduler verfügbar sind.
- Optionen für den Server festlegen  
Überprüfen Sie die Serveroptionsdatei, die mit dem IBM Spectrum Protect-Server installiert wird, um sicherzustellen, dass die korrekten Werte für Ihr System festgelegt sind.
- Sichere Kommunikation mit Transport Layer Security konfigurieren  
Um Daten zu verschlüsseln und die sichere Kommunikation in Ihrer Umgebung zu ermöglichen, ist Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) auf dem IBM Spectrum Protect-Server und dem Client für Sichern/Archivieren aktiviert. Kommunikationsanforderungen zwischen dem Server und dem Client werden mithilfe eines SSL-Zertifikats geprüft.
- Operations Center konfigurieren  
Führen Sie nach der Installation des Operations Center die folgenden Konfigurationsschritte aus, um mit der Verwaltung Ihrer Speicherumgebung zu beginnen.
- Produktlizenz registrieren  
Verwenden Sie zum Registrieren Ihrer Lizenz für das Produkt IBM Spectrum Protect den Befehl REGISTER LICENSE.
- Datenduplizierung konfigurieren  
Erstellen Sie einen Verzeichniscontainerspeicherpool und mindestens ein Verzeichnis für die Verwendung der Inline-Datenduplizierung.
- Datenaufbewahrungsregeln für Ihr Unternehmen definieren  
Nachdem Sie einen Verzeichniscontainerspeicherpool für die Datenduplizierung erstellt haben, aktualisieren Sie die Serverstandardmaßnahme für die Verwendung des neuen Speicherpools. Die Seite Services im Operations Center wird vom Assistenten Speicherpool hinzufügen zur Ausführung dieser Task geöffnet.
- Zeitpläne für Serververwaltungsaktivitäten definieren  
Erstellen Sie Zeitpläne für jede Serververwaltungsoperation, indem Sie den Befehl DEFINE SCHEDULE im Command Builder des Operations Center verwenden.

- Clientzeitpläne definieren  
Erstellen Sie mithilfe des Operations Center Zeitpläne für Clientoperationen.

## Serverinstanz konfigurieren

---

Verwenden Sie den IBM Spectrum Protect-Assistenten für die Serverinstanzkonfiguration, um die Erstkonfiguration für den Server auszuführen.


### Vorbereitende Schritte

---

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Auf dem System, auf dem IBM Spectrum Protect installiert wurde, muss der X Window System-Client vorhanden sein. Außerdem muss ein X Window System-Server auf Ihrem Desktop ausgeführt werden.
- Für das System muss das Secure Shell-Protokoll (SSH-Protokoll) aktiviert sein. Stellen Sie sicher, dass der Port auf den Standardwert 22 gesetzt ist und dass der Port nicht durch eine Firewall blockiert wird. Sie müssen die Kennwortauthentifizierung in der Datei `sshd_config` im Verzeichnis `/etc/ssh/` aktivieren. Stellen Sie außerdem sicher, dass der SSH-Dämonservice über die Zugriffsberechtigungen verfügt, um mithilfe des Werts `localhost` eine Verbindung zum System herstellen zu können.
- Sie müssen sich mit der Benutzer-ID, die Sie für die Serverinstanz erstellt hatten, unter Verwendung des SSH-Protokolls bei IBM Spectrum Protect anmelden können. Wenn Sie den Assistenten verwenden, müssen Sie diese Benutzer-ID und das Kennwort für den Zugriff auf dieses System angeben.
- Wenn Sie in den vorhergehenden Schritten Änderungen an den Einstellungen vorgenommen haben, starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.

 Überprüfen Sie, ob der Remoteregistrierungsdienst gestartet wurde, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie auf Start > Verwaltung > Dienste. Wählen Sie im Fenster Dienste Remoteregistrierung aus. Wurde der Dienst nicht gestartet, klicken Sie auf Starten.
2. Stellen Sie sicher, dass die Ports 137, 139 und 445 nicht durch eine Firewall blockiert sind:
  - a. Klicken Sie auf Start > Systemsteuerung > Windows-Firewall.
  - b. Wählen Sie Erweiterte Einstellungen aus.
  - c. Wählen Sie Eingehende Regeln aus.
  - d. Wählen Sie Neue Regel aus.
  - e. Erstellen Sie eine Portregel für die TCP-Ports 137, 139 und 445, um Verbindungen für Domänennetze und private Netze zu ermöglichen.
3. Konfigurieren Sie die Benutzerkontensteuerung, indem Sie auf die Optionen für die lokale Sicherheitsrichtlinie zugreifen und die folgenden Schritte ausführen.
  - a. Klicken Sie auf Start > Verwaltung > Lokale Sicherheitsrichtlinie. Erweitern Sie Lokale Richtlinien > Sicherheitsoptionen.
  - b. Falls noch nicht bereits aktiviert, aktivieren Sie das integrierte Administratorkonto, indem Sie Konten: Administratorkontostatus > Aktivieren > OK auswählen.
  - c. Falls noch nicht bereits inaktiviert, inaktivieren Sie die Benutzerkontensteuerung für alle Windows-Administratoren, indem Sie Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen > Inaktivieren > OK auswählen.
  - d. Falls noch nicht bereits inaktiviert, inaktivieren Sie die Benutzerkontensteuerung für das integrierte Administratorkonto, indem Sie Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto > Inaktivieren > OK auswählen.
4. Wenn Sie in den vorhergehenden Schritten Änderungen an den Einstellungen vorgenommen haben, starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.


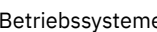

### Informationen zu diesem Vorgang

---



Der Assistent kann gestoppt und erneut gestartet werden, der Server ist jedoch erst betriebsbereit, wenn der gesamte Konfigurationsprozess abgeschlossen ist.

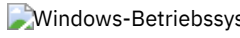
### Vorgehensweise

---

1. Starten Sie die lokale Version des Assistenten.
  -   Öffnen Sie das Programm `dsmicfgx` im Verzeichnis `/opt/tivoli/tsm/server/bin`. Dieser Assistent kann nur als Rootbenutzer ausgeführt werden.
  -  Klicken Sie auf Start > Alle Programme > IBM Spectrum Protect > Konfigurationsassistent.
2. Führen Sie die Anweisungen aus, um die Konfiguration auszuführen. Verwenden Sie die während der IBM Spectrum Protect-Systemkonfiguration aufgezeichneten Informationen (siehe Arbeitsblätter zur Planung), um Verzeichnisse und Optionen im

Assistenten anzugeben.

  Legen Sie im Fenster Serverinformationen fest, dass der Server automatisch unter Verwendung der Instanzbenutzer-ID gestartet werden soll, wenn das System bootet.

 Mithilfe des Konfigurationsassistenten wird festgelegt, dass der Server automatisch gestartet werden soll, wenn ein Warmstart durchgeführt wird.

## Client für Sichern/Archivieren installieren

Installieren Sie als Best Practice den IBM Spectrum Protect-Client für Sichern/Archivieren auf dem Serversystem, sodass der Verwaltungsbefehlszeilenclient und der Scheduler verfügbar sind.

### Vorgehensweise

Um den Client für Sichern/Archivieren zu installieren, führen Sie die Installationsanweisungen für Ihr Betriebssystem aus.

- UNIX- und Linux-Clients für Sichern/Archivieren installieren
- Windows-Client für Sichern/Archivieren installieren

## Optionen für den Server festlegen

Überprüfen Sie die Serveroptionsdatei, die mit dem IBM Spectrum Protect-Server installiert wird, um sicherzustellen, dass die korrekten Werte für Ihr System festgelegt sind.

### Vorgehensweise

1. Wechseln Sie in das Serverinstanzverzeichnis und öffnen Sie die Datei dsmserv.opt.
2. Überprüfen Sie die Werte in der folgenden Tabelle und Ihre Serveroptionseinstellungen auf der Basis der Systemgröße.

| Serveroption        | Wert für kleine Systeme                               | Wert für mittelgroße Systeme                          | Wert für große Systeme                                |
|---------------------|---|---|---|
| ACTIVELOGDIRECTORY  | Während der Konfiguration angegebener Verzeichnispfad | Während der Konfiguration angegebener Verzeichnispfad | Während der Konfiguration angegebener Verzeichnispfad |
| ACTIVELOGSIZE       | 131072  | 131072  | 262144  |
| ARCHLOGCOMPRESS     | Yes   | No  | No  |
| ARCHLOGDIRECTORY    | Während der Konfiguration angegebener Verzeichnispfad | Während der Konfiguration angegebener Verzeichnispfad | Während der Konfiguration angegebener Verzeichnispfad |
| COMMMETHOD          | TCPIP   | TCPIP   | TCPIP   |
| COMMTIMEOUT         | 3600  | 3600  | 3600  |
| DEDUPREQUIRESBACKUP | No  | No  | No  |
| DEVCONFIG           | devconf.dat   | devconf.dat   | devconf.dat   |
| EXPINTERVAL         | 0   | 0   | 0   |
| IDLETIMEOUT         | 60  | 60  | 60  |
| MAXSESSIONS         | 250   | 500   | 1000  |
| NUMOPENVOLSALLOWED  | 20  | 20  | 20  |
| TCPADMINPORT        | 1500  | 1500  | 1500  |
| TCPPORT             | 1500  | 1500  | 1500  |
| VOLUMEHISTORY       | volhist.dat   | volhist.dat   | volhist.dat   |

Aktualisieren Sie, falls erforderlich, Serveroptionseinstellungen in Übereinstimmung mit den Werten in der Tabelle. Um Aktualisierungen durchzuführen, schließen Sie die Datei dsmserv.opt und definieren Sie die Optionen mit dem Befehl SETOPT in der Verwaltungsbefehlszeilenschnittstelle.

Um beispielsweise die Option IDLETIMEOUT mit 60 zu aktualisieren, geben Sie den folgenden Befehl aus:

```
setopt idletimeout 60
```

3. Um für den Server, die Clients und das Operations Center die sichere Kommunikation zu konfigurieren, überprüfen Sie die Optionen in der folgenden Tabelle.

| Serveroption | Alle Systemgrößen   |
|--------------|---|
| SSLFIPSMODE  | NO  |
| TCPPORT      | Geben Sie die Nummer des Ports an, an dem der Server auf Anforderungen von TCP/IP- und SSL-fähigen Sitzungen des Clients wartet.                          |
| TCPADMINPORT | Geben Sie die Adresse des Ports an, an dem der Server auf Anforderungen von TCP/IP- und SSL-fähigen Sitzungen des Verwaltungsbefehlszeilenclients wartet. |

Wenn einer der Optionswerte aktualisiert werden muss, editieren Sie die Datei dmserv.opt unter Verwendung der folgenden Anleitungen:

- Entfernen Sie den Stern am Anfang einer Zeile, um eine Option zu aktivieren.
- Geben Sie in jeder Zeile nur eine einzige Option und den für die Option angegebenen Wert ein.
- Wenn eine Option in mehreren Einträgen in der Datei vorkommt, verwendet der Server den letzten Eintrag.

Sichern Sie Ihre Änderungen und schließen Sie die Datei. Wenn Sie die Datei dmserv.opt direkt editieren, müssen Sie den Server erneut starten, damit die Änderungen wirksam werden.

#### Zugehörige Verweise:

- ➔ Referenz für Serveroptionen
- ➔ SETOPT (Serveroption für dynamische Aktualisierung definieren)

## Sichere Kommunikation mit Transport Layer Security konfigurieren

Um Daten zu verschlüsseln und die sichere Kommunikation in Ihrer Umgebung zu ermöglichen, ist Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) auf dem IBM Spectrum Protect-Server und dem Client für Sichern/Archivieren aktiviert. Kommunikationsanforderungen zwischen dem Server und dem Client werden mithilfe eines SSL-Zertifikats geprüft.

### Informationen zu diesem Vorgang

Ab IBM Spectrum Protect Version 8.1.2 ist SSL standardmäßig aktiviert und der IBM Spectrum Protect-Server und der Client für Sichern/Archivieren werden automatisch für die gegenseitige Kommunikation unter Verwendung des TLS 1.2-Protokolls konfiguriert.

Wie in der folgenden Abbildung gezeigt können Sie die sichere Kommunikation zwischen dem Server und dem Client für Sichern/Archivieren manuell konfigurieren, indem Sie Optionen in der Server- und der Clientoptionsdatei definieren und dann das selbst signierte Zertifikat, das auf dem Server generiert wird, an den Client übertragen. Sie können auch stattdessen ein eindeutiges Zertifikat, das von einer Zertifizierungsstelle (CA) signiert ist, anfordern und übertragen.



Weitere Informationen zum Konfigurieren des Servers und von Clients für die SSL- oder TLS-Kommunikation finden Sie in Speicheragenten, Server, Clients und das Operations Center für die Verbindung zum Server unter Verwendung von SSL konfigurieren.

## Operations Center konfigurieren

Führen Sie nach der Installation des Operations Center die folgenden Konfigurationsschritte aus, um mit der Verwaltung Ihrer Speicherumgebung zu beginnen.

### Vorbereitende Schritte

Wenn Sie zum ersten Mal die Verbindung zum Operations Center herstellen, müssen Sie die folgenden Informationen angeben:

- Verbindungsinformationen für den Server, der als Hub-Server festgelegt werden soll
- Anmeldeberechtigungsnaehweise für eine Administrator-ID, die für diesen Server definiert ist

### Vorgehensweise

1. Legen Sie den Hub-Server fest. Geben Sie in einem Web-Browser die folgende Adresse ein:

```
https://Hostname:sicherer_Port/oc
```

Erläuterungen:

- *Hostname* gibt den Namen des Computers an, auf dem das Operations Center installiert ist.
- *Sicherer\_Port* gibt die Portnummer an, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet.

Wenn beispielsweise der Hostname tsm.storage.mylocation.com lautet und der standardmäßige sichere Port für das Operations Center (Port 11090) verwendet wird, ist die Adresse wie folgt:

```
https://tsm.storage.mylocation.com:11090/oc
```

Wenn Sie sich zum ersten Mal beim Operations Center anmelden, führt Sie ein Assistent durch eine Erstkonfiguration, um einen neuen Administrator mit Systemberechtigung auf dem Server zu konfigurieren.

2. Konfigurieren Sie die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server, indem Sie das Protokoll Secure Sockets Layer (SSL) konfigurieren.  
  
Führen Sie die Anweisungen in Kommunikation zwischen dem Operations Center und dem Hub-Server schützen aus.
3. Optional: Um einen täglichen E-Mail-Bericht mit einer Zusammenfassung des Systemstatus zu empfangen, konfigurieren Sie Ihre E-Mail-Einstellungen im Operations Center.  
  
Führen Sie die Anweisungen in Systemstatus mithilfe von E-Mail-Berichten verfolgen aus.
  - Kommunikation zwischen dem Operations Center und dem Hub-Server schützen  
Um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server zu ermöglichen, fügen Sie das TLS-Zertifikat des Hub-Servers der Truststore-Datei des Operations Center hinzu.

## Produktlizenz registrieren

---

Verwenden Sie zum Registrieren Ihrer Lizenz für das Produkt IBM Spectrum Protect den Befehl REGISTER LICENSE.

### Informationen zu diesem Vorgang


---

Lizenzen werden in Registrierungszertifikatsdateien gespeichert, die Lizenzinformationen für das Produkt enthalten. Die Registrierungszertifikatsdateien befinden sich auf den Installationsmedien und werden während der Installation auf den Server gestellt. Wenn Sie das Produkt registrieren, werden die Lizenzen in einer NODELOCK-Datei im aktuellen Verzeichnis gespeichert.

### Vorgehensweise

---

Registrieren Sie eine Lizenz, indem Sie den Namen der Registrierungszertifikatsdatei angeben, die die Lizenz enthält. Um den Command Builder des Operations Center für diese Task zu verwenden, führen Sie die folgenden Schritte aus.


1. Öffnen Sie das Operations Center.
2. Öffnen Sie den Command Builder des Operations Center, indem Sie den Mauszeiger über das Symbol für Einstellungen  bewegen und auf Command Builder klicken.
3. Geben Sie den Befehl REGISTER LICENSE aus. Um beispielsweise eine IBM Spectrum Protect-Basislizenz zu registrieren, geben Sie den folgenden Befehl aus:

```
register license file=tsmbasic.lic
```


### Nächste Schritte

---

Sichern Sie die Installationsmedien, die Ihre Registrierungszertifikatsdateien enthalten. Möglicherweise müssen Sie Ihre Lizenz erneut registrieren, wenn beispielsweise eine der folgenden Bedingungen erfüllt ist:

- Der Server wird auf einen anderen Computer versetzt.
- Die NODELOCK-Datei ist beschädigt. Der Server speichert Lizenzinformationen in der NODELOCK-Datei, die sich in dem Verzeichnis befindet, von dem aus der Server gestartet wird.
-  Linux-Betriebssysteme Sie ändern den Prozessorchip, der dem Server zugeordnet ist, auf dem der Server installiert ist.

**Zugehörige Verweise:**

 REGISTER LICENSE (Neue Lizenz registrieren)

## Dateneduplizierung konfigurieren

Erstellen Sie einen Verzeichniscontainerspeicherpool und mindestens ein Verzeichnis für die Verwendung der Inline-Dateneduplizierung.

### Vorbereitende Schritte

Verwenden Sie für diese Task die aufgezeichneten Informationen zu Speicherpoolverzeichnissen (siehe Arbeitsblätter zur Planung).

### Vorgehensweise

1. Öffnen Sie das Operations Center.
2. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Speicher.
3. Klicken Sie in der angezeigten Liste auf Speicherpools.
4. Klicken Sie auf die Schaltfläche +Speicherpool.
5. Führen Sie die Schritte im Assistenten Speicherpool hinzufügen aus:
  - o Um die Inline-Dateneduplizierung verwenden zu können, wählen Sie einen Speicherpool Verzeichnis unter dem containerbasierten Speicher aus.
  - o Wenn Sie Verzeichnisse für den Verzeichniscontainerspeicherpool konfigurieren, geben Sie die Verzeichnispfade an, die während der Systemkonfiguration für Speicher erstellt wurden.
6. Klicken Sie nach dem Konfigurieren des neuen Verzeichniscontainerspeicherpools auf Schließen & Maßnahmen anzeigen, um eine Verwaltungsklasse zu aktualisieren und mit der Verwendung des Speicherpools zu beginnen.

## Datenaufbewahrungsregeln für Ihr Unternehmen definieren

Nachdem Sie einen Verzeichniscontainerspeicherpool für die Dateneduplizierung erstellt haben, aktualisieren Sie die Serverstandardmaßnahme für die Verwendung des neuen Speicherpools. Die Seite Services im Operations Center wird vom Assistenten Speicherpool hinzufügen zur Ausführung dieser Task geöffnet.

### Vorgehensweise

1. Wählen Sie auf der Seite Services im Operations Center die Domäne STANDARD aus und klicken Sie auf Details.
2. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen. Die Seite Maßnahmengruppen gibt den Namen der aktiven Maßnahmengruppe an und listet alle Verwaltungsklassen für diese Maßnahmengruppe auf.
3. Klicken Sie auf die Umschaltfläche Konfigurieren und führen Sie die folgenden Änderungen durch:
  - o Ändern Sie das Sicherungsziel für die Verwaltungsklasse STANDARD in den Verzeichniscontainerspeicherpool.
  - o Ändern Sie den Wert für die Spalte 'Sicherungen' in Keine Begrenzung.
  - o Ändern Sie den Aufbewahrungszeitraum. Setzen Sie den Wert für die Spalte 'Zusätzliche Sicherungen aufbewahren' abhängig von Ihren Geschäftsanforderungen auf 30 Tage oder mehr.
4. Sichern Sie Ihre Änderungen und klicken Sie erneut auf die Umschaltfläche Konfigurieren, damit die Maßnahmengruppe nicht mehr editierbar ist.
5. Aktivieren Sie die Maßnahmengruppe, indem Sie auf Aktivieren klicken.

#### Zugehörige Tasks:

Regeln zum Sichern und Archivieren von Clientdaten angeben

## Zeitpläne für Serververwaltungsaktivitäten definieren

Erstellen Sie Zeitpläne für jede Serververwaltungsoperation, indem Sie den Befehl DEFINE SCHEDULE im Command Builder des Operations Center verwenden.

### Informationen zu diesem Vorgang

Planen Sie die Ausführung von Serververwaltungsoperationen im Anschluss an Clientsicherungsoperationen. Sie können das Timing von Zeitplänen steuern, indem Sie die Startzeit in Kombination mit der Dauer für jede Operation definieren.

Das folgende Beispiel zeigt die Planung von Serververwaltungsprozessen in Kombination mit dem Clientsicherungszeitplan für eine Plattenspeicherlösung für mehrere Standorte.

| Operation       | Zeitplan              |
|-----------------|-----------------------|
| Clientsicherung | Startet um 22:00 Uhr. |

| Operation  | Zeitplan   |
|--|--|
| Knotenreplikation  | Startet um 08:00 Uhr bzw. 10 Stunden nach dem Start der Clientsicherung.   |
| Verarbeitung für die Datenbank und die Dateien zur Wiederherstellung nach einem Katastrophenfall | <ul style="list-style-type: none"> <li>Die Datenbanksicherung startet um 11:00 Uhr bzw. 13 Stunden nach dem Start der Clientsicherung. Dieser Prozess wird bis zum Abschluss ausgeführt.</li> <li>Die Sicherung von Einheitenkonfigurationsinformationen und des Datenträgerprotokolls startet um 17:00 Uhr bzw. 6 Stunden nach dem Start der Datenbanksicherung.</li> <li>Das Löschen des Datenträgerprotokolls startet um 20:00 Uhr bzw. 9 Stunden nach dem Start der Datenbanksicherung.</li> </ul> |
| Bestandsverfall  | Startet um 12:00 Uhr bzw. 14 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen. Dieser Prozess wird bis zum Abschluss ausgeführt.  |



## Vorgehensweise

Erstellen Sie nach dem Konfigurieren der Einheitenklasse für die Datenbanksicherungsoperationen Zeitpläne für Datenbanksicherungsoperationen und andere erforderliche Verwaltungsoperationen mithilfe des Befehls DEFINE SCHEDULE. Abhängig von der Größe Ihrer Umgebung müssen Sie die Startzeiten für jeden Zeitplan in dem Beispiel gegebenenfalls anpassen.


1. Definieren Sie eine Einheitenklasse für die Sicherungsoperationen. Erstellen Sie beispielsweise mit dem Befehl DEFINE DEVCLASS eine Einheitenklasse mit dem Namen DBBACK\_FILEDEV:

```
define devclass dback_filedev devtype=file
    directory=Datenbanksicherungsverzeichnisse
```

Dabei ist *Datenbanksicherungsverzeichnisse* eine Liste der für die Datenbanksicherung erstellten Verzeichnisse.

  Wenn beispielsweise vier Verzeichnisse für Datenbanksicherungen mit /tsminst1/TSMbkup00 als Startpunkt vorhanden sind, geben Sie den folgenden Befehl aus:

```
define devclass dback_filedev devtype=file
    directory=/tsminst1/TSMbkup00,
    /tsminst1/TSMbkup01,/tsminst1/TSMbkup02,
    /tsminst1/TSMbkup03"
```

 Wenn beispielsweise vier Verzeichnisse für Datenbanksicherungen mit C:\tsminst1\TSMbkup00 als Startpunkt vorhanden sind, geben Sie den folgenden Befehl aus:

```
define devclass dback_filedev devtype=file
    directory="c:\tsminst1\TSMbkup00,
    c:\tsminst1\TSMbkup01,c:\tsminst1\TSMbkup02,c:\tsminst1\TSMbkup03"
```

2. Legen Sie die Einheitenklasse für automatische Datenbanksicherungsoperationen fest. Geben Sie mit dem Befehl SET DBRECOVERY die im vorhergehenden Schritt erstellte Einheitenklasse an. Wenn beispielsweise die Einheitenklasse den Namen dback\_filedev hat, geben Sie den folgenden Befehl aus:

```
set dbrecovery dback_filedev
```

3. Erstellen Sie mithilfe des Befehls DEFINE SCHEDULE Zeitpläne für die Verwaltungsoperationen. Die folgende Tabelle enthält die erforderlichen Operationen und Beispiele der Befehle.  
Tipp: Der Zeitplan für die Replikation wird separat in einem späteren Schritt erstellt, wenn Sie die Replikation mithilfe des Operations Center konfigurieren.

| Operation             | Beispielbefehl   |
|-----------------------|--|
| Sichern der Datenbank | <p>Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP DB. Wenn Sie ein kleines System konfigurieren, setzen Sie den Parameter COMPRESS auf YES.</p> <p>Geben Sie beispielsweise auf einem kleinen System den folgenden Befehl aus, um einen Sicherungszeitplan zu erstellen, der die neue Einheitenklasse verwendet:</p> <pre>define schedule DBBACKUP type=admin cmd="backup db     devclass=dback_filedev type=full numstreams=3 wait=yes     compress=yes" active=yes desc="Datenbank sichern."     startdate=today starttime=11:00:00 duration=45     durunits=minutes</pre> |




| Operation  | Beispielbefehl  |
|--|---|
| Sichern der Einheitenkonfigurationsinformationen                                       | Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP DEVCONFIG:<br><br><pre>define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig   filenames=devconfig.dat" active=yes desc="Einheitenkonfigurationsdatei sichern." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>   |
| Sichern des Datenträgerprotokolls  | Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP VOLHISTORY:<br><br><pre>define schedule VOLHISTBKUP type=admin cmd="backup volhistory   filenames=volhist.dat" active=yes desc="Datenträgerprotokoll sichern." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>   |
| Entfernen älterer Versionen von Datenbanksicherungen, die nicht mehr erforderlich sind | Erstellen Sie einen Zeitplan für die Ausführung des Befehls DELETE VOLHISTORY:<br><br><pre>define schedule DELVOLHIST type=admin cmd="delete volhistory   type=dbb todate=today-6 totime=now" active=yes desc="Alte Datenbanksicherungen entfernen." startdate=today starttime=20:00:00 duration=45 durunits=minutes</pre>  |
| Entfernen von Objekten, deren zulässige Aufbewahrungsdauer überschritten wurde         | Erstellen Sie einen Zeitplan für die Ausführung des Befehls EXPIRE INVENTORY.<br>Definieren Sie den Parameter RESOURCE auf der Basis der Systemgröße, die Sie konfigurieren: <ul style="list-style-type: none"> <li>o Kleine Systeme: 10</li> <li>o Mittlere Systeme: 30</li> <li>o Große Systeme: 40</li> </ul> Geben Sie beispielsweise auf einem mittelgroßen System den folgenden Befehl aus, um einen Zeitplan mit dem Namen EXPINVENTORY zu erstellen:<br><br><pre>define schedule EXPINVENTORY type=admin cmd="expire inventory   wait=yes resource=30 duration=120" active=yes desc="Verfallene Objekte entfernen." startdate=today starttime=12:00:00 duration=45 durunits=minutes</pre> |

## Nächste Schritte

Nachdem Sie Zeitpläne für die Serververwaltungstasks erstellt haben, können Sie diese im Operations Center anzeigen, indem Sie die folgenden Schritte ausführen:

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Server.
2. Klicken Sie auf Verwaltung.

### Zugehörige Verweise:

 DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)

## Clientzeitpläne definieren

Erstellen Sie mithilfe des Operations Center Zeitpläne für Clientoperationen.

### Vorgehensweise

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Clients.

2. Klicken Sie auf Zeitpläne.
3. Klicken Sie auf +Zeitplan.
4. Führen Sie die Schritte im Assistenten Zeitplan erstellen aus. Definieren Sie auf der Basis der in Zeitpläne für Serververwaltungsaktivitäten geplanten Serververwaltungsaktivitäten für Clientsicherungszeitpläne eine Startzeit von 22:00 Uhr.

## Clients für Sichern/Archivieren installieren und konfigurieren

---

Installieren und konfigurieren Sie im Anschluss an die erfolgreiche Konfiguration Ihres IBM Spectrum Protect-Serversystems die Client-Software, um mit dem Sichern von Daten beginnen zu können.

### Vorgehensweise

---

Um den Client für Sichern/Archivieren zu installieren, führen Sie die Installationsanweisungen für Ihr Betriebssystem aus.

- UNIX- und Linux-Clients für Sichern/Archivieren installieren
- Windows-Client für Sichern/Archivieren installieren

### Nächste Schritte

---

Registrieren Sie Ihre Clients und ordnen Sie Ihre Clients Zeitplänen zu.

- Clients registrieren und Zeitplänen zuordnen  
Sie können Ihre Clients über das Operations Center mithilfe des Assistenten Client hinzufügen hinzufügen und registrieren.
- Clientverwaltungsservice installieren  
Installieren Sie den Clientverwaltungsservice für Clients für Sichern/Archivieren, die unter Linux- und Windows-Betriebssystemen ausgeführt werden. Der Clientverwaltungsservice erfasst Diagnoseinformationen zu Clients für Sichern/Archivieren und stellt die Informationen dem Operations Center für die grundlegende Überwachungsfunktion zur Verfügung.

## Clients registrieren und Zeitplänen zuordnen

---

Sie können Ihre Clients über das Operations Center mithilfe des Assistenten Client hinzufügen hinzufügen und registrieren.

### Vorbereitende Schritte

---

Bestimmen Sie, ob der Client eine Benutzer-ID mit Administratorberechtigung mit Clienteignerberechtigung für den Clientknoten erfordert. Informationen zum Bestimmen der Clients, die eine Benutzer-ID mit Administratorberechtigung erfordern, finden Sie in Technote 7048963.

Einschränkung: Bei einigen Clienttypen müssen der Clientknotenname und die Benutzer-ID mit Administratorberechtigung übereinstimmen. Sie können diese Clients nicht mithilfe der in Version 7.1.7 eingeführten LDAP-Authentifizierungsmethode authentifizieren. Ausführliche Informationen zu dieser Authentifizierungsmethode, die manchmal als integrierter Modus bezeichnet wird, finden Sie in Benutzer mithilfe einer Active Directory-Datenbank authentifizieren.

### Vorgehensweise

---

Um einen Client zu registrieren, führen Sie eine der folgenden Aktionen aus.

- Wenn der Client eine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Befehl REGISTER NODE unter Angabe des Parameters USERID:

```
register node Knotenname Kennwort userid=Knotenname
```

Dabei gibt *Knotenname* den Knotennamen und *Kennwort* das Knotenkennwort an. Ausführliche Informationen finden Sie in Knoten registrieren.

- Wenn der Client keine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Assistenten 'Client hinzufügen' im Operations Center. Führen Sie die folgenden Schritte aus:
  - a. Klicken Sie in der Menüleiste des Operations Center auf Clients.
  - b. Klicken Sie in der Tabelle 'Clients' auf + Client.
  - c. Führen Sie die Schritte im Assistenten Client hinzufügen aus:
    - i. Geben Sie an, dass redundante Daten sowohl auf dem Client als auch auf dem Server gelöscht werden können. Wählen Sie im Bereich 'Clientseitige Dateneduplizierung' das Kontrollkästchen Aktivieren aus.
    - ii. Kopieren Sie im Fenster Konfiguration die Werte für die Optionen TCPSERVERADDRESS, TCPPORT, NODENAME und DEDUPLICATION.

- Tipp: Notieren Sie die Optionswerte und bewahren Sie die Unterlagen an einem sicheren Ort auf. Nachdem Sie die Clientregistrierung abgeschlossen und die Software auf dem Clientknoten installiert haben, verwenden Sie die Werte zum Konfigurieren des Clients.
- iii. Führen Sie die Anweisungen im Assistenten aus, um die Maßnahmendomäne, den Zeitplan und die Optionsgruppe anzugeben.
  - iv. Legen Sie fest, wie Risiken für den Client angezeigt werden, indem Sie die Einstellung für die Gefährdung angeben.
  - v. Klicken Sie auf Client hinzufügen.

## Clientverwaltungsservice installieren

---

Installieren Sie den Clientverwaltungsservice für Clients für Sichern/Archivieren, die unter Linux- und Windows-Betriebssystemen ausgeführt werden. Der Clientverwaltungsservice erfasst Diagnoseinformationen zu Clients für Sichern/Archivieren und stellt die Informationen dem Operations Center für die grundlegende Überwachungsfunktion zur Verfügung.


### Vorgehensweise

---

Installieren Sie den Clientverwaltungsservice auf demselben Computer wie den Client für Sichern/Archivieren, indem Sie die folgenden Schritte ausführen:

1. Laden Sie das Installationspaket für den Clientverwaltungsservice von einer IBM® Download-Site, wie beispielsweise IBM Passport Advantage® oder IBM Fix Central, herunter. Suchen Sie nach einem ähnlichen Dateinamen wie `<Version>-IBM_Spectrum_Protect-CMS-Betriebssystem.bin`.
  2. Erstellen Sie auf dem Clientsystem, das verwaltet werden soll, ein Verzeichnis und kopieren Sie das Installationspaket in dieses Verzeichnis.
  3. Extrahieren Sie den Inhalt der Installationspaketdatei.
  4. Führen Sie die Installationsstapeldatei in dem Verzeichnis aus, in das die Installationsdateien und die zugehörigen Dateien extrahiert wurden. Dabei handelt es sich um das in Schritt 2 erstellte Verzeichnis.
  5. Um den Clientverwaltungsservice zu installieren, führen Sie die Anweisungen im Assistenten von IBM Installation Manager aus. Wenn IBM Installation Manager noch nicht auf dem Clientsystem installiert ist, müssen Sie sowohl IBM Installation Manager als auch die IBM Spectrum Protect-Clientverwaltungsservices auswählen.
- Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen  
Bevor Sie den Clientverwaltungsservice zum Erfassen von Diagnoseinformationen zu einem Client für Sichern/Archivieren verwenden, können Sie überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist.
  - Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren  
Wenn für den Clientverwaltungsservice nicht die Standardkonfiguration verwendet wurde, müssen Sie das Operations Center für den Zugriff auf den Clientverwaltungsservice konfigurieren.

#### Zugehörige Tasks:

-  Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren

## Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen

---

Bevor Sie den Clientverwaltungsservice zum Erfassen von Diagnoseinformationen zu einem Client für Sichern/Archivieren verwenden, können Sie überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist.

### Vorgehensweise

---

Führen Sie auf dem Clientsystem in der Befehlszeile die folgenden Befehle aus, um die Konfiguration des Clientverwaltungsservice anzuzeigen:

- Geben Sie auf Linux-Clientsystemen den folgenden Befehl aus:

```
Clientinstallationsverzeichnis/cms/bin/CmsConfig.sh list
```

Dabei ist *Clientinstallationsverzeichnis* das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist. Geben Sie beispielsweise bei der Standardclientinstallation den folgenden Befehl aus:

```
/opt/tivoli/tsm/cms/bin/CmsConfig.sh list
```

Die Ausgabe sieht ähnlich wie die folgende aus:

```
Listing CMS configuration
```

```
server1.example.com:1500 NO_SSL HOSTNAME  
Capabilities: [LOG_QUERY]
```

```
Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys
Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252
Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

- Geben Sie auf Windows-Clientsystemen den folgenden Befehl aus:

```
Clientinstallationsverzeichnis\cms\bin\CmsConfig.bat list
```

Dabei ist *Clientinstallationsverzeichnis* das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist. Geben Sie beispielsweise bei der Standardclientinstallation den folgenden Befehl aus:

```
C:\"Programme"\Tivoli\TSM\cms\bin\CmsConfig.bat list
```

Die Ausgabe sieht ähnlich wie die folgende aus:

```
Listing CMS configuration
server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
  Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt
  Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252
  Log File: C:\Program Files\Tivoli\TSM\baclient\dsm Sched.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

Wenn der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist, wird in der Ausgabe die Position der Fehlerprotokolldatei angezeigt.

Der Ausgabebetext wird aus der folgenden Konfigurationsdatei extrahiert:

- Auf Linux-Clientsystemen:

```
Clientinstallationsverzeichnis/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
```

- Auf Windows-Clientsystemen:

```
Clientinstallationsverzeichnis\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
```

Wenn die Ausgabe keine Einträge enthält, müssen Sie die Datei *client-configuration.xml* konfigurieren. Anweisungen zum Konfigurieren dieser Datei finden Sie in Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren. Mit dem Befehl *CmsConfig verify* können Sie überprüfen, ob eine Knotendefinition in der Datei *client-configuration.xml* korrekt erstellt wurde.

## Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren

---

Wenn für den Clientverwaltungsservice nicht die Standardkonfiguration verwendet wurde, müssen Sie das Operations Center für den Zugriff auf den Clientverwaltungsservice konfigurieren.

### Vorbereitende Schritte

---

Stellen Sie sicher, dass der Clientverwaltungsservice auf dem Clientsystem installiert und gestartet wurde. Überprüfen Sie, ob die Standardkonfiguration verwendet wird. Die Standardkonfiguration wird nicht verwendet, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Clientverwaltungsservice verwendet nicht die Standardportnummer 9028.
- Der Zugriff auf den Client für Sichern/Archivieren erfolgt nicht über dieselbe IP-Adresse wie für das Clientsystem, auf dem der Client für Sichern/Archivieren installiert ist. Eine andere IP-Adresse kann beispielsweise in den folgenden Situationen verwendet werden:
  - Das Computersystem verfügt über zwei Netzwerke. Der Client für Sichern/Archivieren ist für die Kommunikation in einem Netzwerk konfiguriert, der Clientverwaltungsservice kommuniziert jedoch in dem anderen Netzwerk.
  - Das Clientsystem ist mit DHCP (Dynamic Host Configuration Protocol) konfiguriert. Demzufolge wird dem Clientsystem dynamisch eine IP-Adresse zugeordnet, die während der vorherigen Operation des Clients für Sichern/Archivieren auf dem Server gespeichert wurde. Wenn das Clientsystem erneut gestartet wird, wird ihm möglicherweise eine andere IP-Adresse zugeordnet. Um sicherzustellen, dass das Operations Center das Clientsystem immer finden kann, müssen Sie einen vollständig qualifizierten Domännennamen angeben.

### Vorgehensweise

---

Um das Operations Center für die Verwendung des Clientverwaltungsservice zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie auf der Seite 'Clients' im Operations Center den Client aus.
2. Klicken Sie auf Details > Merkmale.
3. Geben Sie im Feld 'URL für Ferndiagnose' im Abschnitt 'Allgemein' die URL für den Clientverwaltungsservice auf dem Clientsystem an. Die Adresse muss mit `https` beginnen. In der folgenden Tabelle sind Beispiele für die URL für Ferndiagnose aufgeführt.

| Typ der URL  | Beispiel                                     |
|--|--|
| Mit DNS-Hostname und Standardport 9028                       | <code>https://server.example.com</code>      |
| Mit DNS-Hostname und einem anderen Port als dem Standardport | <code>https://server.example.com:1599</code> |
| Mit IP-Adresse und einem anderen Port als dem Standardport   | <code>https://192.0.2.0:1599</code>          |

4. Klicken Sie auf Sichern.

## Nächste Schritte

---

Über die Registerkarte Diagnose im Operations Center können Sie auf Clientdiagnoseinformationen, wie beispielsweise Clientprotokolldateien, zugreifen.

## Zweiten Server konfigurieren

---

Nachdem Sie die Konfiguration für den ersten Server in Ihrem System abgeschlossen haben, konfigurieren Sie den zweiten Server.

### Vorgehensweise

---

Führen Sie die Anweisungen in den folgenden Abschnitten aus:

1. Konfigurieren Sie einen zweiten Server, der mit dem ersten Server identisch ist, indem Sie die Anweisungen in den folgenden Abschnitten ausführen:
  - a. System konfigurieren
  - b. Server und das Operations Center installieren

Da in der Plattenspeicherlösung für mehrere Standorte nur ein einziger Server als Hub-Server konfiguriert ist, müssen Sie das Operations Center nicht auf dem zweiten Server installieren. Wenn Sie die Installationspakete für die Installation auf dem zweiten Server auswählen, wählen Sie nicht das Operations Center aus.

- c. Server und das Operations Center konfigurieren

Überspringen Sie die Tasks zum Konfigurieren des Operations Center.

- d. Clients für Sichern/Archivieren installieren und konfigurieren
2. SSL-Kommunikation zwischen dem Hub-Server und einem Peripherieserver konfigurieren
  3. Zweiten Server als Peripherieserver hinzufügen
  4. Replikation aktivieren

## SSL-Kommunikation zwischen dem Hub-Server und einem Peripherieserver konfigurieren

---

Um die sichere Kommunikation zwischen dem Hub-Server und einem Peripherieserver unter Verwendung des Protokolls Transport Layer Security (TLS) zu ermöglichen, müssen Sie das Zertifikat des Peripherieservers für den Hub-Server definieren.

### Informationen zu diesem Vorgang

---

Der Hub-Server empfängt Status- und Alertinformationen vom Peripherieserver und zeigt diese Informationen im Operations Center an. Um die Status- und Alertinformationen vom Peripherieserver empfangen zu können, muss das Zertifikat des Peripherieservers der Truststore-Datei des Hub-Servers hinzugefügt werden. Außerdem müssen Sie das Operations Center für die Überwachung des Peripherieservers konfigurieren.

Um andere Funktionen des Operations Center, wie beispielsweise die automatische Implementierung von Clientaktualisierungen, aktivieren zu können, muss das Zertifikat des Hub-Servers der Truststore-Datei des Peripherieservers hinzugefügt werden.

### Vorgehensweise

---

1. Führen Sie die folgenden Schritte aus, um das Zertifikat des Peripherieservers für den Hub-Server zu definieren:
  - a. Wechseln Sie auf dem Peripherieserver in das Verzeichnis der Peripherieserverinstanz.
  - b. Geben Sie das erforderliche Zertifikat cert256.arm als Standardzertifikat in der Schlüsseldatenbankdatei des Peripherieservers an. Geben Sie den folgenden Befehl aus:

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
-label "TSM Server SelfSigned SHA Key"
```

- c. Überprüfen Sie die Zertifikate in der Schlüsseldatenbankdatei des Peripherieservers. Geben Sie den folgenden Befehl aus:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

- d. Übertragen Sie die Datei cert256.arm des Peripherieservers sicher auf den Hub-Server.
  - e. Wechseln Sie auf dem Hub-Server in das Verzeichnis der Hub-Server-Instanz.
  - f. Definieren Sie das Zertifikat des Peripherieservers für den Hub-Server. Geben Sie im Verzeichnis der Hub-Server-Instanz den folgenden Befehl aus; dabei ist *Name\_des\_Peripherieservers* der Name des Peripherieservers und *cert256.arm\_für\_Peripherieserver* der Dateiname des Zertifikats des Peripherieservers:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
-label Name_des_Peripherieservers -file cert256.arm_für_Peripherieserver
```

2. Führen Sie die folgenden Schritte aus, um das Zertifikat des Hub-Servers für den Peripherieserver zu definieren:
  - a. Wechseln Sie auf dem Hub-Server in das Verzeichnis der Hub-Server-Instanz.
  - b. Geben Sie das erforderliche Zertifikat cert256.arm als Standardzertifikat in der Schlüsseldatenbankdatei des Hub-Servers an. Geben Sie den folgenden Befehl aus:

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
-label "TSM Server SelfSigned SHA Key"
```

- c. Überprüfen Sie die Zertifikate in der Schlüsseldatenbankdatei des Peripherieservers. Geben Sie den folgenden Befehl aus:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

- d. Übertragen Sie die Datei cert256.arm des Hub-Servers sicher auf den Peripherieserver.
  - e. Wechseln Sie auf dem Peripherieserver in das Verzeichnis der Peripherieserverinstanz.
  - f. Definieren Sie das Zertifikat des Hub-Servers für den Peripherieserver. Geben Sie im Verzeichnis der Peripherieserverinstanz den folgenden Befehl aus; dabei ist *Name\_des\_Hub-Servers* der Name des Hub-Servers und *cert256.arm\_für\_Hub-Server* der Dateiname des Zertifikats des Hub-Servers:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
-label Name_des_Hub-Servers -file cert256.arm_für_Hub-Server
```

3. Starten Sie den Hub-Server und den Peripherieserver erneut.
4. Führen Sie die folgenden Schritte aus, um den Peripherieserver für den Hub-Server und den Hub-Server für den Peripherieserver zu definieren.

- a. Geben Sie die folgenden Befehle sowohl auf dem Hub-Server als auch auf dem Peripherieserver aus:

```
SET SERVERPASSWORD Serverkennwort
SET SERVERHLADDRESS IP-Adresse
SET SERVERLLADDRESS TCP-Port
```

- b. Geben Sie auf dem Hub-Server den Befehl DEFINE SERVER gemäß dem folgenden Beispiel aus:

```
DEFINE SERVER Name_des_Peripherieservers HLA=Adresse_des_Peripherieservers
LLA=spoke_SSLTCPADMINPort SERVERPA=Kennwort_für_Peripherieserver
```

- c. Geben Sie auf dem Peripherieserver den Befehl DEFINE SERVER gemäß dem folgenden Beispiel aus:

```
DEFINE SERVER Name_des_Hub-Servers HLA=Adresse_des_Hub-Servers
LLA=hub_SSLTCPADMINPort SERVERPA=Kennwort_des_Hub-Servers
```

Tipp: Standardmäßig wird die Serverkommunikation verschlüsselt, es sei denn, der Server sendet oder empfängt Objektdaten. Objektdaten werden unter Verwendung von TCP/IP gesendet und empfangen. Wenn die Objektdaten nicht verschlüsselt werden, ist die Serverleistung ähnlich wie bei der Kommunikation über eine TCP/IP-Sitzung und die Sitzung ist sicher. Um die gesamte Kommunikation mit dem angegebenen Server selbst dann zu verschlüsseln, wenn der Server Objektdaten sendet und empfängt, geben Sie den Parameter SSL=YES im Befehl DEFINE SERVER an.

5. Führen Sie die folgenden Schritte aus, um das Operations Center für die Überwachung des Peripherieservers zu konfigurieren:
  - a. Klicken Sie in der Menüleiste des Operations Center auf Server. Der Peripherieserver hat den Status 'Nicht überwacht'. Dieser Status bedeutet, dass - obwohl dieser Server für den Hub-Server mit dem Befehl DEFINE SERVER definiert wurde - der Server noch nicht als Peripherieserver konfiguriert ist.
  - b. Klicken Sie auf den Peripherieserver, um den Eintrag hervorzuheben, und klicken Sie auf Peripherieserver überwachen.

#### Zugehörige Verweise:

- ➔ DEFINE SERVER (Server für Übertragung zwischen Servern definieren)
- ➔ QUERY OPTION (Serveroptionen abfragen)

## Zweiten Server als Peripherieserver hinzufügen

---

Nachdem Sie beide Server in Ihrer Umgebung konfiguriert haben, fügen Sie den zweiten Server dem Hub-Server als Peripherieserver hinzu.

### Vorgehensweise

---

1. Öffnen Sie das Operations Center.
2. Klicken Sie in der Menüleiste des Operations Center auf Server.
3. Führen Sie einen der folgenden Schritte aus:
  - Klicken Sie auf den Server, um ihn hervorzuheben, und klicken Sie in der Menüleiste der Tabelle auf Peripherieserver überwachen.
  - Wenn der Server, der hinzugefügt werden soll, in der Tabelle nicht angezeigt wird, klicken Sie auf +Peripherieserver.
4. Führen Sie die Schritte im Konfigurationsassistenten für den Peripherieserver aus.

## Replikation aktivieren

---

Aktivieren Sie, um Ihre Daten zu schützen, die Knotenreplikation zusätzlich zum Schutz Ihrer Speicherpools.

### Vorgehensweise

---

Um die Knotenreplikation für alle Clients zu aktivieren, die auf dem Quellenserver registriert sind, führen Sie die folgenden Schritte aus:

1. Öffnen Sie das Operations Center.
2. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Speicher und klicken Sie auf Replikation.
3. Klicken Sie auf der Seite Replikation auf +Serverpaar.
4. Führen Sie die Schritte im Assistenten Serverpaar hinzufügen aus:
  - Legen Sie den Quellenserver als den ersten Server fest, der für die Plattenspeicherlösung für mehrere Standorte konfiguriert wurde. Der Zielserver ist der zweite Server.
  - Definieren Sie auf der Basis der in Zeitpläne für Serververwaltungsaktivitäten definieren geplanten Serververwaltungsaktivitäten für den Knotenreplikationszeitplan eine Startzeit von 10 Stunden nach dem Fenster zum Durchführen von Clientsicherungen.
  - Der Assistent definiert auf der Basis des Datenvolumens, das geschützt wird, und auf der Basis des geplanten Zeitpunkts der Clientreplikation Speicherpoolschutzzeitpläne für Sie.

### Nächste Schritte

---

Wenn Sie planen, die gegenseitige Replikation zwischen zwei Standorten zu definieren, führen Sie den Assistenten Serverpaar hinzufügen erneut aus, und legen Sie den zweiten Server als Quellenserver und den ersten Server als Zielserver fest.

## Implementierung abschließen

---

Nachdem die IBM Spectrum Protect- Lösung konfiguriert wurde und aktiv ist, testen Sie Sicherungsoperationen und konfigurieren Sie die Überwachung, um sicherzustellen, dass alles ordnungsgemäß funktioniert.

### Vorgehensweise

---

1. Testen Sie Sicherungsoperationen, um sicherzustellen, dass Ihre Daten wie erwartet geschützt werden.
  - a. Wählen Sie auf der Seite Clients im Operations Center die Clients aus, die gesichert werden sollen, und klicken Sie auf Sichern.
  - b. Wählen Sie auf der Seite Server im Operations Center den Server aus, dessen Datenbank gesichert werden soll. Klicken Sie auf Sichern und führen Sie die Anweisungen im Fenster Datenbank sichern aus.
  - c. Überprüfen Sie, ob die Sicherungsoperationen erfolgreich ohne Warnungen oder Fehlermeldungen ausgeführt wurden.  
Tipp: Sie können auch stattdessen die GUI des Clients für Sichern/Archivieren zum Sichern von Clientdaten verwenden und die Serverdatenbank sichern, indem Sie den Befehl BACKUP DB in einer Verwaltungsbefehlszeile ausgeben.
2. Konfigurieren Sie die Überwachung für Ihre Lösung, indem Sie die Anweisungen in Plattenspeicherlösung für mehrere Standorte überwachen ausführen.

## Plattenspeicherlösung für mehrere Standorte überwachen

---

Überwachen Sie nach der Implementierung einer Plattenspeicherlösung für mehrere Standorte mit IBM Spectrum Protect die Lösung, um ihre korrekte Funktionsweise sicherzustellen. Indem die Lösung täglich und regelmäßig überwacht wird, können Sie bestehende und potenzielle Probleme erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden.

### Informationen zu diesem Vorgang

---

Die Überwachung einer Lösung erfolgt bevorzugt über die Verwendung des Operations Center, das den Gesamtsystemstatus und den detaillierten Systemstatus in einer grafischen Benutzerschnittstelle bereitstellt. Darüber hinaus können Sie das Operations Center zum Generieren eines täglichen E-Mail-Berichts mit einer Zusammenfassung des Systemstatus konfigurieren.

In einigen Fällen möchten Sie vielleicht erweiterte Überwachungstools verwenden, um bestimmte Überwachungs- oder Fehlerbehebungstasks auszuführen.

Tipp: Wenn Sie planen, Probleme bei Clients für Sichern/Archivieren unter Linux- oder Windows-Betriebssystemen zu diagnostizieren, installieren Sie IBM Spectrum Protect-Clientverwaltungsservices auf jedem Computer, auf dem ein Client für Sichern/Archivieren installiert ist. Auf diese Art und Weise können Sie sicherstellen, dass die Schaltfläche Diagnose im Operations Center zur Diagnose von Problemen bei Clients für Sichern/Archivieren verfügbar ist. Um den Clientverwaltungsservice zu installieren, führen Sie die Anweisungen in Clientverwaltungsservice installieren aus.

### Vorgehensweise

---

1. Führen Sie tägliche Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für tägliche Überwachungstasks.
2. Führen Sie regelmäßige Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für regelmäßige Überwachungstasks.
3. Um zu überprüfen, ob Ihre IBM Spectrum Protect-Lösung die Lizenzierungsanforderungen erfüllt, führen Sie die Anweisungen in Lizenzierung überprüfen aus.
4. Informationen zur Konfiguration des Operations Center zum Erstellen von E-Mail-Statusberichten finden Sie in Systemstatus mithilfe von E-Mail-Berichten verfolgen.

### Nächste Schritte

---

Beheben Sie alle erkannten Probleme. Wenn ein Problem durch Ändern der Konfiguration Ihrer Lösung behoben werden soll, führen Sie die Anweisungen in Operationen für eine Plattenspeicherlösung für mehrere Standorte verwalten aus. Die folgenden Ressourcen sind ebenfalls verfügbar:

- Informationen zur Behebung von Leistungsproblemen finden Sie in Leistung.
- Informationen zur Behebung anderer Typen von Problemen finden Sie in Fehlerbehebung.

## Prüfliste für tägliche Überwachungstasks

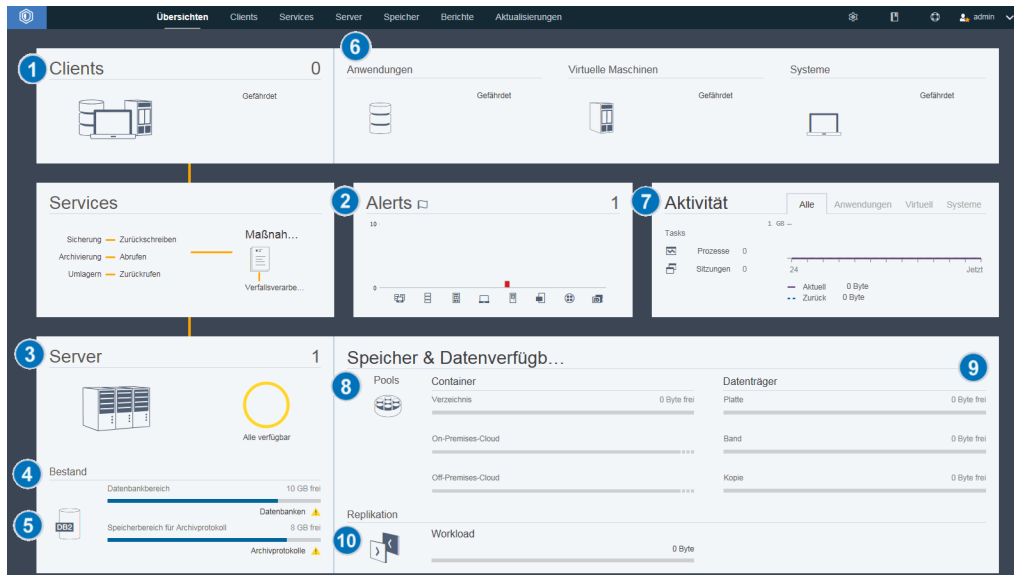
---


Um sicherzustellen, dass die täglichen Überwachungstasks für Ihre IBM Spectrum Protect-Lösung ausgeführt werden, überprüfen Sie die Prüfliste für tägliche Überwachungstasks.

Führen Sie die täglichen Überwachungstasks über die Seite Übersicht im Operations Center aus. Sie können auf die Seite Übersicht zugreifen, indem Sie das Operations Center öffnen und auf Übersichten klicken.

Die folgende Abbildung zeigt die Position zur Ausführung der jeweiligen Task.










Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen  und klicken Sie auf Command Builder.


In der folgenden Tabelle sind die täglichen Überwachungstasks sowie Anweisungen zur Ausführung jeder Task aufgeführt.

Tabelle 1. Tägliche Überwachungstasks



| Task   | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|--|--|--|
| <p><b>1</b> Bestimmen Sie, ob Clients vorhanden sind, bei denen die Gefahr besteht, dass sie aufgrund fehlgeschlagener oder versäumter Sicherungsoperationen ungeschützt sind.</p> | <p>Um zu überprüfen, ob Clients gefährdet sind, suchen Sie nach einem Hinweis Gefährdet. Um Details anzuzeigen, klicken Sie auf den Bereich 'Clients'.</p> <p>Achtung: Wenn der Prozentsatz für Gefährdet sehr viel höher als üblicherweise ist, kann dies eine Ransomware-Attacke anzeigen. Eine Ransomware-Attacke kann das Fehlschlagen von Sicherungsoperationen zur Folge haben und somit Clients in den Status 'Gefährdet' versetzen. Wenn beispielsweise der Prozentsatz gefährdeter Clients normalerweise zwischen 5 % und 10 % liegt, sich aber auf 40 % oder 50 % erhöht, ermitteln Sie die Ursache.</p> <p>Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie die Clientfehler- und -planungsprotokolle anzeigen, indem Sie die folgenden Schritte ausführen:</p> <ol style="list-style-type: none"> <li>1. Wählen Sie in der Tabelle 'Clients' den Client aus und klicken Sie auf Details.</li> <li>2. Um ein Problem zu diagnostizieren, klicken Sie auf Diagnose.</li> </ol> | <p>Greifen Sie bei Clients, für die der Clientverwaltungsservice nicht installiert ist, auf das Clientverwaltungssystem zu, um die Clientfehlerprotokolle zu überprüfen.</p> |



| Task   | Basisprozeduren   | Erweiterte Prozeduren und Fehlerbehebungsinformationen  |
|--|---|---|
| <p><b>2</b> Bestimmen Sie, ob clientbezogene oder serverbezogene Fehler einen Bedieneringriff erfordern.</p>                                       | <p>Um die Bewertung jedes zurückgemeldeten Alerts zu bestimmen, bewegen Sie den Mauszeiger im Bereich 'Alerts' über die Spalten.</p>  | <p>Um zusätzliche Informationen zu Alerts anzuzeigen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf den Bereich 'Alerts'.</li> <li>2. Wählen Sie in der Tabelle 'Alerts' einen Alert aus.</li> <li>3. Überprüfen Sie die Nachrichten im Fenster 'Aktivitätenprotokoll'. In dem Fenster werden zugehörige Nachrichten angezeigt, die vor und nach dem Auftreten des ausgewählten Alerts ausgegeben wurden.</li> </ol> |
| <p><b>3</b> Bestimmen Sie, ob die vom Operations Center verwalteten Server verfügbar sind, um Datenschutzservices für Clients bereitzustellen.</p> | <ol style="list-style-type: none"> <li>1. Um zu überprüfen, ob Server gefährdet sind, suchen Sie im Bereich 'Server' nach einem Hinweis Nicht verfügbar.</li> <li>2. Um zusätzliche Informationen anzuzeigen, klicken Sie auf den Bereich 'Server'.</li> <li>3. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details.</li> </ol> | <p> Tipp: Wenn Sie ein Problem erkennen, das sich auf die Servermerkmale bezieht, aktualisieren Sie die Servermerkmale:</p> <ol style="list-style-type: none"> <li>1. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details.</li> <li>2. Um die Servermerkmale zu aktualisieren, klicken Sie auf Merkmale.</li> </ol>   |


| Task   | Basisprozeduren   | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|--|---|--|
| <p>4 Bestimmen Sie, ob für den Serverbestand, der aus der Serverdatenbank, der aktiven Protokolldatei und dem Archivprotokoll besteht, genügend Speicherbereich verfügbar ist.</p> | <ol style="list-style-type: none"> <li>1. Klicken Sie auf den Bereich 'Server'.</li> <li>2. Zeigen Sie in der Spalte 'Status' der Tabelle den Status des Servers an und beheben Sie alle Probleme: <ul style="list-style-type: none"> <li>o Normal  Für die Serverdatenbank, die aktive Protokolldatei und das Archivprotokoll ist genügend Speicherbereich verfügbar.</li> <li>o Kritisch  Für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll ist nicht genügend Speicherbereich verfügbar. Sie müssen unverzüglich Speicherbereich hinzufügen; andernfalls werden die vom Server bereitgestellten Datenschutzservices unterbrochen.</li> <li>o Warnung  Der Speicherbereich für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll wird knapp. Wenn diese Bedingung bestehen bleibt, müssen Sie Speicherbereich hinzufügen.</li> <li>o Nicht verfügbar  Der Status kann nicht abgerufen werden. Stellen Sie sicher, dass der Server aktiv ist und keine Netzprobleme vorliegen. Dieser Status wird auch angezeigt, wenn die Überwachungsadministrator-ID gesperrt ist oder aus anderen Gründen auf dem Server nicht verfügbar ist. Diese ID hat den Namen IBM-OC-Name_des_Hub-Servers.</li> <li>o Nicht überwacht  Nicht überwachte Server sind für den Hub-Server definiert, aber nicht für die Verwaltung durch das Operations Center konfiguriert. Um einen nicht überwachten Server zu konfigurieren, wählen Sie den Server aus und klicken Sie auf Peripherieserver überwachen.</li> </ul> </li> </ol> | <p>Sie können auch auf der Seite Alerts nach zugehörigen Alerts suchen. Weitere Anweisungen zur Fehlerbehebung finden Sie in Serverprobleme beheben.</p> |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|---|--|--|
| <p><b>5</b> Überprüfen Sie Operationen zur Sicherung der Serverdatenbank.</p>   | <p>Um zu bestimmen, ob ein Server kürzlich gesichert wurde, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf den Bereich 'Server'.</li> <li>2. Überprüfen Sie in der Tabelle 'Server' die Spalte 'Letzte Datenbanksicherung'.</li> </ol>   | <p>Um detaillierte Informationen zu Sicherungsoperationen abzurufen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Wählen Sie in der Tabelle 'Server' eine Zeile aus und klicken Sie auf Details.</li> <li>2. Bewegen Sie im Bereich 'Datenbanksicherung' den Mauszeiger über die Häkchen, um Informationen zu Sicherungsoperation zu überprüfen.</li> </ol> <p>Wenn eine Datenbank nicht kürzlich (beispielsweise innerhalb der letzten 24 Stunden) gesichert wurde, können Sie eine Sicherungsoperation starten:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Server'.</li> <li>2. Wählen Sie in der Tabelle einen Server aus und klicken Sie auf Sichern.</li> </ol> <p>Um zu bestimmen, ob die Serverdatenbank für automatische Sicherungsoperationen konfiguriert ist, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>2. Geben Sie den Befehl QUERY DB aus: <pre>query db f=d</pre> </li> <li>3. Überprüfen Sie in der Ausgabe das Feld Einheitenklassenname für Gesamtsicherungen. Wenn eine Einheitenklasse angegeben ist, ist der Server für automatische Datenbanksicherungen konfiguriert.</li> </ol> |
| <p><b>6</b> Überwachen Sie andere Serververwaltungstasks. Serververwaltungstasks können die Ausführung von Zeitplänen für Verwaltungsbefehle, Verwaltungsscripts und zugehörigen Befehlen umfassen.</p> | <p>Um nach Informationen zu Prozessen zu suchen, die aufgrund von Serverproblemen fehlgeschlagen sind, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf Server &gt; Verwaltung.</li> <li>2. Um das zwei Wochen umfassende Verlaufsprotokoll eines Prozesses abzurufen, zeigen Sie Spalte 'History' an.</li> <li>3. Um weitere Informationen zu einem geplanten Prozess abzurufen, bewegen Sie den Mauszeiger über das Kontrollkästchen, das dem Prozess zugeordnet ist.</li> </ol> | <p>Weitere Informationen zum Überwachen von Prozessen und Beheben von Problemen, finden Sie in der Onlinehilfe des Operations Center.</p>  |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|---|--|--|
| <p><b>7</b> Überprüfen Sie, ob das Datenvolumen, das kürzlich an Server bzw. von Servern gesendet wurde, innerhalb des erwarteten Bereichs liegt.</p> | <ul style="list-style-type: none"> <li>• Um eine Übersicht über die Aktivität der letzten 24 Stunden abzurufen, zeigen Sie den Bereich 'Aktivität' an.</li> <li>• Um die Aktivität der letzten 24 Stunden mit der Aktivität der vorherigen 24 Stunden zu vergleichen, studieren Sie die Zahlen in den Bereichen 'Aktuell' und 'Vorherig'.</li> </ul> | <ul style="list-style-type: none"> <li>• Wenn mehr Daten als erwartet an den Server gesendet wurden, bestimmen Sie die Clients, die mehr Daten sichern und ermitteln Sie die Ursache. Möglicherweise funktioniert die clientseitige Datenduplizierung nicht ordnungsgemäß.<br/>Achtung: Wenn das Volumen gesicherter Daten deutlich umfangreicher als üblicherweise ist, kann dies eine Ransomware-Attacke anzeigen. Wenn Daten durch Ransomware verschlüsselt werden, werden die Daten vom System als geändert wahrgenommen und die geänderten Daten werden gesichert. Demzufolge wird das Volumen gesicherter Daten umfangreicher. Um die betroffenen Clients zu bestimmen, klicken Sie auf die Registerkarten Anwendungen, Virtuell oder Systeme.</li> <li>• Wenn weniger Daten als erwartet an den Server gesendet wurden, überprüfen Sie, ob Clientsicherungsoperationen gemäß Zeitplan ausgeführt werden.</li> </ul> |

| Task   | Basisprozeduren   | Erweiterte Prozeduren und Fehlerbehebungsinformationen  |
|--|---|---|
| <p><b>8</b> Stellen Sie sicher, dass Speicherpools zum Sichern von Clientdaten verfügbar sind.</p> | <p>1. Wenn im Bereich 'Speicher &amp; Datenverfügbarkeit' Probleme angezeigt werden, klicken Sie auf Pools, um die Details anzuzeigen:</p> <ul style="list-style-type: none"> <li>○ Wenn der Status Kritisch  angezeigt wird, ist in dem Speicherpool nicht genügend Speicherbereich verfügbar oder der Speicherpool hat den Zugriffsstatus UNAVAILABLE (Nicht verfügbar).<br/>Achtung: Wenn der Status kritisch ist, ermitteln Sie die Ursache: <ul style="list-style-type: none"> <li>■ Wenn die Dateneduplizierungsrate für einen Speicherpool deutlich fällt, kann dies eine Ransomware-Attacke anzeigen. Während einer Ransomware-Attacke werden Daten verschlüsselt und können nicht dedupliziert werden. Um die Dateneduplizierungsrate zu verifizieren, überprüfen Sie in der Tabelle 'Speicherpools' den Wert in der Spalte 'Einsparungen in %'.</li> <li>■ Wenn ein Speicherpool wider Erwarten zu 100 % ausgelastet ist, kann dies eine Ransomware-Attacke anzeigen. Um die Auslastung zu verifizieren, überprüfen Sie den Wert in der Spalte 'Verwendete Kapazität'.<br/>Bewegen Sie den Mauszeiger über die Werte, um den Prozentsatz für den verwendeten Speicherbereich und den Prozentsatz für den freien Speicherbereich anzuzeigen.</li> </ul> </li> <li>○ Wenn der Status Warnung  angezeigt wird, wird der Speicherbereich für den Speicherpool knapp oder der Speicherpool hat den Zugriffsstatus READONLY (Lesezugriff).</li> </ul> <p>2. Um den verwendeten Speicherbereich, den freien Speicherbereich und den Gesamtspeicherbereich für Ihren ausgewählten Speicherpool anzuzeigen, bewegen Sie den Mauszeiger über die Einträge in der Spalte 'Verwendete Kapazität'.</p> | <p>Um die Speicherpoolkapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie eine Zeile in der Tabelle 'Speicherpools' aus und klicken Sie auf Details.</p> |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|---|--|--|
| <p>9 Stellen Sie sicher, dass Speichereinheiten für Sicherungsoperationen verfügbar sind.</p> | <p>Überprüfen Sie im Bereich 'Speicher &amp; Datenverfügbarkeit' im Abschnitt 'Datenträger' unterhalb der Balken für die Kapazität den Status, der neben Einheiten angegeben ist. Wenn der Status Kritisch  oder Warnung  für eine Einheit angezeigt wird, müssen Sie das Problem untersuchen. Um Details anzuzeigen, klicken Sie auf Einheiten.</p> | <p>Platteneinheiten können aus den folgenden Gründen den Status 'Kritisch' oder 'Warnung' haben:</p> <ul style="list-style-type: none"> <li>• Für Einheitenklassen DISK können Datenträger offline sein oder den Zugriffsstatus READONLY (Lesezugriff) haben. In der Spalte 'Plattenspeicher' der Tabelle 'Platteneinheiten' wird der Status der Datenträger angezeigt.</li> <li>• Für nicht gemeinsam genutzte Einheitenklassen FILE können Verzeichnisse offline sein. Außerdem ist unter Umständen nicht genügend freier Speicherbereich für die Zuordnung von Arbeitsdatenträgern verfügbar. In der Spalte 'Plattenspeicher' der Tabelle 'Platteneinheiten' wird der Status der Verzeichnisse angezeigt.</li> <li>• Für gemeinsam genutzte Einheitenklassen FILE sind Laufwerke unter Umständen nicht verfügbar. Ein Laufwerk ist nicht verfügbar, wenn es offline ist, während der Antwort an den Server gestoppt wurde oder sein Pfad offline ist. In anderen Spalten der Tabelle 'Platteneinheiten' wird der Status der Laufwerke und Pfade angezeigt.</li> </ul> |

| Task   | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|--|--|--|
| <p>10 Überwachen Sie Knotenreplikationsprozesse.</p> | <ol style="list-style-type: none"> <li>Um den Gesamtstatus der Knotenreplikationsprozesse abzurufen, zeigen Sie den Bereich 'Replikation' auf der Seite Übersicht im Operations Center an.</li> <li>Um Informationen zu jedem replizierten Serverpaar anzuzeigen, klicken Sie auf den Bereich 'Replikation'.<br/>Achtung: Wenn Sie eine nicht erwartete Erhöhung der Anzahl Replikationsfehler beobachten, kann dies eine Ransomware-Attacke anzeigen. Ermitteln Sie die Fehlerursache.</li> <li>Um das Datenvolumen, das im Laufe der letzten zwei Wochen repliziert wurde, und die Geschwindigkeit der Replikation anzuzeigen, wählen Sie ein Serverpaar aus und klicken Sie auf Details.</li> <li>Um Replikationsinformationen für einen Client anzuzeigen, klicken Sie auf der Seite Übersicht im Operations Center auf Clients. Studieren Sie die Informationen in der Spalte 'Replikationsworkload'.<br/>Achtung: Wenn Sie eine drastische, nicht erwartete Erhöhung der Replikationslast beobachten, kann dies eine Ransomware-Attacke anzeigen. Ermitteln Sie die Ursache für die erhöhte Last.</li> </ol> | <p>Zeigen Sie für die erweiterte Überwachung mithilfe von Befehlen Informationen zu aktiven und beendeten Knotenreplikationsprozessen an:</p> <ol style="list-style-type: none"> <li>Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>Geben Sie den Befehl QUERY REPLICATION aus. Anweisungen finden Sie in QUERY REPLICATION (Knotenreplikationsprozesse abfragen). Wenn die Replikationsoperation erfolgreich ausgeführt wurde, stimmt der Wert für Gesamtzahl der zu replizierenden Dateien mit dem Wert für Gesamtzahl der replizierten Dateien überein.</li> </ol> <p>Um Nachrichten anzuzeigen, die sich auf einen Knotenreplikationsprozess auf einem Quellen- oder Zielreplikationsserver beziehen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>Klicken Sie auf der Seite Übersicht im Operations Center auf Server.</li> <li>Wählen Sie den Quellen- oder Zielreplikationsserver aus und klicken Sie auf Details: <ul style="list-style-type: none"> <li>Um aktive Tasks anzuzeigen, klicken Sie auf Aktive Tasks, wählen die Task aus und überprüfen, ob der Status Aktiv angezeigt wird. Ausführliche Informationen enthalten die zugehörigen Aktivitätenprotokolle.</li> <li>Um abgeschlossene Tasks anzuzeigen, klicken Sie auf Abgeschlossene Tasks, wählen die Task aus und überprüfen, ob der Status Abgeschlossen angezeigt wird. Ausführliche Informationen enthalten die zugehörigen Aktivitätenprotokolle.</li> </ul> </li> </ol> |

## Prüfliste für regelmäßige Überwachungstasks

Um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert, führen Sie die Tasks in der Prüfliste für regelmäßige Überwachungstasks aus. Planen Sie regelmäßige Tasks häufig genug, sodass Sie potenzielle Probleme erkennen können, bevor diese wirklich problematisch werden.




Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen  und klicken Sie auf Command Builder.







Tabelle 1. Regelmäßige Überwachungstasks

| Task | Basisprozeduren | Erweiterte Prozeduren und Fehlerbehebung |
|------|-----------------|--|
|------|-----------------|--|




| Task                                      | Basisprozeduren   | Erweiterte Prozeduren und Fehlerbehebung  |
|---|---|---|
| <p>Überwachen Sie die Systemleistung.</p> | <p>Bestimmen Sie den für Clientsicherungsoperationen erforderlichen Zeitraum:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients. Suchen Sie den Server, der dem Client zugeordnet ist.</li> <li>2. Klicken Sie auf Server. Wählen Sie den Server aus und klicken Sie auf Details.</li> <li>3. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die in den letzten 24 Stunden abgeschlossen wurden, klicken Sie auf Abgeschlossene Tasks.</li> <li>4. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die vor mehr als 24 Stunden abgeschlossen wurden, verwenden Sie den Befehl QUERY ACTLOG. Führen Sie die Anweisungen in QUERY ACTLOG (Aktivitätenprotokoll abfragen) aus.</li> <li>5. Wenn die Dauer von Clientsicherungsoperationen zunimmt, ohne dass ein offensichtlicher Grund erkennbar ist, überprüfen Sie Ursache.</li> </ol> <p>Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie Leistungsprobleme für den Client für Sichern/Archivieren diagnostizieren, indem Sie die folgenden Schritte ausführen:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients.</li> <li>2. Wählen Sie einen Client für Sichern/Archivieren aus und klicken Sie auf Details.</li> <li>3. Um Clientprotokolle abzurufen, klicken Sie auf Diagnose.</li> </ol> | <p>Informationen zur Verkürzung der Zeit, die der Client zum Sichern von Daten auf dem Server benötigt, finden Sie in Häufig auftretende Clientleistungsprobleme lösen.</p> <p>Suchen Sie nach Leistungsengpässen. Anweisungen finden Sie in Leistungsengpässe identifizieren.</p> <p>Informationen zur Identifikation und Behebung anderer Leistungsprobleme finden Sie in Leistung.</p> |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung   |
|---|--|--|
| <p>Bestimmen Sie die Platteneinsparungen, die durch die Datendeduplizierung bereitgestellt werden.</p>                                  | <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf Pools.</li> <li>2. Wählen Sie einen Pool aus und klicken Sie auf Kurzübersicht.</li> <li>3. Zeigen Sie im Bereich 'Datendeduplizierung' die Zeile 'Eingesparter Speicherbereich' an.</li> </ol>   | <p>Um für die erweiterte Überwachung detaillierte Statistikdaten zu dem Datendeduplizierungsprozess für einen bestimmten Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool abzurufen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>2. Fordern Sie einen Statistikbericht an, indem Sie den Befehl GENERATE DEDUPSTATS ausgeben. Führen Sie die Anweisungen in GENERATE DEDUPSTATS (Datendeduplizierungsstatistikdaten für einen Verzeichniscontainerspeicherpool generieren) aus.</li> <li>3. Zeigen Sie den Statistikbericht an, indem Sie den Befehl QUERY DEDUPSTATS ausgeben. Führen Sie die Anweisungen in QUERY DEDUPSTATS (Datendeduplizierungsstatistikdaten abfragen) aus.</li> </ol> |
| <p>Stellen Sie sicher, dass aktuelle Sicherungsdateien für Einheitenkonfigurations- und Datenträgerprotokolldaten gesichert werden.</p> | <p>Greifen Sie auf Ihre Speicherpositionen zu, um sicherzustellen, dass die Dateien verfügbar sind. Die bevorzugte Methode ist die Sicherung der Dateien an zwei Positionen.</p> <p>Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>2. Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, geben Sie die folgenden Befehle aus: <pre>query option volhistory query option devconfig</pre> </li> <li>3. Überprüfen Sie in der Ausgabe die Spalte 'Optionseinstellung', um die Dateipositionen zu finden.</li> </ol> <p>Wenn ein Katastrophenfall eintritt, sind sowohl die Protokolldatei für Datenträger als auch die Einheitenkonfigurationsdatei für die Zurückschreibung der Serverdatenbank erforderlich.</p> |  |




| Task   | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung |
|--|--|--|
| <p>Bestimmen Sie, ob für das Instanzverzeichnisdateisystem genügend Speicherbereich verfügbar ist.</p> | <p>Stellen Sie sicher, dass im Instanzverzeichnisdateisystem mindestens 20 % freier Speicherbereich verfügbar ist. Führen Sie die für Ihr Betriebssystem zutreffende Aktion aus:</p> <ul style="list-style-type: none"> <li>•  <b>AIX-Betriebssysteme</b> Um den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus: <pre>df -g Instanzverzeichnis</pre> <p>Dabei gibt <i>Instanzverzeichnis</i> das Instanzverzeichnis an.</p> </li> <li>•  <b>Linux-Betriebssysteme</b> Um den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus: <pre>df -h Instanzverzeichnis</pre> <p>Dabei gibt <i>Instanzverzeichnis</i> das Instanzverzeichnis an.</p> </li> <li>•  <b>Windows-Betriebssysteme</b> Klicken Sie in Windows-Explorer mit der rechten Maustaste auf das Dateisystem und klicken Sie auf Eigenschaften. Zeigen Sie die Kapazitätsdaten an.</li> </ul> <p>Die bevorzugte Position des Instanzverzeichnisses ist von dem Betriebssystem abhängig, unter dem der Server installiert ist:</p> <ul style="list-style-type: none"> <li>•  <b>AIX-Betriebssysteme</b></li> <li>•  <b>Linux-Betriebssysteme</b><br/>/home/tsminst1/tsminst1</li> <li>•  <b>Windows-Betriebssysteme</b><br/>C:\tsminst1</li> </ul> <p>Tipp: Wenn Sie ein Arbeitsblatt zur Planung ausgefüllt haben, ist die Position des Instanzverzeichnisses im Arbeitsblatt vermerkt.</p> |  |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung  |
|---|--|---|
| <p>Ermitteln Sie nicht erwartete Clientaktivität.</p> | <p>Um im Rahmen der Überwachung der Clientaktivität zu bestimmen, ob das Datenvolumen das erwartete Volumen überschreitet, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Clients'.</li> <li>2. Um die Aktivität der vergangen zwei Wochen anzuzeigen, doppelklicken Sie auf einen beliebigen Client.</li> <li>3. Um die Anzahl Byte anzuzeigen, die an den Client gesendet wurden, klicken Sie auf die Registerkarte Merkmale.</li> <li>4. Zeigen Sie im Bereich 'Letzte Sitzung' die Zeile 'An Client gesendet' an.</li> </ol> | <p>Wenn Sie auf einen Client in der Tabelle 'Clients' doppelklicken, wird im Bereich Aktivität im Lauf von 2 Wochen das Datenvolumen angezeigt, das vom Client jeden Tag an den Server gesendet wurde.</p> <p>Überprüfen Sie in regelmäßigen Abständen die SQL-Aktivitätsübersichtstabelle, die statistische Daten zu Clientsitzungen enthält. Um die aktuelle Aktivität mit der vorherigen Aktivität zu vergleichen, verwenden Sie eine Anweisung SQL SELECT. Wenn der Grad an Aktivität sich deutlich von dem für die vorherige Aktivität unterscheidet, kann dies eine Ransomware-Attacke anzeigen.</p> <p>Überprüfen Sie das Aktivitätenprotokoll in regelmäßigen Abständen. Suchen Sie nach ANE-Nachrichten, die angeben, wie viele Dateien gesichert und überprüft wurden. Vergleichen Sie die aktuellen Dateneduplizierungsraten mit den vorherigen Raten. Wenn eine ungewöhnlich hohe Anzahl Dateien gesichert wurde oder die Dateneduplizierungsrate wider Erwarten auf 0 fällt, kann dies eine Ransomware-Attacke anzeigen.</p> |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung  |
|---|--|---|
| <p>Überwachen Sie das Speicherpoolwachstum im Laufe der Zeit.</p> | <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Pools'.</li> <li>2. Um die Kapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie einen Pool aus und klicken Sie auf Details.</li> </ol> | <p>Tipps:</p> <ul style="list-style-type: none"> <li>• Um die Zeit anzugeben, die verstreichen muss, bevor alle deduplizierten Speicherbereiche aus einem Verzeichniscontainerspeicherpool oder einem Cloud-Containerspeicherpool entfernt werden, nachdem sie nicht mehr vom Bestand referenziert werden, führen Sie die folgenden Schritte aus: <ol style="list-style-type: none"> <li>1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus.</li> <li>2. Klicken Sie auf Details &gt; Merkmale.</li> <li>3. Geben Sie im Feld <code>Verzögerungszeitraum für Containerwiederverwendung</code> den Zeitraum an.</li> </ol> </li> <li>• Bestimmen Sie die Dateneduplizierungsleistung für Verzeichniscontainer- und Cloud-Containerspeicherpools mithilfe des Befehls <code>GENERATE DEDUPSTATS</code>.</li> <li>• Um Deduplizierungsstatistikdaten für einen Speicherpool anzuzeigen, führen Sie die folgenden Schritte aus: <ol style="list-style-type: none"> <li>1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus.</li> <li>2. Klicken Sie auf Details &gt; Merkmale.</li> </ol> </li> </ul> <p>Verwenden Sie dementsprechend den Befehl <code>QUERY EXTENTUPDATES</code>, um Informationen zu Aktualisierungen an Datenbereichen in Verzeichniscontainer- oder Cloud-Containerspeicherpools anzuzeigen. Anhand der Befehlsausgabe können Sie die Datenbereiche bestimmen, die nicht mehr referenziert werden, sowie die Datenbereiche, die zum Löschen vom System auswählbar sind. Überwachen Sie in der Ausgabe die Anzahl Datenbereiche, die zum Löschen vom System auswählbar sind. Diese Messgröße steht in direkten Zusammenhang mit dem Umfang des freien Speicherbereichs in dem Containerspeicherpool.</p> <ul style="list-style-type: none"> <li>• Um den Umfang des physischen Speicherbereichs anzuzeigen, der von einem Dateibereich nach dem Entfernen der Dateneduplizierungseinsparungen belegt wird, verwenden Sie den Befehl <code>select * from occupancy</code>. Die Befehlsausgabe umfasst den Wert für <code>LOGICAL_MB</code>. <code>LOGICAL_MB</code> gibt an, wie viel Speicherbereich von diesem Dateibereich belegt wird.</li> </ul> |

| Task   | Basisprozeduren   | Erweiterte Prozeduren und Fehlerbehebung   |
|--|---|--|
| Werten Sie das Timing von Clientzeitplänen aus. Stellen Sie sicher, dass die Start- und Endzeiten von Clientzeitplänen Ihre Geschäftsanforderungen erfüllen. | Klicken Sie auf der Seite Übersicht im Operations Center auf Clients > Zeitpläne.<br><br>In der Tabelle 'Zeitpläne' wird in der Spalte 'Start' die konfigurierte Startzeit für die geplante Operation angezeigt. Um anzuzeigen, wann die letzte Operation gestartet wurde, bewegen Sie den Mauszeiger über das Uhrensymbol. | <p> Tipp: Wenn die Ausführung einer Clientoperation länger als erwartet dauert, empfangen Sie unter Umständen eine Warnung. Führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite 'Übersicht' im Operations Center den Mauszeiger über Clients und klicken Sie auf Zeitpläne.</li> <li>2. Wählen Sie einen Zeitplan aus und klicken Sie auf Details.</li> <li>3. Zeigen Sie die Details eines Zeitplans an, indem Sie auf den blauen Pfeil neben der Zeile klicken.</li> <li>4. Geben Sie im Feld Ausführungszeit die Uhrzeit an, zu der eine Warnung ausgegeben wird, wenn die geplante Operation nicht ausgeführt wird.</li> <li>5. Klicken Sie auf Sichern.</li> </ol> |
| Werten Sie das Timing von Verwaltungstasks aus. Stellen Sie sicher, dass die Start- und Endzeiten von Verwaltungstasks Ihre Geschäftsanforderungen erfüllen. | Klicken Sie auf der Seite Übersicht im Operations Center auf Server > Verwaltung.<br><br>Überprüfen Sie in der Tabelle 'Verwaltung' die Informationen in der Spalte 'Letzte Ausführungsdauer'. Um anzuzeigen, wann die letzte Verwaltungstask gestartet wurde, bewegen Sie den Mauszeiger über das Uhrensymbol.             | <p> Tipp: Wenn die Ausführung einer Verwaltungstask zu lange dauert, ändern Sie die Startzeit oder die maximale Ausführungszeit. Führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>2. Um die Startzeit oder die maximale Ausführungszeit für eine Task zu ändern, geben Sie den Befehl UPDATE SCHEDULE aus. Anweisungen finden Sie in UPDATE SCHEDULE (Clientzeitplan aktualisieren).</li> </ol>  |

#### Zugehörige Verweise:

-  [QUERY ACTLOG \(Aktivitätenprotokoll abfragen\)](#)
-  [UPDATE STGPOOL \(Speicherpool aktualisieren\)](#)
-  [QUERY EXTENTUPDATES \(Aktualisierte Datenbereiche abfragen\)](#)

## Lizenz Einhaltung überprüfen

Stellen Sie sicher, dass die Bedingungen Ihrer Lizenzvereinbarung von Ihrer IBM Spectrum Protect-Lösung eingehalten werden. Indem die Einhaltung regelmäßig überprüft wird, können Sie Trends beim Datenwachstum oder der PVU-Nutzung verfolgen. Planen Sie anhand dieser Informationen den weiteren Kauf von Lizenzen.

### Informationen zu diesem Vorgang

Die Methode zur Überprüfung der Einhaltung der Lizenzbedingungen durch Ihre Lösung variiert abhängig von den Bedingungen Ihrer IBM Spectrum Protect-Lizenzvereinbarung.

#### Front-End-Kapazitätslizenzierung

Das Front-End-Modell bestimmt die Lizenzvoraussetzungen auf der Basis des zurückgemeldeten Volumens an primären Daten, das von Clients gesichert wird. Clients umfassen Anwendungen, virtuelle Maschinen und Systeme.

#### Back-End-Kapazitätslizenzierung

Das Back-End-Modell bestimmt Lizenzvoraussetzungen auf der Basis der Terabyte Daten, die in primären Speicherpools und Repositories gespeichert werden.

Tipps:

- Um die Genauigkeit von Schätzungen der Front-End- und Back-End-Kapazität zu gewährleisten, installieren Sie die neueste Version der Client-Software auf jedem Clientknoten.
- Die Informationen zur Front-End- und Back-End-Kapazität im Operations Center dienen zum Zweck der Planung und Schätzung.

#### PVU-Lizenzierung



Das PVU-Modell basiert auf der Nutzung von PVUs durch Servereinheiten.

Wichtig: Die von IBM Spectrum Protect bereitgestellten PVU-Berechnungen werden als Schätzungen betrachtet und sind nicht rechtsverbindlich. Die von IBM Spectrum Protect zurückgemeldeten PVU-Lizenzinformationen werden nicht als zulässiger Ersatz für das IBM® License Metric Tool angesehen.

Die neuesten Informationen zu Lizenzierungsmodellen finden Sie in den Informationen zu Produktdetails und Lizenzen auf der Website der IBM Spectrum Protect-Produktfamilie. Wenden Sie sich bei Fragen oder Problemstellungen zu Lizenzierungsanforderungen an Ihren IBM Spectrum Protect-Software-Provider.

## Vorgehensweise

Führen Sie zur Überwachung der Lizenz Einhaltung die Schritte aus, die den Bedingungen Ihrer Lizenzvereinbarung entsprechen. Tipp: Das Operations Center stellt einen E-Mail-Bericht bereit, in dem die Front-End- und Back-End-Kapazitätsnutzung zusammengefasst sind. Berichte können automatisch regelmäßig an einen oder mehrere Empfänger gesendet werden. Klicken Sie für die Konfiguration und Verwaltung von E-Mail-Berichten in der Menüleiste des Operations Center auf Berichte.

| Option                  | Bezeichnung   |
|-------------------------|---|
| <b>Front-End-Modell</b> | <p>a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen  und klicken Sie auf Lizenzierung.</p> <p>Die Schätzung der Front-End-Kapazität wird auf der Seite 'Front-End-Nutzung' angezeigt.</p> <p>b. Wenn in der Spalte 'Keine Zurückmeldung' ein Wert angezeigt wird, klicken Sie auf die Zahl, um Clients zu identifizieren, von denen keine Kapazitätsnutzung zurückgemeldet wurde.</p> <p>c. Um die Kapazität für Clients zu schätzen, für die keine Kapazitätsnutzung zurückgemeldet wurde, rufen Sie die folgende FTP-Site auf, auf der Tools und Anweisungen zum Messen der Kapazität bereitgestellt werden:</p> <p><code>ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools</code></p> <p>Um die Front-End-Kapazität mithilfe eines Scripts zu messen, führen Sie die Anweisungen im aktuellen Lizenzierungshandbuch aus.</p> <p>d. Addieren Sie den Operations Center-Schätzwert und alle Schätzwerte, die Sie mithilfe eines Scripts ermittelt haben.</p> <p>e. Überprüfen Sie, ob die geschätzte Kapazität die Bedingungen Ihrer Lizenzvereinbarung einhält.</p> |
| <b>Back-End-Modell</b>  | <p>Einschränkung: Wenn der Quellen- und der Zielreplikationsserver nicht dieselben Maßnahmeneinstellungen verwenden, können Sie das Operations Center nicht zur Überwachung der Back-End-Kapazitätsnutzung für replizierte Clients verwenden. Informationen zur Schätzung der Kapazitätsnutzung für diese Clients finden Sie in Technote 1656476.</p> <p>a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen  und klicken Sie auf Lizenzierung.</p> <p>b. Klicken Sie auf die Registerkarte Back-End.</p> <p>c. Überprüfen Sie, ob das geschätzte Datenvolumen die Bedingungen Ihrer Lizenzvereinbarung einhält.</p>   |
| <b>PVU-Modell</b>       | Informationen zur Vorgehensweise beim Prüfen der Einhaltung der PVU-Lizenzbedingungen finden Sie in Einhaltung des PVU-Lizenzierungsmodells prüfen.   |

## Systemstatus mithilfe von E-Mail-Berichten verfolgen

Konfigurieren Sie das Operations Center für die Generierung von E-Mail-Berichten zur Zusammenfassung des Systemstatus. Sie können eine Mail-Server-Verbindung konfigurieren, Berichtseinstellungen ändern und wahlweise angepasste SQL-Berichte erstellen.

### Vorbereitende Schritte

Bevor Sie E-Mail-Berichte konfigurieren, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- Es ist ein SMTP-Host-Server (SMTP = Simple Mail Transfer Protocol) verfügbar, um Berichte als E-Mail senden und empfangen zu können. Der SMTP-Server muss als offenes Mail-Relay konfiguriert sein. Außerdem müssen Sie sicherstellen, dass der IBM Spectrum Protect-Server, der E-Mail-Nachrichten sendet, Zugriff auf den SMTP-Server hat. Wenn das Operations Center auf einem anderen Computer installiert ist, ist für diesen Computer kein Zugriff auf den SMTP-Server erforderlich.
- Um E-Mail-Berichte konfigurieren zu können, müssen Sie über Systemberechtigung für den Server verfügen.

- Um die Empfänger anzugeben, können Sie eine oder mehrere E-Mail-Adressen oder Administrator-IDs eingeben. Wenn eine Administrator-ID eingegeben werden soll, muss die ID auf dem Hub-Server registriert sein und der ID muss eine E-Mail-Adresse zugeordnet sein. Eine E-Mail-Adresse für einen Administrator können Sie mithilfe des Parameters EMAILADDRESS im Befehl UPDATE ADMIN angeben.

## Informationen zu diesem Vorgang

---

Sie können das Operations Center zum Senden eines Berichts über allgemeine Operationen, eines Lizenzinhaltsberichts und eines oder mehrerer angepasster Berichte, die SQL-Anweisungen SELECT zum Abfragen verwalteter Server verwenden, konfigurieren.

## Vorgehensweise

---

Um E-Mail-Berichte zu konfigurieren und zu verwalten, führen Sie die folgenden Schritte aus:


1. Klicken Sie in der Menüleiste des Operations Center auf Berichte.
2. Wenn noch keine E-Mail-Server-Verbindung konfiguriert ist, klicken Sie auf Mail-Server konfigurieren und füllen Sie die Felder aus. Nach der Konfiguration des Mail-Servers sind der Bericht über allgemeine Operationen und der Lizenzinhaltsbericht aktiviert.
3. Um Berichtseinstellungen zu ändern, wählen Sie einen Bericht aus, klicken Sie auf Details und aktualisieren Sie das Formular.
4. Optional: Um einen angepassten SQL-Bericht hinzuzufügen, klicken Sie auf + Bericht und füllen Sie die Felder aus.  
Tipp: Um einen Bericht sofort auszuführen und zu senden, wählen Sie den Bericht aus und klicken Sie auf Senden.

## Ergebnisse

---

Aktivierte Berichte werden gemäß den angegebenen Einstellungen gesendet.

### Zugehörige Verweise:

 UPDATE ADMIN (Administrator aktualisieren)

## Operationen für eine Plattenspeicherlösung für mehrere Standorte verwalten

---

Verwenden Sie diese Informationen, um Operationen für eine Plattenspeicherlösung für mehrere Standorte mit IBM Spectrum Protect zu verwalten, die einen Server umfasst und Datenduplizierung für mehrere Standorte verwendet.

- **Operations Center verwalten**  
Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt.
- **Anwendungen, virtuelle Maschinen und Systeme schützen**  
Der Server schützt Daten für Clients, die Anwendungen, virtuelle Maschinen und Systeme umfassen können. Um Clientdaten schützen zu können, müssen Sie den Clientknoten beim Server registrieren und einen Sicherungszeitplan zum Schützen der Clientdaten auswählen.
- **Datenspeicher verwalten**  
Verwalten Sie Ihre Daten effizient und fügen Sie dem Server unterstützte Einheiten und Datenträger zum Speichern von Clientdaten hinzu.
- **Replikation verwalten**  
Verwenden Sie die Replikation für die Wiederherstellen von Daten an einem Standort zur Wiederherstellung nach einem Katastrophenfall und zur Beibehaltung desselben Stands von Dateien auf dem Quellenserver und dem Zielsystem. Sie können die Replikation auf Knotenebene verwalten. Sie können Daten auch auf Speicherpool-Ebene schützen.
- **Server schützen**  
Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.
- **Server stoppen und starten**  
Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.
- **Durchführung eines Upgrades für den Server planen**  
Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.
- **Vorbereitungen für einen Ausfall oder eine Systemaktualisierung**  
Treffen Sie Vorbereitungen in IBM Spectrum Protect, damit Ihr System während eines geplanten Stromausfalls oder einer geplanten Systemaktualisierung in einem konsistenten Zustand verbleibt.



- Plan zur Wiederherstellung nach einem Katastrophenfall implementieren  
Implementieren Sie eine Strategie zur Wiederherstellung nach einem Katastrophenfall, um Ihre Anwendungen in einem Katastrophenfall wiederherstellen und hohe Serververfügbarkeit sicherstellen zu können.
- Wiederherstellung nach einem Datenverlust oder Systemausfall  
Mithilfe von IBM Spectrum Protect können Sie Daten wiederherstellen, die bei einem Katastrophenfall oder Systemausfall verloren gegangen sind. Sie können Verzeichniscontainerspeicherpools, Clientdaten und Datenbanken wiederherstellen.

## Operations Center verwalten

---

Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt.

- Peripherieserver hinzufügen und entfernen  
In einer Umgebung mit mehreren Servern können Sie dem Hub-Server die anderen Server, die als *Peripherieserver* bezeichnet werden, hinzufügen.
- Web-Server starten und stoppen  
Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Unter Umständen müssen Sie den Web-Server stoppen und starten, um beispielsweise Konfigurationsänderungen durchzuführen.
- Assistenten für die Erstkonfiguration erneut starten  
Unter Umständen müssen Sie den Assistenten für die Erstkonfiguration im Operations Center erneut starten, um beispielsweise Konfigurationsänderungen durchzuführen.
- Hub-Server ändern  
Mithilfe des Operations Center können Sie den Hub-Server von IBM Spectrum Protect entfernen und einen anderen Hub-Server konfigurieren.
- Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben  
Wenn bestimmte Probleme auftreten, möchten Sie möglicherweise die Operations Center-Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben, bei dem die IBM Spectrum Protect-Server nicht als Hub- oder Peripherieserver definiert sind.

## Peripherieserver hinzufügen und entfernen

---

In einer Umgebung mit mehreren Servern können Sie dem Hub-Server die anderen Server, die als *Peripherieserver* bezeichnet werden, hinzufügen.

### Informationen zu diesem Vorgang

---

Die Peripherieserver senden Alerts und Statusinformationen an den Hub-Server. Das Operations Center zeigt eine konsolidierte Sicht der Alerts und Statusinformationen für den Hub-Server und alle Peripherieserver.

- Peripherieserver hinzufügen  
Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server einen oder mehrere Peripherieserver hinzufügen.
- Peripherieserver entfernen  
Sie können einen Peripherieserver aus dem Operations Center entfernen.

## Peripherieserver hinzufügen

---

Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server einen oder mehrere Peripherieserver hinzufügen.

### Vorbereitende Schritte

---

Die Kommunikation zwischen dem Peripherieserver und dem Hub-Server muss unter Verwendung des Protokolls Transport Layer Security (TLS) geschützt werden. Um die Kommunikation zu schützen, fügen Sie das Zertifikat des Peripherieservers der Truststore-Datei des Hub-Servers hinzu.

### Vorgehensweise

---

1. Klicken Sie in der Menüleiste des Operations Center auf Server. Die Seite Server wird geöffnet.

In der Tabelle auf der Seite Server könnte ein Server den Status "Nicht überwacht" haben. Dieser Status bedeutet, dass - obwohl ein Administrator diesen Server mit dem Befehl DEFINE SERVER für den Hub-Server definiert hat - der Server noch nicht als

Peripherieserver konfiguriert ist.

2. Führen Sie einen der folgenden Schritte aus:
  - Klicken Sie auf den Server, um ihn hervorzuheben, und klicken Sie in der Menüleiste der Tabelle auf Peripherieserver überwachen.
  - Wenn der Server, der hinzugefügt werden soll, in der Tabelle nicht angezeigt wird und die sichere SSL-/TLS-Kommunikation nicht erforderlich ist, klicken Sie in der Menüleiste der Tabelle auf +Peripherieserver.
3. Geben Sie die erforderlichen Informationen an und führen Sie die Schritte im Konfigurationsassistenten für den Peripherieserver aus.  
Tipp: Wenn der Aufbewahrungszeitraum für Ereignissätze des Servers weniger als 14 Tage beträgt, wird der Zeitraum automatisch auf 14 Tage zurückgesetzt, wenn Sie den Server als Peripherieserver konfigurieren.

## Peripherieserver entfernen

---

Sie können einen Peripherieserver aus dem Operations Center entfernen.

### Informationen zu diesem Vorgang

---

Unter Umständen müssen Sie einen Peripherieserver in den folgenden Situationen entfernen:

- Der Peripherieserver soll von einem Hub-Server auf einen anderen Hub-Server versetzt werden.
- Der Peripherieserver soll stillgelegt werden.

### Vorgehensweise

---

Um den Peripherieserver aus der Gruppe der Server zu entfernen, die vom Hub-Server verwaltet werden, führen Sie die folgenden Schritte aus:

1. Geben Sie in der IBM Spectrum Protect-Befehlszeile auf dem Hub-Server den folgenden Befehl aus:

```
QUERY MONITORSETTINGS
```

2. Kopieren Sie in der Ausgabe des Befehls den Namen im Feld Überwachte Gruppe.
3. Geben Sie auf dem Hub-Server den folgenden Befehl aus; dabei ist *Gruppenname* der Name der überwachten Gruppe und *Mitgliedsname* der Name des Peripherieservers:

```
DELETE GRPMEMBER Gruppenname Mitgliedsname
```

4. Optional: Wenn der Peripherieserver von einem Hub-Server auf einen anderen Hub-Server versetzt werden soll, dürfen Sie diesen Schritt **nicht** ausführen. Andernfalls können Sie die Alertausgabe und Überwachung auf dem Peripherieserver inaktivieren, indem Sie auf dem Peripherieserver die folgenden Befehle ausgeben:

```
SET STATUSMONITOR OFF  
SET ALERTMONITOR OFF
```

5. Optional: Wenn die Definition des Peripherieservers für andere Zwecke verwendet wird, wie beispielsweise unternehmensweite Konfiguration, Befehlsweiterleitung, Speichern virtueller Datenträger oder Speicherarchivverwaltung, dürfen Sie diesen Schritt **nicht** ausführen. Andernfalls können Sie die Definition des Peripherieservers auf dem Hub-Server löschen, indem Sie auf dem Hub-Server den folgenden Befehl ausgeben:

```
DELETE SERVER Name_des_Peripherieservers
```

Tipp: Wenn eine Serverdefinition sofort nach dem Entfernen des Servers aus der überwachten Gruppe gelöscht wird, können Statusinformationen für den Server ohne zeitliche Begrenzung im Operations Center verbleiben.

Um dieses Problem zu verhindern, warten Sie, bis das Intervall für die Erfassung von Statusdaten überschritten wurde, bevor Sie die Serverdefinition löschen. Das Intervall für die Erfassung von Statusdaten wird auf der Seite 'Einstellungen' des Operations Center angezeigt.

## Web-Server starten und stoppen


---


Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Unter Umständen müssen Sie den Web-Server stoppen und starten, um beispielsweise Konfigurationsänderungen durchzuführen.



### Vorgehensweise


---

1. Stoppen Sie den Web-Server.

-  AIX-Betriebssysteme Geben Sie im Verzeichnis */Installationsverzeichnis/ui/utills* (dabei gibt *Installationsverzeichnis* das Verzeichnis an, in dem das Operations Center installiert ist) den folgenden Befehl aus:  

```
./stopserver.sh
```
  -  Linux-Betriebssysteme Geben Sie den folgenden Befehl aus:  

```
service opscenter.rc stop
```
  -  Windows-Betriebssysteme Stoppen Sie den Dienst IBM Spectrum Protect Operations Center im Fenster Dienste.
2. Starten Sie den Web-Server.
-  AIX-Betriebssysteme Geben Sie im Verzeichnis */Installationsverzeichnis/ui/utills* (dabei gibt *Installationsverzeichnis* das Verzeichnis an, in dem das Operations Center installiert ist) den folgenden Befehl aus:  


```
./startserver.sh
```
  -  Linux-Betriebssysteme Geben Sie die folgenden Befehle aus:  
Starten Sie den Server:  

```
service opscenter.rc start
```

  
Starten Sie den Server erneut:  

```
service opscenter.rc restart
```

  
Bestimmen Sie, ob der Server aktiv ist:  

```
service opscenter.rc status
```
  -  Windows-Betriebssysteme Starten Sie den Dienst IBM Spectrum Protect Operations Center im Fenster Dienste.

## Assistenten für die Erstkonfiguration erneut starten

---

Unter Umständen müssen Sie den Assistenten für die Erstkonfiguration im Operations Center erneut starten, um beispielsweise Konfigurationsänderungen durchzuführen.

### Vorbereitende Schritte

---

Um die folgenden Einstellungen zu ändern, verwenden Sie die Seite Einstellungen im Operations Center, anstatt den Assistenten für die Erstkonfiguration erneut zu starten:

- Häufigkeit, mit der Statusdaten aktualisiert werden
- Dauer, die Alerts aktiv, inaktiv oder geschlossen bleiben
- Bedingungen, die angeben, dass Clients gefährdet sind

Die Hilfe des Operations Center enthält weitere Informationen zum Ändern dieser Einstellungen.







### Informationen zu diesem Vorgang

---

Um den Assistenten für die Erstkonfiguration erneut zu starten, müssen Sie eine Merkmalsdatei löschen, die Informationen zur Hub-Server-Verbindung enthält. Alle für den Hub-Server konfigurierten Einstellungen für Alertausgabe, Überwachung oder Gefährdung bzw. serverübergreifenden Einstellungen werden nicht gelöscht. Diese Einstellungen werden als Standardeinstellungen im Konfigurationsassistenten verwendet, wenn der Assistent erneut gestartet wird.

### Vorgehensweise

---

1. Stoppen Sie den Web-Server des Operations Center.
2. Wechseln Sie auf dem Computer, auf dem das Operations Center installiert ist, in das folgende Verzeichnis (dabei ist *Installationsverzeichnis* das Verzeichnis, in dem das Operations Center installiert ist):
  -  AIX-Betriebssysteme  Linux-Betriebssysteme *Installationsverzeichnis/ui/Liberty/usr/servers/guiServer*
  -  Windows-Betriebssysteme *Installationsverzeichnis\ui\Liberty\usr\servers\guiServer*
 Beispiel:
  -  AIX-Betriebssysteme  Linux-Betriebssysteme */opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer*
  -  Windows-Betriebssysteme *c:\Programme\Tivoli\TSM\ui\Liberty\usr\servers\guiServer*
3. Löschen Sie im Verzeichnis *guiServer* die Datei *serverConnection.properties*.
4. Starten Sie den Web-Server des Operations Center.
5. Öffnen Sie das Operations Center.

6. Rekonfigurieren Sie mithilfe des Konfigurationsassistenten das Operations Center. Geben Sie ein neues Kennwort für die Überwachungsadministrator-ID an.
7. Aktualisieren auf jedem Peripherieserver, der bereits zuvor mit dem Hub-Server verbunden war, das Kennwort für die Überwachungsadministrator-ID, indem Sie den folgenden Befehl in der IBM Spectrum Protect-Befehlszeilenschnittstelle ausgeben:

```
UPDATE ADMIN IBM-OC-Name_des_Hub-Servers neues_Kennwort
```

Einschränkung: Übernehmen Sie alle anderen Einstellungen für diese Administrator-ID unverändert. Nachdem Sie das Anfangskennwort angegeben haben, wird dieses Kennwort automatisch vom Operations Center verwaltet.

## Hub-Server ändern

---

Mithilfe des Operations Center können Sie den Hub-Server von IBM Spectrum Protect entfernen und einen anderen Hub-Server konfigurieren.

### Vorgehensweise

---

1. Starten Sie den Assistenten für die Erstkonfiguration des Operations Center erneut. Im Rahmen dieser Prozedur löschen Sie die bestehende Hub-Server-Verbindung.
2. Verwenden Sie den Assistenten, um das Operations Center für die Verbindung zu dem neuen Hub-Server zu konfigurieren.

#### Zugehörige Tasks:

Assistenten für die Erstkonfiguration erneut starten

## Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben

---

Wenn bestimmte Probleme auftreten, möchten Sie möglicherweise die Operations Center-Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben, bei dem die IBM Spectrum Protect-Server nicht als Hub- oder Peripherieserver definiert sind.

### Vorgehensweise

---

Um die Konfiguration zurückzuschreiben, führen Sie die folgenden Schritte aus:

1. Stoppen Sie den Web-Server des Operations Center.
2. Dekonfigurieren Sie den Hub-Server, indem Sie die folgenden Schritte ausführen:
  - a. Geben Sie auf dem Hub-Server die folgenden Befehle aus:

```
SET MONITORINGADMIN ""
SET MONITOREDSEVERGROUP ""
SET STATUSMONITOR OFF
SET ALERTMONITOR OFF
REMOVE ADMIN IBM-OC-Name_des_Hub-Servers
```

**Tipp:** *IBM-OC-Name\_des\_Hub-Servers* ist die Überwachungsadministrator-ID, die bei der Erstkonfiguration des Hub-Servers automatisch erstellt wurde.

- b. Setzen Sie das Kennwort für den Hub-Server zurück, indem Sie den folgenden Befehl auf dem Hub-Server ausgeben:

```
SET SERVERPASSWORD ""
```

**Achtung:** Führen Sie diesen Schritt nicht aus, wenn der Hub-Server für andere Server für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation konfiguriert ist.

3. Dekonfigurieren Sie alle Peripherieserver, indem Sie die folgenden Schritte ausführen:
  - a. Um zu bestimmen, ob noch Peripherieserver vorhanden sind, die als Mitglieder der Servergruppe definiert sind, geben Sie auf dem Hub-Server den folgenden Befehl aus:

```
QUERY SERVERGROUP IBM-OC-Name_des_Hub-Servers
```

**Tipp:** *IBM-OC-Name\_des\_Hub-Servers* ist der Name der überwachten Servergruppe, die bei der Konfiguration des ersten Peripherieservers automatisch erstellt wurde. Dieser Servergruppenname stimmt auch mit der Überwachungsadministrator-ID überein, die bei der Erstkonfiguration des Hub-Servers automatisch erstellt wurde.

- b. Um Peripherieserver aus der Servergruppe zu löschen, geben Sie auf dem Hub-Server für jeden Peripherieserver den folgenden Befehl aus:

```
DELETE GRPMEMBER IBM-OC-Name_des_Hub-Servers Name_des_Peripherieservers
```

- c. Nachdem alle Peripherieserver aus der Servergruppe gelöscht wurden, geben Sie auf dem Hub-Server die folgenden Befehle aus:

```
DELETE SERVERGROUP IBM-OC-Name_des_Hub-Servers
SET MONITOREDSEVERGROUP ""
```

d. Geben Sie auf jedem Peripherieserver die folgenden Befehle aus:

```
REMOVE ADMIN IBM-OC-Name_des_Hub-Servers
SETOPT PUSHSTATUS NO
SET ALERTMONITOR OFF
SET STATUSMONITOR OFF
```

e. Löschen Sie die Definition des Hub-Servers, indem Sie auf jedem Peripherieserver den folgenden Befehl ausgeben:

```
DELETE SERVER Name_des_Hub-Servers
```

Achtung: Führen Sie diesen Schritt nicht aus, wenn die Definition für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation verwendet wird.

f. Löschen Sie die Definition jedes Peripherieservers, indem Sie auf dem Hub-Server den folgenden Befehl ausgeben:

```
DELETE SERVER Name_des_Peripherieservers
```

Achtung: Führen Sie diesen Schritt nicht aus, wenn die Serverdefinition für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation verwendet wird.

4. Schreiben Sie die Standardeinstellungen auf jeden Server zurück, indem Sie die folgenden Befehle ausgeben:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Starten Sie den Assistenten für die Erstkonfiguration des Operations Center erneut.

#### Zugehörige Tasks:

Assistenten für die Erstkonfiguration erneut starten  
Web-Server starten und stoppen

## Anwendungen, virtuelle Maschinen und Systeme schützen

---

Der Server schützt Daten für Clients, die Anwendungen, virtuelle Maschinen und Systeme umfassen können. Um Clientdaten schützen zu können, müssen Sie den Clientknoten beim Server registrieren und einen Sicherungszeitplan zum Schützen der Clientdaten auswählen.

- Clients hinzufügen  
Nach der Implementierung einer Datenschutzlösung mit IBM Spectrum Protect können Sie die Lösung durch Hinzufügen von Clients erweitern.
- Clientoperationen verwalten  
Sie können Fehler, die einen Client für Sichern/Archivieren betreffen, mithilfe des Operations Center, das Vorschläge zur Behebung von Fehlern bereitstellt, auswerten und beheben. Bei Fehlern für andere Typen von Clients müssen Sie die Fehlerprotokolle auf dem Client überprüfen und in der Produktdokumentation nachlesen.
- Client-Upgrades verwalten  
Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.
- Clientknoten stilllegen  
Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.
- Daten zum Freigeben von Speicherbereich inaktivieren  
In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegebenen Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

## Clients hinzufügen

---

Nach der Implementierung einer Datenschutzlösung mit IBM Spectrum Protect können Sie die Lösung durch Hinzufügen von Clients erweitern.

## Informationen zu diesem Vorgang

---

Die Prozedur beschreibt grundlegende Schritte zum Hinzufügen eines Clients. Spezifischere Anweisungen zum Konfigurieren von Clients enthält die Dokumentation für das auf dem Clientknoten installierte Produkt. Folgende Typen von Clients können vorhanden sein:

### Anwendungsclientknoten

Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

### Systemclientknoten

Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

### VM-Clientknoten

Clientknoten virtueller Maschinen bestehen aus einem einzelnen Gasthost in einem Hypervisor. Jede virtuelle Maschine wird als ein Dateibereich dargestellt.

## Vorgehensweise

---

Um einen Client hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Wählen Sie die Software aus, die auf dem Clientknoten installiert werden soll, und planen Sie die Installation. Führen Sie die Anweisungen in Client-Software auswählen und Installation planen aus.
2. Geben Sie an, wie Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in Regeln zum Sichern und Archivieren von Clientdaten angeben aus.
3. Geben Sie an, wann Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in Sicherungs- und Archivierungsoperationen planen aus.
4. Um Clients das Herstellen einer Verbindung zum Server zu ermöglichen, registrieren Sie den Client. Führen Sie die Anweisungen in Clients registrieren aus.
5. Um einen Clientknoten zu schützen, installieren und konfigurieren Sie die ausgewählte Software auf dem Clientknoten. Führen Sie die Anweisungen in Clients installieren und konfigurieren aus.

## Client-Software auswählen und Installation planen

---

Unterschiedliche Typen von Daten erfordern unterschiedliche Typen von Schutz. Geben Sie den Typ der Daten an, die geschützt werden müssen, und wählen Sie die geeignete Software aus.

## Informationen zu diesem Vorgang

---

Das bevorzugte Verfahren ist die Installation des Clients für Sichern/Archivieren auf allen Clientknoten, sodass Sie den Clientakzeptor auf dem Clientknoten konfigurieren und starten können. Der Clientakzeptor ist für die effiziente Ausführung geplanter Operationen konzipiert.

Der Clientakzeptor führt Zeitpläne für die folgenden Produkte aus: Client für Sichern/Archivieren, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail und IBM Spectrum Protect for Virtual Environments. Wenn Sie ein Produkt installieren, für das der Clientakzeptor keine Zeitpläne ausführt, müssen Sie die Konfigurationsanweisungen in der Produktdokumentation ausführen, um sicherzustellen, dass geplante Operationen ausgeführt werden können.

## Vorgehensweise

---

Wählen Sie abhängig von Ihrer Zielsetzung die zu installierenden Produkte aus und lesen Sie die Installationsanweisungen. Tipp: Wenn Sie die Client-Software jetzt installieren, müssen Sie auch die in Clients installieren und konfigurieren beschriebenen Clientkonfigurationstasks ausführen, bevor Sie den Client verwenden können.

| Ziel | Produkt und Beschreibung | Installationsanweisungen |
|------|--------------------------|--------------------------|
|------|--------------------------|--------------------------|

| Ziel  | Produkt und Beschreibung  | Installationsanweisungen   |
|---|---|--|
| Schutz eines Dateiservers oder einer Workstation  | Der Client für Sichern/Archivieren sichert und archiviert Dateien und Verzeichnisse von Dateiservern und Workstations in Speicher. Es ist auch möglich, Sicherungsversionen und archivierte Kopien von Dateien zurückzuschreiben und abzurufen.   | <ul style="list-style-type: none"> <li>Anforderungen für den Client für Sichern/Archivieren</li> <li>UNIX- und Linux-Clients für Sichern/Archivieren installieren</li> <li>Windows-Client für Sichern/Archivieren installieren</li> </ul>  |
| Schutz von Anwendungen mit Momentaufnahme sicherungs- und -zurückschreibungs funktionalität | IBM Spectrum Protect Snapshot schützt Daten mit integrierter anwendungsgesteuerter Momentaufnahmesicherungs- und -zurückschreibungs funktionalität. Sie können Daten schützen, die von IBM DB2-Datenbanksoftware sowie SAP-, Oracle-, Microsoft Exchange Server- und Microsoft SQL Server-Anwendungen gespeichert werden. | <ul style="list-style-type: none"> <li>Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen</li> <li>Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen</li> <li>Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen</li> </ul> |
| Schutz einer E-Mail-Anwendung auf einem IBM Domino-Server                                   | IBM Spectrum Protect for Mail: Data Protection for IBM® Domino automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass IBM Domino-Server heruntergefahren werden.  | <ul style="list-style-type: none"> <li>Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0)</li> <li>Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0)</li> </ul>  |
| Schutz einer E-Mail-Anwendung auf einem Server mit Microsoft Exchange Server                | IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass Server mit Microsoft Exchange Server heruntergefahren werden.   | Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server   |
| Schutz einer IBM DB2-Datenbank  | Mithilfe der Anwendungsprogrammierschnittstelle (API) des Clients für Sichern/Archivieren können DB2-Daten auf dem IBM Spectrum Protect-Server gesichert werden.  | IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)  |
| Schutz einer IBM Informix-Datenbank   | Mithilfe der API des Clients für Sichern/Archivieren können Informix-Daten auf dem IBM Spectrum Protect-Server gesichert werden.  | IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)  |
| Schutz einer Microsoft SQL-Datenbank  | IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server schützt Microsoft SQL-Daten.   | Data Protection for SQL Server unter Windows Server Core installieren  |
| Schutz einer Oracle-Datenbank   | IBM Spectrum Protect for Databases: Data Protection for Oracle schützt Oracle-Daten.  | Installation von Data Protection for Oracle  |
| Schutz einer SAP-Umgebung   | IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP stellt Schutz bereit, der für SAP-Umgebungen angepasst ist. Das Produkt dient der Verbesserung der Verfügbarkeit von SAP-Datenbankservern und der Verringerung des Verwaltungsaufwands.  | <ul style="list-style-type: none"> <li>IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 installieren</li> <li>IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle installieren</li> </ul>  |

| Ziel                             | Produkt und Beschreibung   | Installationsanweisungen   |
|----------------------------------|--|--|
| Schutz einer virtuellen Maschine | <p>IBM Spectrum Protect for Virtual Environments stellt Schutz bereit, der für virtuelle Microsoft Hyper-V- und VMware-Umgebungen angepasst ist. Mithilfe von IBM Spectrum Protect for Virtual Environments können Sie immer inkrementelle Sicherungen erstellen, die auf einem zentralen Server gespeichert werden, Sicherungsmaßnahmen erstellen und virtuelle Maschinen oder einzelne Dateien zurückschreiben.</p> <p>Sie können auch stattdessen den Client für Sichern/Archivieren zum Sichern und Zurückschreiben einer vollständigen virtuellen VMware- oder Microsoft Hyper-V-Maschine verwenden. Es ist auch möglich, Dateien oder Verzeichnisse von einer virtuellen VMware-Maschine zu sichern und zurückzuschreiben.</p> | <ul style="list-style-type: none"> <li>• Data Protection for Microsoft Hyper-V installieren</li> <li>• Installation und Upgrade für Data Protection for VMware durchführen</li> <li>• IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)</li> </ul> |

Tipp: Um den Client für die Speicherbereichsverwaltung zu verwenden, können Sie IBM Spectrum Protect for Space Management oder IBM Spectrum Protect HSM for Windows installieren.

## Regeln zum Sichern und Archivieren von Clientdaten angeben

Stellen Sie vor dem Hinzufügen eines Clients sicher, dass entsprechende Regeln zum Sichern und Archivieren der Clientdaten angegeben sind. Während des Clientregistrierungsprozesses ordnen Sie den Clientknoten einer Maßnahmendomäne zu, die die Regeln enthält, die die Regeln enthält, die steuern, wie und wann Clientdaten gespeichert werden.

### Vorbereitende Schritte

Legen Sie die weitere Vorgehensweise fest:

- Wenn Sie mit den Maßnahmen, die für Ihre Lösung konfiguriert sind, vertraut sind und wissen, dass für die Maßnahmen keine Änderungen erforderlich sind, fahren Sie mit Sicherungs- und Archivierungsoperationen planen fort.
- Wenn Sie mit den Maßnahmen nicht vertraut sind, führen Sie die Schritte in dieser Prozedur aus.

### Informationen zu diesem Vorgang

Maßnahmen haben Auswirkungen auf das Datenvolumen, das im Laufe der Zeit gespeichert wird, und den Zeitraum, den Daten aufbewahrt werden und für die Zurückschreibung durch Clients verfügbar sind. Um Datenschutzziele zu erreichen, können Sie die Standardmaßnahme aktualisieren und eigene Maßnahmen erstellen. Eine Maßnahme umfasst die folgenden Regeln:

- Angabe, wie und wann Dateien in Serverspeicher gesichert und archiviert werden
- Anzahl Kopien einer Datei und Zeitraum, den Kopien im Serverspeicher aufbewahrt werden

Während des Clientregistrierungsprozesses ordnen Sie einen Client einer *Maßnahmendomäne* zu. Die Maßnahme für einen bestimmten Client wird durch die Regeln in der Maßnahmendomäne festgelegt, der der Client zugeordnet ist. In der Maßnahmendomäne befinden sich die Regeln, die wirksam sind, in der aktiven *Maßnahmengruppe*.

Wenn ein Client eine Datei sichert oder archiviert, wird die Datei an eine Verwaltungsklasse in der aktiven Maßnahmengruppe der Maßnahmendomäne gebunden. Eine *Verwaltungsklasse* ist die wichtigste Gruppe von Regeln zur Verwaltung von Clientdaten. Die Sicherungs- und Archivierungsoperationen auf dem Client verwenden die Einstellungen in der Standardverwaltungsklasse der Maßnahmendomäne, es sei denn, Sie passen die Maßnahme weiter an. Eine Maßnahme kann angepasst werden, indem weitere Verwaltungsklassen definiert werden und ihre Verwendung über Clientoptionen zugeordnet wird.

Clientoptionen können in einer lokalen, editierbaren Datei auf dem Clientsystem und in einer Clientoptionsgruppe auf dem Server angegeben werden. Die Optionen in der Clientoptionsgruppe auf dem Server können die Optionen in der lokalen Clientoptionsdatei überschreiben oder den Optionen in der lokalen Clientoptionsdatei hinzugefügt werden.

### Vorgehensweise

1. Überprüfen Sie die Maßnahmen, die für Ihre Lösung konfiguriert sind, indem Sie die Anweisungen in Maßnahmen anzeigen ausführen.



2. Wenn geringfügige Änderungen erforderlich sind, um die Datenaufbewahrungsanforderungen zu erfüllen, führen Sie die Anweisungen in Maßnahmen editieren aus.
3. Optional: Wenn Maßnahmendomänen erstellt oder umfangreiche Änderungen an Maßnahmen durchgeführt werden müssen, um Datenaufbewahrungsanforderungen zu erfüllen, lesen Sie die Informationen in Maßnahmen anpassen.

## Maßnahmen anzeigen

---

Zeigen Sie Maßnahmen an, um zu bestimmen, ob die Maßnahmen zur Erfüllung Ihrer Anforderungen editiert werden müssen.

### Vorgehensweise

---

1. Um die aktive Maßnahmengruppe für eine Maßnahmendomäne anzuzeigen, führen Sie die folgenden Schritte aus:
  - a. Wählen Sie auf der Seite Services im Operations Center eine Maßnahmendomäne aus und klicken Sie auf Details.
  - b. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen.  
Tipp: Um sicherzustellen, dass Sie Daten nach einer Ransomware-Attacke wiederherstellen können, beachten Sie die folgenden Richtlinien:
    - Stellen Sie sicher, dass der Wert in der Spalte 'Sicherungen' mindestens 2 beträgt. Der bevorzugte Wert ist 3, 4 oder höher.
    - Stellen Sie sicher, dass der Wert in der Spalte 'Zusätzliche Sicherungen aufbewahren' mindestens 14 Tage beträgt. Der bevorzugte Wert ist 30 Tage oder mehr.
    - Stellen Sie sicher, dass der Wert in der Spalte 'Archivierungen aufbewahren' mindestens 30 Tage beträgt.Wenn IBM Spectrum Protect for Space Management-Software auf dem Client installiert ist, stellen Sie sicher, dass diese Daten vor ihrer Umlagerung gesichert werden. Geben Sie im Befehl `DEFINE MGMTCLASS` oder `UPDATE MGMTCLASS MIGREQUIRESBKUP=YES` an. Befolgen Sie dann die Richtlinien im Tipp.
2. Um inaktive Maßnahmengruppen für eine Maßnahmendomäne anzuzeigen, führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf der Seite Maßnahmengruppen auf die Umschaltfläche Konfigurieren. Jetzt können Sie die inaktiven Maßnahmengruppen anzeigen und editieren.
  - b. Blättern Sie mithilfe der vorwärts und rückwärts gerichteten Pfeile durch die inaktiven Maßnahmengruppen. Wenn Sie eine inaktive Maßnahmengruppe anzeigen, sind die unterschiedlichen Einstellungen für die inaktive und aktive Maßnahmengruppe hervorgehoben.
  - c. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppen sind nicht mehr editierbar.

## Maßnahmen editieren

---

Um die Regeln zu ändern, die für eine Maßnahmendomäne gelten, editieren Sie die aktive Maßnahmengruppe für die Maßnahmendomäne. Sie können auch eine andere Maßnahmengruppe für eine Domäne aktivieren.

### Vorbereitende Schritte

---

Änderungen an Maßnahmen können sich auf die Datenaufbewahrung auswirken. Stellen Sie sicher, dass weiterhin Daten gesichert werden, die für Ihr Unternehmen von entscheidender Bedeutung sind, sodass Sie diese Daten in einem Katastrophenfall zurückschreiben können. Stellen Sie außerdem sicher, dass Ihr System über genügend Speicherbereich für geplante Sicherungsoperationen verfügt.

### Informationen zu diesem Vorgang

---

Sie editieren eine Maßnahmengruppe, indem Sie eine oder mehrere Verwaltungsklassen in der Maßnahmengruppe ändern. Wenn Sie die aktive Maßnahmengruppe editieren, stehen die Änderungen den Clients erst zur Verfügung, nachdem Sie die Maßnahmengruppe reaktiviert haben. Um die editierte Maßnahmengruppe Clients zur Verfügung zu stellen, aktivieren Sie die Maßnahmengruppe.

Obwohl Sie mehrere Maßnahmengruppen für eine Maßnahmendomäne definieren können, kann nur eine einzige Maßnahmengruppe aktiv sein. Wenn Sie eine andere Maßnahmengruppe aktivieren, ersetzt diese die momentan aktive Maßnahmengruppe.

Informationen zu bevorzugten Verfahren zum Definieren von Maßnahmen finden Sie in Maßnahmen anpassen.

### Vorgehensweise

---

1. Wählen Sie auf der Seite Services im Operations Center eine Maßnahmendomäne aus und klicken Sie auf Details.
2. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen.

Die Seite Maßnahmengruppen gibt den Namen der aktiven Maßnahmengruppe an und listet alle Verwaltungsklassen für diese Maßnahmengruppe auf.

3. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppe ist editierbar.

4. Optional: Um eine Maßnahmengruppe zu editieren, die nicht aktiv ist, klicken Sie auf die vorwärts und rückwärts gerichteten Pfeile, um die Maßnahmengruppe zu lokalisieren.
5. Editieren Sie die Maßnahmengruppe, indem Sie eine der folgenden Aktionen ausführen:

| Option  | Bezeichnung   |
|---|---|
| <b>Verwaltungsklasse hinzufügen</b>   | <ol style="list-style-type: none"> <li>a. Klicken Sie in der Tabelle 'Maßnahmengruppen' auf + Verwaltungsklasse.</li> <li>b. Um die Regeln zum Sichern und Archivieren von Daten anzugeben, füllen Sie die Felder im Fenster Verwaltungsklasse hinzufügen aus.</li> <li>c. Um die Verwaltungsklasse als Standardverwaltungsklasse festzulegen, wählen Sie das Kontrollkästchen Als Standardwert definieren aus.</li> <li>d. Klicken Sie auf Hinzufügen.</li> </ol>                                    |
| <b>Verwaltungsklasse löschen</b>  | Klicken Sie in der Spalte 'Verwaltungsklasse' auf -.<br>Tipp: Um die Standardverwaltungsklasse zu löschen, müssen Sie zunächst eine andere Verwaltungsklasse als Standardverwaltungsklasse zuordnen.  |
| <b>Legen Sie eine Verwaltungsklasse als Standardverwaltungsklasse fest.</b> | Klicken Sie in der Spalte 'Standard' für die Verwaltungsklasse auf das Optionsfeld.<br>Tipp: Die Standardverwaltungsklasse verwaltet Clientdateien, wenn einer Datei keine andere Verwaltungsklasse zugeordnet ist oder keine andere Verwaltungsklasse zur Verwaltung geeignet ist. Um sicherzustellen, dass Clients immer Dateien sichern und archivieren können, wählen Sie eine Standardverwaltungsklasse aus, die sowohl Regeln für das Sichern als auch für das Archivieren von Dateien enthält. |
| <b>Verwaltungsklasse ändern</b>   | Um die Merkmale einer Verwaltungsklasse zu ändern, aktualisieren Sie die Felder in der Tabelle.   |

6. Klicken Sie auf Sichern.  
Achtung: Wenn Sie eine neue Maßnahmengruppe aktivieren, können Daten verloren gehen. Daten, die unter einer Maßnahmengruppe geschützt werden, werden möglicherweise unter einer anderen Maßnahmengruppe nicht geschützt. Daher müssen Sie vor dem Aktivieren einer Maßnahmengruppe sicherstellen, dass die Unterschiede zwischen der vorherigen Maßnahmengruppe und der neuen Maßnahmengruppe keinen Datenverlust zur Folge haben.
7. Klicken Sie auf Aktivieren. Es wird eine Zusammenfassung der Unterschiede zwischen der aktiven Maßnahmengruppe und der neuen Maßnahmengruppe angezeigt. Stellen Sie sicher, dass die Änderungen in der neuen Maßnahmengruppe mit Ihren Datenaufbewahrungsanforderungen konsistent sind, indem Sie die folgenden Schritte ausführen:
  - a. Überprüfen Sie die Unterschiede zwischen entsprechenden Verwaltungsklassen in den beiden Maßnahmengruppen und wägen Sie die Konsequenzen für Clientdateien ab. Clientdateien, die an Verwaltungsklassen in der aktiven Maßnahmengruppe gebunden sind, werden in der neuen Maßnahmengruppe an die Verwaltungsklassen mit denselben Namen gebunden.
  - b. Ermitteln Sie Verwaltungsklassen in der aktiven Maßnahmengruppe, die in der neuen Maßnahmengruppe keine Entsprechung haben und wägen Sie die Konsequenzen für Clientdateien ab. Clientdateien, die an diese Verwaltungsklassen gebunden sind, werden von der Standardverwaltungsklasse in der neuen Maßnahmengruppe verwaltet.
  - c. Wenn die Änderungen, die durch die Maßnahmengruppe implementiert werden sollen, akzeptabel sind, wählen Sie das Kontrollkästchen Ich weiß, dass diese Aktualisierungen zu einem Datenverlust führen können aus und klicken Sie auf Aktivieren.

## Sicherungs- und Archivierungsoperationen planen

Bevor Sie einen neuen Client beim Server registrieren, müssen Sie sicherstellen, dass ein Zeitplan verfügbar ist, um anzugeben, wann Sicherungs- und Archivierungsoperationen ausgeführt werden. Während des Registrierungsprozesses können Sie dem Client einen Zeitplan zuordnen.

### Vorbereitende Schritte

Legen Sie die weitere Vorgehensweise fest:

- Wenn Sie mit den Zeitplänen, die für die Lösung konfiguriert sind, vertraut sind und für die Zeitpläne keine Änderungen erforderlich sind, fahren Sie mit Clients registrieren fort.
- Wenn Sie mit den Zeitplänen nicht vertraut sind oder für die Zeitpläne Änderungen erforderlich sind, führen Sie die Schritte in dieser Prozedur aus.

### Informationen zu diesem Vorgang


Normalerweise müssen Sicherungsoperationen für alle Clients täglich ausgeführt werden. Planen Sie Client- und Server-Workloads mit Bedacht, um die beste Leistung für Ihre Speicherumgebung zu erzielen. Um die Überschneidung von Client- und Serveroperationen zu verhindern, planen Sie die Ausführung von Clientsicherungs- und -archivierungsoperationen gegebenenfalls für die Nacht. Wenn sich

Client- und Serveroperationen überschneiden oder ihnen nicht genügend Zeit und Ressourcen zur Verarbeitung zur Verfügung gestellt werden, können eine Verschlechterung der Systemleistung, fehlgeschlagene Operationen und andere Probleme die Folge sein.


## Vorgehensweise

- Überprüfen Sie die verfügbaren Zeitpläne, indem Sie den Mauszeiger in der Menüleiste des Operations Center über Clients bewegen. Klicken Sie auf Zeitpläne.
- Optional: Ändern oder Erstellen Sie einen Zeitplan, indem Sie die folgenden Schritte ausführen:

| Option                    | Bezeichnung  |
|---------------------------|--|
| <b>Zeitplan ändern</b>    | <ol style="list-style-type: none"><li>Wählen Sie in der Sicht Zeitpläne den Zeitplan aus und klicken Sie auf Details.</li><li>Zeigen Sie auf der Seite Zeitplandetails Details an, indem Sie auf die blauen Pfeile am Anfang der Zeilen klicken.</li><li>Ändern Sie die Einstellungen im Zeitplan und klicken Sie auf Sichern.</li></ol> |
| <b>Zeitplan erstellen</b> | Klicken Sie in der Sicht Zeitpläne auf +Zeitplan und führen Sie die Schritte zum Erstellen eines Zeitplans aus.  |

- Optional: Verwenden Sie zum Konfigurieren von Zeitplaneinstellungen, die im Operations Center nicht sichtbar sind, einen Serverbefehl. Angenommen, Sie möchten eine Clientoperation planen, mit der ein bestimmtes Verzeichnis gesichert und einer anderen Verwaltungsklasse als der Standardverwaltungsklasse zugeordnet wird.
  - Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.
  - Geben Sie zum Erstellen eines Zeitplans den Befehl DEFINE SCHEDULE und zum Ändern eines Zeitplans den Befehl UPDATE SCHEDULE aus. Ausführliche Informationen zu den Befehlen finden Sie in DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren) bzw. UPDATE SCHEDULE (Clientzeitplan aktualisieren).

### Zugehörige Tasks:

-  Zeitplan für tägliche Operationen optimieren

## Clients registrieren

Registrieren Sie einen Client, um sicherzustellen, dass der Client die Verbindung zum Server herstellen und der Server Clientdaten schützen kann.

## Vorbereitende Schritte

Bestimmen Sie, ob der Client eine Benutzer-ID mit Administratorberechtigung mit Clienteignerberechtigung für den Clientknoten erfordert. Informationen zum Bestimmen der Clients, die eine Benutzer-ID mit Administratorberechtigung erfordern, finden Sie in Technote 7048963.

Einschränkung: Bei einigen Clienttypen müssen der Clientknotenname und die Benutzer-ID mit Administratorberechtigung übereinstimmen. Sie können diese Clients nicht mithilfe der in Version 7.1.7 eingeführten LDAP-Authentifizierungsmethode authentifizieren. Ausführliche Informationen zu dieser Authentifizierungsmethode, die manchmal als integrierter Modus bezeichnet wird, finden Sie in Benutzer mithilfe einer Active Directory-Datenbank authentifizieren.

## Vorgehensweise

Um einen Client zu registrieren, führen Sie eine der folgenden Aktionen aus.

- Wenn der Client eine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Befehl REGISTER NODE unter Angabe des Parameters USERID:

```
register node Knotenname Kennwort userid=Knotenname
```

Dabei gibt *Knotenname* den Knotennamen und *Kennwort* das Knotenkennwort an. Ausführliche Informationen finden Sie in Knoten registrieren.

- Wenn der Client keine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Assistenten 'Client hinzufügen' im Operations Center. Führen Sie die folgenden Schritte aus:
  - Klicken Sie in der Menüleiste des Operations Center auf Clients.
  - Klicken Sie in der Tabelle 'Clients' auf + Client.
  - Führen Sie die Schritte im Assistenten Client hinzufügen aus:
    - Geben Sie an, dass redundante Daten sowohl auf dem Client als auch auf dem Server gelöscht werden können. Wählen Sie im Bereich 'Clientseitige Dateneduplizierung' das Kontrollkästchen Aktivieren aus.
    - Kopieren Sie im Fenster Konfiguration die Werte für die Optionen TCPSERVERADDRESS, TCPPORT, NODENAME und DEPLICATION.

- Tipp: Notieren Sie die Optionswerte und bewahren Sie die Unterlagen an einem sicheren Ort auf. Nachdem Sie die Clientregistrierung abgeschlossen und die Software auf dem Clientknoten installiert haben, verwenden Sie die Werte zum Konfigurieren des Clients.
- iii. Führen Sie die Anweisungen im Assistenten aus, um die Maßnahmendomäne, den Zeitplan und die Optionsgruppe anzugeben.
  - iv. Legen Sie fest, wie Risiken für den Client angezeigt werden, indem Sie die Einstellung für die Gefährdung angeben.
  - v. Klicken Sie auf Client hinzufügen.

**Zugehörige Verweise:**

- ➔ Option 'tcpserveraddress'
- ➔ Option 'tcpport'
- ➔ Option 'nodename'
- ➔ Option 'deduplication'

## Clients installieren und konfigurieren

Bevor Sie einen Clientknoten schützen können, müssen Sie die ausgewählte Software installieren und konfigurieren.

### Vorgehensweise

Wenn Sie die Software bereits installiert haben, starten Sie mit Schritt 2.

- 1. Führen Sie eine der folgenden Aktionen aus:
  - o Um Software auf einem Anwendungs- oder Clientknoten zu installieren, führen Sie die Anweisungen aus.

| Software  | Link zu Anweisungen   |
|---|---|
| IBM Spectrum Protect-Client für Sichern/Archivieren   | <ul style="list-style-type: none"> <li>■ UNIX- und Linux-Clients für Sichern/Archivieren installieren</li> <li>■ Windows-Client für Sichern/Archivieren installieren</li> </ul> <p>Tipp: Sie können vorhandene Clients auch mithilfe des Operations Center aktualisieren. Anweisungen finden Sie in Clientaktualisierungen planen.</p>  |
| IBM Spectrum Protect for Databases                    | <ul style="list-style-type: none"> <li>■ Installation von Data Protection for Oracle</li> <li>■ Data Protection for SQL Server unter Windows Server Core installieren</li> </ul>  |
| IBM Spectrum Protect for Mail                         | <ul style="list-style-type: none"> <li>■ Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0)</li> <li>■ Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0)</li> <li>■ Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li> </ul> |
| IBM Spectrum Protect Snapshot                         | <ul style="list-style-type: none"> <li>■ Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen</li> <li>■ Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen</li> <li>■ Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen</li> </ul>  |
| IBM Spectrum Protect for Enterprise Resource Planning | <ul style="list-style-type: none"> <li>■ IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 installieren</li> <li>■ IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle installieren</li> </ul>   |

- o Um Software auf einem VM-Clientknoten zu installieren, führen Sie die Anweisungen für den ausgewählten Sicherungstyp aus.

| Sicherungstyp  | Link zu Anweisungen   |
|--|---|
| Wenn Sie planen, VMware-Gesamtsicherungen virtueller Maschinen zu erstellen, installieren und konfigurieren Sie den IBM Spectrum Protect-Client für Sichern/Archivieren. | <ul style="list-style-type: none"> <li>■ UNIX- und Linux-Clients für Sichern/Archivieren installieren</li> <li>■ Windows-Client für Sichern/Archivieren installieren</li> </ul> |

| Sicherungstyp   | Link zu Anweisungen   |
|---|---|
| Wenn Sie planen, immer inkrementelle Gesamtsicherungen virtueller Maschinen zu erstellen, installieren und konfigurieren Sie IBM Spectrum Protect for Virtual Environments und den Client für Sichern/Archivieren auf demselben Clientknoten oder auf unterschiedlichen Clientknoten. | <ul style="list-style-type: none"> <li>■ IBM Spectrum Protect for Virtual Environments-Onlineproduktokumentation</li> </ul> Tipp: Die Software für IBM Spectrum Protect for Virtual Environments und den Client für Sichern/Archivieren sind im IBM Spectrum Protect for Virtual Environments-Installationspaket enthalten. |

2. Um Clients das Herstellen einer Verbindung zum Server zu ermöglichen, fügen Sie die Werte für die Optionen TCPSERVERADDRESS, TCPPORT und NODENAME in der Clientoptionsdatei hinzu oder aktualisieren Sie diese. Verwenden Sie die Werte, die Sie beim Registrieren des Clients notiert haben (Clients registrieren).
  - Fügen Sie für Clients, die unter einem AIX-, Linux- oder Mac OS X-Betriebssystem installiert sind, die Werte der Clientsystemoptionsdatei dsm.sys hinzu.
  - Fügen Sie für Clients, die unter einem Windows-Betriebssystem installiert sind, die Werte der Clientsystemoptionsdatei dsm.opt hinzu.
 Standardmäßig befinden sich die Optionsdateien im Installationsverzeichnis.
3. Wenn ein Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem installiert wurde, installieren Sie den Clientverwaltungsservice auf dem Client. Führen Sie die Anweisungen in Clientverwaltungsservice installieren aus.
4. Konfigurieren Sie den Client für die Ausführung geplanter Operationen. Führen Sie die Anweisungen in Client für die Ausführung geplanter Operationen konfigurieren aus.
5. Optional: Konfigurieren Sie die Kommunikation durch eine Firewall. Führen Sie die Anweisungen in Client/Server-Kommunikation durch eine Firewall konfigurieren aus.
6. Führen Sie eine Testsicherung aus, um sicherzustellen, dass Daten wie geplant geschützt werden. Führen Sie beispielsweise für einen Client für Sichern/Archivieren die folgenden Schritte aus:
  - a. Wählen Sie auf der Seite 'Clients' im Operations Center den Client aus, der gesichert werden soll, und klicken Sie auf Sichern.
  - b. Überprüfen Sie, ob die Sicherung erfolgreich ausgeführt wird und keine Warnungen oder Fehlernachrichten vorhanden sind.
7. Überwachen Sie die Ergebnisse der geplanten Operationen für den Client im Operations Center.

## Nächste Schritte

Um zu ändern, welche Daten vom Client gesichert werden, führen Sie die Anweisungen in Bereich einer Clientsicherung ändern aus.

## Client für die Ausführung geplanter Operationen konfigurieren

Sie müssen einen Client-Scheduler auf dem Clientknoten konfigurieren und starten. Der Client-Scheduler ermöglicht die Kommunikation zwischen dem Client und dem Server, sodass geplante Operationen erfolgen können. Beispielsweise umfassen geplante Operationen normalerweise das Sichern von Dateien von einem Client.

## Informationen zu diesem Vorgang

Die bevorzugte Methode ist die Installation des Clients für Sichern/Archivieren auf allen Clientknoten, sodass Sie den Clientakzeptor auf dem Clientknoten konfigurieren und starten können. Der Clientakzeptor ist für die effiziente Ausführung geplanter Operationen konzipiert. Der Clientakzeptor verwaltet den Client-Scheduler derart, dass der Scheduler nur in erforderlichen Fällen ausgeführt wird:

- Wenn der Zeitpunkt erreicht ist, an dem der Server nach der nächsten geplanten Operation abgefragt werden soll
- Wenn der Zeitpunkt erreicht ist, an dem die nächste geplante Operation gestartet werden soll

Durch die Verwendung des Clientakzeptors ist es möglich, die Anzahl Hintergrundprozesse auf dem Client zu reduzieren und Probleme in Bezug auf die Speicheraufbewahrungsdauer zu vermeiden.

Der Clientakzeptor führt Zeitpläne für die folgenden Produkte aus: Client für Sichern/Archivieren, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail und IBM Spectrum Protect for Virtual Environments. Wenn Sie ein Produkt installiert hatten, für das der Clientakzeptor keine Zeitpläne ausführt, führen Sie die Konfigurationsanweisungen in der Produktdokumentation aus, um sicherzustellen, dass geplante Operationen ausgeführt werden können.

Wenn Ihr Unternehmen standardmäßig ein Zeitplanungstool eines anderen Anbieters verwendet, können Sie statt des Clientakzeptors dieses Zeitplanungstool verwenden. Normalerweise starten Zeitplanungstools anderer Anbieter Clientprogramme direkt mithilfe von Betriebssystembefehlen. Informationen zum Konfigurieren eines Zeitplanungstools eines anderen Anbieters enthält die Produktdokumentation.

Um den Client-Scheduler mithilfe des Clientakzeptors zu konfigurieren und zu starten, führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

### AIX und Oracle Solaris

- Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
- Klicken Sie auf die Registerkarte Web-Client.
- Klicken Sie im Feld Optionen für verwaltete Services auf Zeitplan. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option Beides.
- Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, setzen Sie in der Datei `dsm.sys` die Option `passwordaccess` auf `generate`.
- Um das Clientknotenkenntwort zu speichern, geben Sie den folgenden Befehl aus und geben Sie auf Anforderung das Clientknotenkenntwort ein:

```
dsmc query sess
```

- Starten Sie den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

```
/usr/bin/dsmcad
```

- Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie der Systemstartdatei (normalerweise `/etc/inittab`) den folgenden Eintrag hinzu:

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Clientakzeptordämon
```

### Linux

- Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
- Klicken Sie auf die Registerkarte Web-Client.
- Klicken Sie im Feld Optionen für verwaltete Services auf Zeitplan. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option Beides.
- Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, setzen Sie in der Datei `dsm.sys` die Option `passwordaccess` auf `generate`.
- Um das Clientknotenkenntwort zu speichern, geben Sie den folgenden Befehl aus und geben Sie auf Anforderung das Clientknotenkenntwort ein:

```
dsmc query sess
```

- Starten Sie den Clientakzeptor, indem Sie sich mit der Rootbenutzer-ID anmelden und den folgenden Befehl ausgeben:

```
service dsmcad start
```

- Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie den Service hinzu, indem Sie in einer Shelleingabeaufforderung den folgenden Befehl ausgeben:

```
# chkconfig --add dsmcad
```

### MAC OS X

- Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
- Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, klicken Sie auf Berechtigung, wählen Sie Kennwort generieren aus und klicken Sie auf Anwenden.
- Um anzugeben, wie Services verwaltet werden, klicken Sie auf Web-Client, wählen Sie Zeitplan aus, klicken Sie auf Anwenden und dann auf OK.
- Um sicherzustellen, dass das generierte Kennwort gespeichert wird, starten Sie den Client für Sichern/Archivieren erneut.
- Starten Sie den Clientakzeptor mithilfe der Anwendung 'IBM Spectrum Protect Tools for Administrators'.

### Windows

- Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Dienstprogramme > Setup-Assistent > Hilfe zum Konfigurieren des Client-Schedulers. Klicken Sie auf Weiter.
- Lesen Sie die Informationen auf der Seite Schedulerassistent und klicken Sie auf Weiter.
- Wählen Sie auf der Seite Scheduler-Task die Option Neuen oder zusätzlichen Scheduler installieren aus und klicken Sie auf Weiter.
- Geben Sie auf der Seite Schedulername und -position einen Namen für den Client-Scheduler an, der hinzugefügt wird. Wählen Sie dann Scheduler mit Clientakzeptordämon (CAD) verwalten aus, um den Scheduler zu verwalten, und klicken Sie auf Weiter.

- e. Geben Sie den Namen ein, der diesem Clientakzeptor zugeordnet werden soll. Der Standardname ist 'Clientakzeptor'. Klicken Sie auf Weiter.
- f. Schließen Sie die Konfiguration ab, indem Sie den Assistenten durchlaufen.
- g. Aktualisieren Sie die Clientoptionsdatei, dsm.opt, und setzen Sie die Option passwordaccess auf generate.
- h. Um das Clientknotenkenwort zu speichern, geben Sie den folgenden Befehl in der Eingabeaufforderung aus:

```
dsmc query sess
```

Geben Sie auf Anforderung das Clientknotenkenwort ein.

- i. Starten Sie den Clientakzeptorservice über die Seite Systemsteuerung. Wenn Sie beispielsweise den Standardnamen verwendet haben, starten Sie den Service 'Clientakzeptor'. Starten Sie nicht den Scheduler-Service, den Sie auf der Seite Schedulername und -position angegeben haben. Der Scheduler-Service wird wie erforderlich automatisch vom Clientakzeptorservice gestartet und gestoppt.

## Client/Server-Kommunikation durch eine Firewall konfigurieren

---

Wenn ein Client durch eine Firewall mit einem Server kommunizieren muss, müssen Sie die Client/Server-Kommunikation durch die Firewall ermöglichen.

### Vorbereitende Schritte

---

Wenn Sie den Assistenten 'Client hinzufügen' zum Registrieren eines Clients verwendet hatten, bestimmen Sie die Optionswerte in der Clientoptionsdatei, die während dieses Prozesses abgerufen wurden. Sie können die Werte zur Angabe von Ports verwenden.

### Informationen zu diesem Vorgang

---

Achtung: Konfigurieren Sie eine Firewall nicht derart, dass dies eine Beendigung der Sitzungen zur Folge hätte, die von einem Server oder Speicheragenten verwendet werden. Die Beendigung einer gültigen Sitzung kann zu unvorhersehbaren Ergebnissen führen. Prozesse und Sitzungen scheinen unter Umständen aufgrund von Ein-/Ausgabebefehlen gestoppt zu werden. Um das Ausschließen von Sitzungen von Zeitlimitbeschränkungen zu erleichtern, konfigurieren Sie bekannte Ports für IBM Spectrum Protect-Komponenten. Stellen Sie sicher, dass die Serveroption KEEPALIVE auf den Standardwert YES gesetzt bleibt. Auf diese Art und Weise kann sichergestellt werden, dass die Client/Server-Kommunikation unterbrechungsfrei erfolgt. Anweisungen zum Definieren der Serveroption KEEPALIVE finden Sie in KEEPALIVE.

### Vorgehensweise

---

Öffnen Sie die folgenden Ports, um Zugriff durch die Firewall zu ermöglichen:

TCP/IP-Port für den Client für Sichern/Archivieren, den Verwaltungsbefehlszeilenclient und den Client-Scheduler

Geben Sie den Port über die Option tcpport in der Clientoptionsdatei an. Die Option tcpport in der Clientoptionsdatei muss mit der Option TCPPORT in der Serveroptionsdatei übereinstimmen. Der Standardwert ist 1500. Wenn ein anderer Wert als der Standardwert verwendet werden soll, geben Sie eine Zahl zwischen 1024 und 32767 an.

HTTP-Port, um die Kommunikation zwischen dem Web-Client und fernen Workstations zu ermöglichen

Geben Sie den Port für die ferne Workstation an, indem Sie die Option httpport in der Clientoptionsdatei der fernen Workstation festlegen. Der Standardwert ist 1581.

TCP/IP-Ports für die ferne Workstation

Der Standardwert von 0 (null) hat zur Folge, dass zwei freie Portnummern der fernen Workstation nach dem Zufallsprinzip zugeordnet werden. Wenn die Portnummern nicht nach dem Zufallsprinzip zugeordnet werden sollen, geben Sie über die Option webports in der Clientoptionsdatei der fernen Workstation Werte an.

TCP/IP-Port für Verwaltungssitzungen

Geben Sie den Port an, an dem der Server auf Anforderungen von Verwaltungsclientsitzungen wartet. Der Wert der Clientoption tcpadminport muss mit dem Wert der Serveroption TCPADMINPORT übereinstimmen. Auf diese Art und Weise können Sie sichere Verwaltungssitzungen in einem privaten Netz gewährleisten.

## Clientoperationen verwalten

---

Sie können Fehler, die einen Client für Sichern/Archivieren betreffen, mithilfe des Operations Center, das Vorschläge zur Behebung von Fehlern bereitstellt, auswerten und beheben. Bei Fehlern für andere Typen von Clients müssen Sie die Fehlerprotokolle auf dem Client überprüfen und in der Produktdokumentation nachlesen.

### Informationen zu diesem Vorgang

---

In einigen Fällen können Clientfehler behoben werden, indem der Clientakzeptor gestoppt und gestartet wird. Wenn Clientknoten oder Administrator-IDs gesperrt sind, können Sie das Problem beheben, indem Sie den Clientknoten bzw. die Administrator-ID entsperren und dann das Kennwort zurücksetzen.

Ausführliche Anweisungen zum Identifizieren und Beheben von Clientfehlern finden Sie in [Clientprobleme lösen](#).

- Fehler in Clientfehlerprotokollen auswerten  
Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.
- Clientakzeptor stoppen und erneut starten  
Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.
- Kennwörter zurücksetzen  
Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.
- Bereich einer Clientsicherung ändern  
Wenn Sie Clientsicherungsoperationen konfigurieren, ist das bevorzugte Verfahren das Ausschließen von Objekten, die nicht erforderlich sind. Angenommen, Sie möchten normalerweise temporäre Dateien von einer Sicherungsoperation ausschließen.

## Fehler in Clientfehlerprotokollen auswerten

---

Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.

### Vorbereitende Schritte

---

Um Fehler in einem Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem zu beheben, stellen Sie sicher, dass der Clientverwaltungsservice installiert und gestartet wurde. Installationsanweisungen finden Sie in [Clientverwaltungsservice installieren](#). Anweisungen zur Überprüfung der Installation finden Sie in [Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen](#).

### Vorgehensweise

---

Um Clientfehler zu diagnostizieren und zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn der Clientverwaltungsservice auf dem Clientknoten installiert ist, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Details.
  3. Klicken Sie auf der Seite 'Zusammenfassung' auf die Registerkarte Diagnose.
  4. Überprüfen Sie die abgerufenen Protokollnachrichten.  
Tipps:
    - Um das Fenster 'Clientprotokolle' ein- oder auszublenden, doppelklicken Sie auf den Rahmen des Fensters 'Clientprotokolle'.
    - Um die Größe des Fensters 'Clientprotokolle' zu ändern, klicken Sie auf den Rahmen des Fensters 'Clientprotokolle' und ziehen Sie den Rahmen.

Wenn auf der Seite 'Diagnose' Vorschläge angezeigt werden, wählen Sie einen Vorschlag aus. Im Fenster 'Clientprotokolle' sind die Clientprotokollnachrichten, auf die sich der Vorschlag bezieht, hervorgehoben.
- 5. Lösen Sie die in den Fehlernachrichten angegebenen Probleme mithilfe der Vorschläge.  
Tipp: Vorschläge werden nur für einen Teil der Clientnachrichten bereitgestellt.
- Wenn der Clientverwaltungsservice nicht auf dem Clientknoten installiert ist, überprüfen Sie die Fehlerprotokolle für den installierten Client.

## Clientakzeptor stoppen und erneut starten

---

Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.

### Informationen zu diesem Vorgang

---



In einigen Fällen können Clientzeitplanungsprobleme behoben werden, indem der Clientakzeptor gestoppt und erneut gestartet wird. Der Clientakzeptor muss aktiv sein, um sicherzustellen, dass geplante Operationen auf dem Client ausgeführt werden können. Wenn Sie beispielsweise die IP-Adresse oder den Domännennamen des Servers ändern, müssen Sie den Clientakzeptor erneut starten.

## Vorgehensweise

---

Führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

### AIX und Oracle Solaris

- Um den Clientakzeptor zu stoppen, führen Sie die folgenden Schritte aus:
  - Bestimmen Sie die Prozess-ID für den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

```
ps -ef | grep dsmcad
```

Überprüfen Sie die Ausgabe. In der folgenden Beispielausgabe lautet die Prozess-ID für den Clientakzeptor 6764:

```
root 6764      1   0 16:26:35 ?          0:00 /usr/bin/dsmcad
```

- Geben Sie in der Befehlszeile den folgenden Befehl aus:

```
kill -9 PID
```

Dabei gibt *PID* die Prozess-ID für den Clientakzeptor an.

- Um den Clientakzeptor zu starten, geben Sie in der Befehlszeile den folgenden Befehl aus:

```
/usr/bin/dsmcad
```

### Linux

- Um den Clientakzeptor zu stoppen, ohne ihn erneut zu starten, geben Sie den folgenden Befehl aus:

```
# service dsmcad stop
```

- Um den Clientakzeptor zu stoppen und erneut zu starten, geben Sie den folgenden Befehl aus:

```
# service dsmcad restart
```

### MAC OS X

Klicken Sie auf Applications > Utilities > Terminal.

- Um den Clientakzeptor zu stoppen, geben Sie den folgenden Befehl aus:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Um den Clientakzeptor zu starten, geben Sie den folgenden Befehl aus:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

### Windows

- Um den Clientakzeptorservice zu stoppen, führen Sie die folgenden Schritte aus:
  - Klicken Sie auf Start > Verwaltung > Dienste.
  - Doppelklicken Sie auf den Clientakzeptorservice.
  - Klicken Sie auf Beenden und OK.
- Um den Clientakzeptorservice erneut zu starten, führen Sie die folgenden Schritte aus:
  - Klicken Sie auf Start > Verwaltung > Dienste.
  - Doppelklicken Sie auf den Clientakzeptorservice.
  - Klicken Sie auf Starten und OK.

### Zugehörige Verweise:

 Fehler für Clientzeitplanung beheben

## Kennwörter zurücksetzen

---

Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.

## Vorgehensweise

---

Um Kennwortprobleme zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn ein Client für Sichern/Archivieren auf einem Clientknoten installiert ist und das Kennwort verloren gegangen ist oder Sie das Kennwort vergessen haben, führen Sie die folgenden Schritte aus:
  1. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

```
update node Knotenname neues_Kennwort forcepwreset=yes
```

Dabei gibt *Knotenname* den Clientknoten und *neues\_Kennwort* das Kennwort an, das Sie zuordnen.

2. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.  
Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf generate gesetzt haben.
- Wenn ein Administrator aufgrund von Kennwortproblemen ausgesperrt ist, führen Sie die folgenden Schritte aus:
    1. Um dem Administrator den Zugriff auf den Server zu ermöglichen, geben Sie den Befehl UNLOCK ADMIN aus. Anweisungen finden Sie in UNLOCK ADMIN (Administrator entsperren).
    2. Legen Sie mit dem Befehl UPDATE ADMIN ein neues Kennwort fest:

```
update admin Administratorname neues_Kennwort forcepwreset=yes
```

Dabei gibt *Administratorname* den Namen des Administrators und *neues\_Kennwort* das Kennwort an, das Sie zuordnen.

- Wenn ein Clientknoten gesperrt ist, führen Sie die folgenden Schritte aus:
  1. Bestimmen Sie, warum der Clientknoten gesperrt ist und ob er entsperrt werden muss. Wenn beispielsweise der Clientknoten stillgelegt ist, wird der Clientknoten aus der Produktionsumgebung entfernt. Sie können die Stilllegungsoperation nicht zurücknehmen und der Clientknoten bleibt gesperrt. Ein Clientknoten kann auch gesperrt sein, wenn die Clientdaten Gegenstand einer rechtlichen Untersuchung sind.
  2. Verwenden Sie zum Entsperren eines Clientknotens den Befehl UNLOCK NODE. Anweisungen finden Sie in UNLOCK NODE (Clientknoten entsperren).
  3. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

```
update node Knotenname neues_Kennwort forcepwreset=yes
```

Dabei gibt *Knotenname* den Namen des Knotens und *neues\_Kennwort* das Kennwort an, das Sie zuordnen.

4. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.  
Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf generate gesetzt haben.

## Bereich einer Clientsicherung ändern

---

Wenn Sie Clientsicherungsoperationen konfigurieren, ist das bevorzugte Verfahren das Ausschließen von Objekten, die nicht erforderlich sind. Angenommen, Sie möchten normalerweise temporäre Dateien von einer Sicherungsoperation ausschließen.

### Informationen zu diesem Vorgang

---

Indem Sie nicht benötigte Objekte von Sicherungsoperationen ausschließen, können Sie die Größe des Speicherbereichs, der für Sicherungsoperationen erforderlich ist, und die Speicherkosten besser steuern. Abhängig von Ihrem Lizenzpaket ist es unter Umständen auch möglich, die Lizenzierungskosten zu begrenzen.

## Vorgehensweise

---

Die Vorgehensweise beim Ändern des Bereichs von Sicherungsoperationen ist von dem Produkt abhängig, das auf dem Clientknoten installiert ist:

- Bei einem Client für Sichern/Archivieren können Sie eine Einschluss-/Ausschlussliste erstellen, um eine Datei, Dateigruppen oder Verzeichnisse in Sicherungsoperationen einzuschließen oder von Sicherungsoperationen auszuschließen. Um eine Einschluss-/Ausschlussliste zu erstellen, führen Sie die Anweisungen in Einschluss-/Ausschlussliste erstellen aus.

Um die konsistente Verwendung einer Einschluss-/Ausschlussliste für alle Clients eines bestimmten Typs zu gewährleisten, können Sie auf dem Server eine Clientoptionsgruppe erstellen, die die erforderlichen Optionen enthält. Anschließend ordnen Sie die Clientoptionsgruppe jedem Client desselben Typs zu. Ausführliche Informationen finden Sie in Clientoperationen über Clientoptionsgruppen steuern.

- Für einen Client für Sichern/Archivieren können Sie die Objekte, die in eine Teilsicherungsoperation eingeschlossen werden sollen, mithilfe der Option domain angeben. Führen Sie die Anweisungen in Clientoption 'domain' aus.
- Führen Sie für andere Produkte die Anweisungen in der Produktdokumentation aus, um zu definieren, welche Objekte in Sicherungsoperationen eingeschlossen und von Sicherungsoperationen ausgeschlossen werden sollen.

## Client-Upgrades verwalten

Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.

### Vorbereitende Schritte

1. Überprüfen Sie die Voraussetzungen für die Client/Server-Kompatibilität in Technote 1053218. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden.
2. Überprüfen Sie die Systemvoraussetzungen für den Client in IBM Spectrum Protect Supported Operating Systems.
3. Wenn die Lösung Speicheragenten oder Speicherarchivclients umfasst, überprüfen Sie die Informationen zur Kompatibilität von Speicheragenten bzw. Speicherarchivclients mit Servern, die als Speicherarchivmanager konfiguriert sind. Siehe Technote 1302789.

Wenn Sie planen, ein Upgrade für einen Speicherarchivmanager und einen Speicherarchivclient durchzuführen, müssen Sie zuerst das Upgrade für den Speicherarchivmanager durchführen.

### Vorgehensweise

Um ein Software-Upgrade durchzuführen, führen Sie die in der folgenden Tabelle aufgelisteten Anweisungen aus.

| Software  | Link zu Anweisungen   |
|---|---|
| IBM Spectrum Protect-Client für Sichern/Archivieren   | <ul style="list-style-type: none"> <li>• Clientaktualisierungen planen</li> </ul>   |
| IBM Spectrum Protect Snapshot                         | <ul style="list-style-type: none"> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen</li> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen</li> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen</li> </ul>  |
| IBM Spectrum Protect for Databases                    | <ul style="list-style-type: none"> <li>• Upgrade für Data Protection for SQL Server durchführen</li> <li>• Installation von Data Protection for Oracle</li> <li>• Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li> </ul>   |
| IBM Spectrum Protect for Enterprise Resource Planning | <ul style="list-style-type: none"> <li>• Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 durchführen</li> <li>• Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle durchführen</li> </ul>   |
| IBM Spectrum Protect for Mail                         | <ul style="list-style-type: none"> <li>• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0)</li> <li>• Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0)</li> <li>• Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li> </ul> |
| IBM Spectrum Protect for Virtual Environments         | <ul style="list-style-type: none"> <li>• Installation und Upgrade für Data Protection for VMware durchführen</li> <li>• Data Protection for Microsoft Hyper-V installieren</li> </ul>   |

## Clientknoten stilllegen

Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.

## Informationen zu diesem Vorgang

---

Wenn Sie den Stilllegungsprozess starten, sperrt der Server den Clientknoten, um zu verhindern, dass dieser auf den Server zugreift. Dateien, die zu dem Clientknoten gehören, werden nacheinander gelöscht; anschließend wird der Clientknoten gelöscht. Sie können die folgenden Typen von Clientknoten stilllegen:

### Anwendungsclientknoten

Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

### Systemclientknoten

Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

### VM-Clientknoten

Clientknoten virtueller Maschinen bestehen aus einem einzelnen Gasthost in einem Hypervisor. Jede virtuelle Maschine wird als ein Dateibereich dargestellt.

Die einfachste Methode zur Stilllegung eines Clientknotens ist die Verwendung des Operations Center. Der Stilllegungsprozess wird im Hintergrund ausgeführt. Wenn der Client für die Replikation von Clientdaten konfiguriert ist, entfernt das Operations Center den Client automatisch aus der Replikation auf dem Quellen- und dem Zielreplikationsserver, bevor es den Client stilllegt.

Tipp: Sie können einen Clientknoten auch stilllegen, indem Sie den Befehl `DECOMMISSION NODE` oder `DECOMMISSION VM` ausgeben. Diese Methode kann beispielsweise in den folgenden Fällen verwendet werden:

- Um den Stilllegungsprozess für einen späteren Zeitpunkt zu planen oder eine Serie von Befehlen unter Verwendung eines Scripts auszuführen, geben Sie die Ausführung des Stilllegungsprozesses im Hintergrund an.
- Um den Stilllegungsprozess zu Zwecken der Fehlerbehebung zu überwachen, geben Sie die Ausführung des Stilllegungsprozesses im Vordergrund an. Wenn Sie den Prozess im Vordergrund ausführen, müssen Sie warten, bis der Prozess abgeschlossen ist, bevor Sie die Arbeit mit anderen Tasks fortsetzen können.

## Vorgehensweise

---

Führen Sie eine der folgenden Aktionen aus:

- Um einen Client mithilfe des Operations Center im Hintergrund stillzulegen, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Weitere > Stilllegen.
- Um einen Clientknoten mithilfe eines Verwaltungsbefehls stillzulegen, führen Sie die folgenden Schritte aus:
  1. Bestimmen Sie, ob der Clientknoten für die Knotenreplikation konfiguriert ist, indem Sie den Befehl `QUERY NODE` ausgeben. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, führen Sie den folgenden Befehl aus:

```
query node austin format=detailed
```

Überprüfen Sie das Ausgabefeld 'Replikationsstatus'.

2. Wenn der Clientknoten für die Replikation konfiguriert ist, entfernen Sie den Clientknoten aus der Replikation, indem Sie den Befehl `REMOVE REPLNODE` ausgeben. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

```
remove replnode austin
```

3. Führen Sie eine der folgenden Aktionen aus:

- Um einen Anwendungs- oder Systemclientknoten im Hintergrund stillzulegen, geben Sie den Befehl `DECOMMISSION NODE` aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

```
decommission node austin
```

- Um einen Anwendungs- oder Systemclientknoten im Vordergrund stillzulegen, geben Sie den Befehl `DECOMMISSION NODE` unter Angabe des Parameters `wait=yes` aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

```
decommission node austin wait=yes
```

- Um eine virtuelle Maschine im Hintergrund stillzulegen, geben Sie den Befehl DECOMMISSION VM aus. Wenn beispielsweise die virtuelle Maschine den Namen AUSTIN hat, der Dateibereich 7 ist und der Dateibereichsname über die Dateibereichs-ID angegeben wird, geben Sie den folgenden Befehl aus:

```
decommission vm austin 7 nametype=fsid
```

Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Um eine virtuelle Maschine im Vordergrund stillzulegen, geben Sie den Befehl DECOMMISSION VM unter Angabe des Parameters wait=yes aus. Geben Sie beispielsweise den folgenden Befehl aus:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

## Nächste Schritte

---

Achten Sie auf Fehlermeldungen, die unter Umständen in der Benutzerschnittstelle oder in der Befehlsausgabe unmittelbar nach der Ausführung des Prozesses angezeigt werden.

Um zu überprüfen, ob der Clientknoten stillgelegt wurde, gehen Sie wie folgt vor:

1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients.
2. Überprüfen Sie in der Tabelle 'Clients' in der Spalte 'Gefährdet' den Status:
  - Der Status 'Stillgelegt' (DECOMMISSIONED) gibt an, dass der Knoten stillgelegt wurde.
  - Ein Nullwert gibt an, dass der Knoten nicht stillgelegt wurde.
  - Der Status 'Anstehend' (PENDING) gibt an, dass der Knoten gerade stillgelegt wird oder der Stilllegungsprozess fehlgeschlagen ist.

Tipp: Wenn der Status eines anstehenden Stilllegungsprozesses bestimmt werden soll, geben Sie den folgenden Befehl aus:

```
query process
```

3. Überprüfen Sie die Befehlsausgabe:

- Wenn für den Stilllegungsprozess ein Status angegeben ist, ist der Prozess in Bearbeitung. Beispiel:

```
query process
Prozess-      Prozessbeschreibung      Prozessstatus
nummer
-----      -
          3      DECOMMISSION NODE      Anzahl der für Knoten NODE1 inaktivierten
                                          Sicherungsobjekte: 8 Objekte inaktiviert.
```

- Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie keine Fehlermeldung empfangen haben, ist der Prozess unvollständig. Ein Prozess kann unvollständig sein, wenn Dateien, die dem Knoten zugeordnet sind, noch nicht inaktiviert wurden. Führen Sie nach der Inaktivierung der Dateien den Stilllegungsprozess erneut aus.
- Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie eine Fehlermeldung empfangen, ist der Prozess fehlgeschlagen. Führen Sie den Stilllegungsprozess erneut aus.

### Zugehörige Verweise:

- 🔗 [DECOMMISSION NODE \(Clientknoten stilllegen\)](#)
- 🔗 [DECOMMISSION VM \(Virtuelle Maschine stilllegen\)](#)
- 🔗 [QUERY NODE \(Knoten abfragen\)](#)
- 🔗 [REMOVE REPLNODE \(Clientknoten aus Replikation entfernen\)](#)

## Daten zum Freigeben von Speicherbereich inaktivieren

---

In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegebenen Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

## Informationen zu diesem Vorgang

---

Einige Anwendungsclients sichern Daten immer als aktive Sicherungsdaten auf dem Server. Da aktive Sicherungsdaten nicht durch die Bestandsverfallsmaßnahmen verwaltet werden, werden die Daten nicht automatisch gelöscht und belegen unbegrenzt Serverspeicher. Um den Speicherbereich freizugeben, der von veralteten Daten belegt wird, können Sie die Daten inaktivieren.

Wenn Sie den Inaktivierungsprozess ausführen, werden alle aktiven Sicherungsdaten, die vor dem angegebenen Datum gespeichert wurden, inaktiv. Die Daten werden gelöscht, sobald sie verfallen, und können nicht zurückgeschrieben werden. Die Inaktivierungsfunktion gilt nur für Anwendungsclients, die Oracle-Datenbanken schützen.

## Vorgehensweise

---

1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients.
2. Wählen Sie in der Tabelle 'Clients' einen oder mehrere Clients aus und klicken Sie auf Weitere > Bereinigen.  
Befehlszeilenmethode: Inaktivieren Sie Daten mit dem Befehl DEACTIVATE DATA.

### Zugehörige Verweise:

[DEACTIVATE DATA \(Daten für einen Clientknoten inaktivieren\)](#)

## Datenspeicher verwalten

---

Verwalten Sie Ihre Daten effizient und fügen Sie dem Server unterstützte Einheiten und Datenträger zum Speichern von Clientdaten hinzu.

- **Speicherpoolcontainer prüfen**  
Mit der Prüfung eines Speicherpoolcontainers wird auf Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Speicherpool geprüft.
- **Bestandskapazität verwalten**  
Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.
- **Speichernutzung und Prozessorauslastung verwalten**  
Der Speicherbedarf und die Prozessorauslastung müssen verwaltet werden, um sicherzustellen, dass der Server Datenprozesse wie Sicherung und Datenduplizierung ausführen kann. Berücksichtigen Sie die Auswirkung auf die Leistung, wenn Sie bestimmte Prozesse ausführen.
- **Geplante Aktivitäten optimieren**  
Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

### Zugehörige Verweise:

[Speicherpooltypen](#)

## Speicherpoolcontainer prüfen

---

Mit der Prüfung eines Speicherpoolcontainers wird auf Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Speicherpool geprüft.

## Informationen zu diesem Vorgang

---

Sie prüfen einen Speicherpoolcontainer in den folgenden Situationen:

- Sie geben den Befehl QUERY DAMAGED aus und es wird ein Problem erkannt.
- Der Server zeigt Nachrichten zu beschädigten Datenbereichen an.
- Ihre Hardware meldet ein Problem und es werden Fehlernachrichten angezeigt, die sich auf den Speicherpoolcontainer beziehen.

## Vorgehensweise

---

1. Um einen Speicherpoolcontainer zu prüfen, geben Sie den Befehl AUDIT CONTAINER aus. Geben Sie beispielsweise den folgenden Befehl aus, um den Container 000000000000076c.dcf zu prüfen:

```
audit container c:\tsm-storage\07\000000000000076c.dcf
```

2. Überprüfen Sie die Ausgabe der Nachricht ANR4891I auf Informationen zu allen beschädigten Datenbereichen.

## Nächste Schritte

---

Wenn Sie Probleme mit dem Speicherpoolcontainer erkennen, können Sie Daten auf der Basis Ihrer Konfiguration zurückschreiben. Sie können den Inhalt des Speicherpools mit dem Befehl REPAIR STGPOOL reparieren.

Einschränkung: Sie können den Inhalt des Speicherpools nur reparieren, wenn der Speicherpool mit dem Befehl PROTECT STGPOOL geschützt wurde.

### Zugehörige Verweise:

- 🔗 AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)
- 🔗 QUERY DAMAGED (Beschädigte Daten in einem Verzeichniscontainer- oder Cloud-Containerspeicherpool abfragen)

## Bestandskapazität verwalten

---

Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.

## Vorbereitende Schritte

---

Die aktive Protokolldatei und das Archivprotokoll haben die folgenden Merkmale:

- Die Größe der aktiven Protokolldatei kann maximal 512 GB betragen. Weitere Informationen zum Festlegen der Größe der aktiven Protokolldatei für Ihr System finden Sie in Planung der Speicherarrays.
- Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist. Die Größe des Archivprotokolls ist im Gegensatz zur Größe der aktiven Protokolldatei nicht auf eine vordefinierte Größe festgelegt. Archivprotokolldateien werden automatisch gelöscht, wenn sie nicht mehr benötigt werden.

Als Best Practice können Sie wahlweise ein Archivübernahmeprotokoll erstellen, in dem Archivprotokolldateien gespeichert werden, wenn das Archivprotokollverzeichnis voll ist.

Bestimmen Sie über das Operations Center, welche Komponente des Bestands voll ist. Stellen Sie sicher, dass der Server gestoppt wird, bevor Sie eine der Bestandskomponenten vergrößern.

## Vorgehensweise

---

- Um die Datenbank zu vergrößern, führen Sie die folgenden Schritte aus:
  - Erstellen Sie in unterschiedlichen Laufwerken oder Dateisystemen ein oder mehrere Verzeichnisse für die Datenbank.
  - Geben Sie den Befehl EXTEND DBSPACE aus, um der Datenbank das Verzeichnis oder die Verzeichnisse hinzuzufügen. Die Instanzbenutzer-ID des Datenbankmanagers muss Zugriff auf die Verzeichnisse haben. Standardmäßig erfolgt eine Neuverteilung der Daten auf alle Datenbankverzeichnisse und eine Konsolidierung des Speicherbereichs.  
Tipps:
    - Die Zeit, die für die vollständige Neuverteilung von Daten und die Konsolidierung von Speicherbereich erforderlich ist, variiert abhängig von der Größe Ihrer Datenbank. Stellen Sie sicher, dass Sie dies bei der Planung berücksichtigen.
    - Stellen Sie sicher, dass die Verzeichnisse, die Sie angeben, dieselbe Größe wie vorhandene Verzeichnisse haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorablesenzugriff und zur Verteilung der Datenbank verringert.
  - Stoppen Sie den Server und starten Sie ihn erneut, um die neuen Verzeichnisse vollständig nutzen zu können.
  - Reorganisieren Sie die Datenbank, falls erforderlich. Die Index- und Tabellenreorganisation für die Serverdatenbank kann dazu beitragen, unerwartetes Datenbankwachstum und Leistungsprobleme zu verhindern. Weitere Informationen zur Reorganisation der Datenbank finden Sie in Technote 1683633.
- Um die Datenbank für Server der Version 7.1 und höher zu verkleinern, geben Sie im Serverinstanzverzeichnis die folgenden DB2-Befehle aus:  
Einschränkung: Die Befehle können die E/A-Aktivität erhöhen und sich unter Umständen auf die Serverleistung auswirken. Um Leistungsprobleme auf ein Mindestmaß zu reduzieren, warten Sie, bis ein Befehl abgeschlossen ist, bevor Sie den nächsten Befehl ausgeben. Die DB2-Befehle können ausgegeben werden, wenn der Server aktiv ist.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
```

```

db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE5 REDUCE MAX

```

- Um die aktive Protokolldatei zu vergrößern oder zu verkleinern, führen Sie die folgenden Schritte aus:
  1. Stellen Sie sicher, dass die Position für die aktive Protokolldatei über genügend Speicherbereich für die erhöhte Protokollgröße verfügt. Wenn ein Protokollspiegel vorhanden ist, muss auch die Position für den Spiegel über genügend Speicherbereich für die erhöhte Protokollgröße verfügen.
  2. Stoppen Sie den Server.
  3. Aktualisieren Sie in der Datei dmserv.opt die Option ACTIVELOGSIZE mit der neuen Größe der aktiven Protokolldatei (angegeben in Megabyte).  
Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option ACTIVELOGSIZE. Die folgende Tabelle enthält Richtlinien für den Speicherbedarf:

Tabelle 1. Schätzen des Speicherbedarfs für Datenträger und Dateibereiche

| Wert für die Option ACTIVELOGSIZE | Größe des im Verzeichnis für aktive Protokolldateien zu reservierender freier Speicherbereich zusätzlich zum Speicherbereich für ACTIVELOGSIZE |
|-----------------------------------|--|
| 16 GB bis 128 GB                  | 5120 MB  |
| 129 GB bis 256 GB                 | 10240 MB   |
| 257 GB bis 512 GB                 | 20480 MB   |

Um die Größe der aktiven Protokolldatei in die maximale Größe von 512 GB zu ändern, geben Sie die folgende Serveroption ein:

```
activelogsize 524288
```

4. Wenn Sie planen, ein neues Verzeichnis für aktive Protokolldateien zu verwenden, aktualisieren Sie den in der Serveroption ACTIVELOGDIRECTORY angegebenen Verzeichnisnamen. Das neue Verzeichnis muss leer sein und die Benutzer-ID des Datenbankmanagers muss Zugriff auf dieses Verzeichnis haben.
  5. Starten Sie den Server erneut.
- Komprimieren Sie die Archivprotokolle, um die Größe des Speicherbereichs, der zum Speichern benötigt wird, zu reduzieren. Aktivieren Sie die dynamische Komprimierung für das Archivprotokoll, indem Sie den folgenden Befehl ausgeben:

```
setopt archlogcompress yes
```

Einschränkung: Gehen Sie mit Vorsicht vor, wenn Sie die Serveroption ARCHLOGCOMPRESS auf Systemen mit kontinuierlich hoher Datenträgerverwendung und hohen Workloads aktivieren. Ein Aktivieren dieser Option in dieser Systemumgebung kann Verzögerungen beim Archivieren von Protokolldateien aus dem Dateisystem für aktive Protokolldateien in das Dateisystem für Archivprotokolle haben. Diese Verzögerung kann zur Folge haben, dass der Speicherbereich im Dateisystem für aktive Protokolldateien knapp wird. Sie müssen den verfügbaren Speicherbereich im Dateisystem für aktive Protokolldateien überwachen, nachdem die Komprimierung für das Archivprotokoll aktiviert wurde. Wenn für das Dateisystem für das Verzeichnis für aktive Protokolldateien fast kein Speicherbereich mehr verfügbar ist, muss die Serveroption ARCHLOGCOMPRESS inaktiviert werden. Mit dem Befehl SETOPT können Sie die Komprimierung für das Archivprotokoll sofort inaktivieren, ohne den Server stoppen zu müssen.

#### Zugehörige Verweise:

- ➔ Serveroption ACTIVELOGSIZE
- ➔ EXTEND DBSPACE (Speicherbereich für die Datenbank vergrößern)
- ➔ SETOPT (Serveroption für dynamische Aktualisierung definieren)

## Speichernutzung und Prozessorauslastung verwalten

Der Speicherbedarf und die Prozessorauslastung müssen verwaltet werden, um sicherzustellen, dass der Server Datenprozesse wie Sicherung und Datenduplizierung ausführen kann. Berücksichtigen Sie die Auswirkung auf die Leistung, wenn Sie bestimmte Prozesse ausführen.



## Vorbereitende Schritte

---

- Stellen Sie sicher, dass Ihre Konfiguration die erforderliche Hardware und Software verwendet. Weitere Informationen finden Sie in IBM Spectrum Protect Supported Operating Systems.
- Weitere Informationen zur Verwaltung von Ressourcen, wie beispielsweise Datenbank und Wiederherstellungsprotokoll, finden Sie in Planung der Speicherarrays.
- Fügen Sie zusätzlichen Systemspeicher hinzu, um festzustellen, ob sich die Leistung verbessert. Überwachen Sie die Speichernutzung regelmäßig, um zu bestimmen, ob weiterer Speicher erforderlich ist.

## Vorgehensweise

---

1. Geben Sie, falls möglich, Speicherbereich aus dem Dateisystemcache frei.
2. Verwenden Sie zur Verwaltung des Systemspeichers, den jeder Server auf einem System verwendet, die Serveroption DBMEMPERCENT. Begrenzen Sie den Prozentsatz des Systemspeichers, der vom Datenbankmanager jedes Servers verwendet werden kann. Wenn alle Server gleich wichtig sind, verwenden Sie denselben Wert für jeden Server. Wenn ein Server der Produktionsserver ist und die anderen Server Testserver sind, definieren Sie für den Produktionsserver einen höheren Wert als für die Testserver.
3. Definieren Sie den Benutzerdatengrenzwert und den privaten Speicher für die Datenbank, um sicherzustellen, dass immer genügend privater Speicher verfügbar ist. Wenn der private Speicher knapp wird, kann dies Fehler, eine nicht optimale Leistung und Instabilität zur Folge haben.

## Geplante Aktivitäten optimieren

---

Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

## Vorgehensweise

---


1. Überwachen Sie die Systemleistung regelmäßig, um sicherzustellen, dass Clientsicherungs- und Serververwaltungstasks erfolgreich ausgeführt werden. Führen Sie die Anweisungen in Plattenspeicherlösung für mehrere Standorte überwachen aus.
  2. Optional: Wenn die Überwachungsdaten anzeigen, dass sich die Server-Workload erhöht hat, überprüfen Sie die Planungsinformationen. Überprüfen Sie, ob die Kapazität des Systems in den folgenden Fällen ausreichend ist:
    - Erhöhung der Anzahl Clients
    - Zunahme des Datenvolumens, das gesichert wird
    - Änderung des Zeitraums, der für Sicherungen verfügbar ist
  3. Bestimmen Sie, ob Ihre Lösung auf dem von Ihnen erwarteten Niveau ausgeführt wird. Überprüfen Sie die Clientzeitpläne dahingehend, ob Tasks innerhalb des geplanten Zeitrahmens ausgeführt werden:
    - a. Wählen Sie auf der Seite Clients im Operations Center den Client aus.
    - b. Klicken Sie auf Details.
    - c. Überprüfen Sie auf der Seite Zusammenfassung des Clients die für Gesichert und Repliziert angegebene Aktivität, um alle Risiken zu ermitteln.Passen Sie, falls erforderlich, den Zeitpunkt und die Häufigkeit für die Ausführung von Clientsicherungsoperationen an.
  4. Planen Sie ausreichend Zeit ein, um die folgenden Verwaltungstasks innerhalb von 24 Stunden erfolgreich ausführen zu können:
    - a. Schützen von Speicherpools
    - b. Replizieren von Knotendaten
    - c. Sichern der Datenbank
    - d. Ausführen der Verfallsverarbeitung, um Clientsicherungen und Archivierungsdateikopien aus dem Serverspeicher zu entfernenTipp: Planen Sie einen geeigneten Zeitpunkt für den Start von Verwaltungstasks und die Ausführung in der korrekten Reihenfolge. Planen Sie beispielsweise Replikationstasks im Anschluss an die erfolgreiche Ausführung von Clientsicherungen.
- Clients von einem Server auf einen anderen versetzen  
Um zu verhindern, dass der Speicherbereich auf einem Server knapp wird, oder um Workloadprobleme zu beheben, müssen Sie unter Umständen Clientknoten von einem Server auf einen anderen versetzen.

### Zugehörige Konzepte:

 Leistung

### Zugehörige Tasks:

Zeitpläne für Serververwaltungsaktivitäten definieren

 Daten deduplizieren (Version 7.1.1)

## Replikation verwalten

---

Verwenden Sie die Replikation für die Wiederherstellen von Daten an einem Standort zur Wiederherstellung nach einem Katastrophenfall und zur Beibehaltung desselben Stands von Dateien auf dem Quellenserver und dem Zielsystem. Sie können die Replikation auf Knotenebene verwalten. Sie können Daten auch auf Speicherpoolebene schützen.

- **Replikationskompatibilität**  
Vor dem Konfigurieren von Replikationsoperationen mit IBM Spectrum Protect müssen Sie sicherstellen, dass die Quellen- und Zielreplikationsserver für die Replikation kompatibel sind.
- **Knotenreplikation aktivieren**  
Sie können die Knotenreplikation zum Schützen Ihrer Daten aktivieren.
- **Daten in Verzeichniscontainerspeicherpools schützen**  
Schützen Sie Daten in Verzeichniscontainerspeicherpools, um die Knotenreplikationszeit zu reduzieren und die Reparatur von Daten in Verzeichniscontainerspeicherpools zu ermöglichen.
- **Replikationseinstellungen ändern**  
Ändern Sie Replikationseinstellungen im Operations Center. Ändern Sie Einstellungen wie die Anzahl Replikationssitzungen, Replikationsregeln, die Daten, die repliziert werden sollen, den Replikationszeitplan und die Replikationsworkload.
- **Unterschiedliche Aufbewahrungsmaßnahmen für den Quellenserver und den Zielsystem festlegen**  
Auf dem Zielreplikationsserver können Sie Maßnahmen festlegen, mit denen die replizierten Clientknotendaten anders als auf dem Quellenserver verwaltet werden. Beispielsweise können Sie auf dem Quellen- und dem Zielsystem eine unterschiedliche Anzahl Versionen von Dateien aufbewahren.

## Replikationskompatibilität

Vor dem Konfigurieren von Replikationsoperationen mit IBM Spectrum Protect müssen Sie sicherstellen, dass die Quellen- und Zielreplikationsserver für die Replikation kompatibel sind.

Tabelle 1. Replikationskompatibilität von Serverversionen

| Version des Quellenreplikationsservers | Kompatible Versionen für den Zielreplikationsserver |
|--|---|
| Version 7.1                            | Version 7.1 oder höher                              |
| Version 7.1.1                          | Version 7.1 oder höher                              |
| Version 7.1.3                          | Version 7.1.3 oder höher                            |
| Version 7.1.4                          | Version 7.1.3 oder höher                            |
| Version 7.1.5                          | Version 7.1.3 oder höher                            |
| Version 7.1.6                          | Version 7.1.3 oder höher                            |
| Version 7.1.7                          | Version 7.1.3 oder höher                            |
| Version 7.1.8                          | Version 7.1.3 oder höher                            |
| Version 8.1                            | Version 7.1.3 oder höher                            |
| Version 8.1.1                          | Version 7.1.3 oder höher                            |
| Version 8.1.2                          | Version 7.1.3 oder höher                            |
| Version 8.1.3                          | Version 7.1.3 oder höher                            |

## Knotenreplikation aktivieren

Sie können die Knotenreplikation zum Schützen Ihrer Daten aktivieren.

### Vorbereitende Schritte

Stellen Sie sicher, dass die Quellen- und Zielsystem für die Replikation kompatibel sind.

### Informationen zu diesem Vorgang

Replizieren Sie den Clientknoten, um alle Clientdaten, einschließlich Metadaten, zu replizieren. Standardmäßig ist die Knotenreplikation inaktiviert, wenn Sie den Server zum ersten Mal starten.

Tipps:

- Um die Replikationsverarbeitungszeit zu reduzieren, schützen Sie den Speicherpool vor dem Replizieren von Clientknoten. Wenn die Knotenreplikation gestartet wird, werden die Datenbereiche, die bereits durch den Speicherpoolschutz repliziert werden, übersprungen.

- Die Replikation erfordert mehr Speicherkapazität und genügend Bandbreite für die Ausführung der Verarbeitung. Ändern Sie die Größe der Datenbank und der zugehörigen Protokolle, um sicherzustellen, dass Transaktionen ausgeführt werden können.

## Vorgehensweise

---


Um die Knotenreplikation zu aktivieren, führen Sie im Operations Center die folgenden Schritte aus:

- a. Klicken Sie auf der Seite Server auf Details.
- b. Klicken Sie auf der Seite Details auf Merkmale.
- c. Wählen Sie im Abschnitt Replikation im Feld Abgehende Replikation die Option Aktiviert aus.
- d. Klicken Sie auf Sichern.

## Nächste Schritte

---

Führen Sie die folgenden Aktionen aus:

1. Informationen zur Überprüfung, ob die Replikation erfolgreich war, finden Sie in Prüfliste für tägliche Überwachungstasks.
2.  Wenn der IBM Spectrum Protect-Server Knoten auf einen fernen Server repliziert, prüfen Sie, ob der Datendurchsatz an den fernen Server mithilfe der Technologie von Aspera Fast Adaptive Secure Protocol (FASP) verbessert werden kann. Führen Sie die Anweisungen in Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann aus.

**Zugehörige Verweise:**  
Replikationskompatibilität

## Daten in Verzeichniscontainerspeicherpools schützen

---

Schützen Sie Daten in Verzeichniscontainerspeicherpools, um die Knotenreplikationszeit zu reduzieren und die Reparatur von Daten in Verzeichniscontainerspeicherpools zu ermöglichen.

## Vorbereitende Schritte

---

Stellen Sie sicher, dass mindestens ein Verzeichniscontainerspeicherpool auf dem Zielreplikationsserver vorhanden ist. Wenn Sie die Replikation im Operations Center aktivieren, können Sie den Speicherpoolschutz planen. Um die Replikation zu konfigurieren und den Speicherpoolschutz zu aktivieren, führen Sie die folgenden Schritte aus:

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Speicher und klicken Sie auf Replikation.
2. Klicken Sie auf der Seite 'Replikation' auf Serverpaar.
3. Führen Sie die Schritte im Assistenten 'Serverpaar hinzufügen' aus.

## Informationen zu diesem Vorgang

---

Durch das Schützen eines Verzeichniscontainerspeicherpools werden Datenbereiche in einem anderen Speicherpool gesichert und die Leistung bei der Knotenreplikation wird gegebenenfalls verbessert. Wenn die Knotenreplikation gestartet wird, werden die Datenbereiche, die bereits durch Speicherpoolschutz gesichert werden, übersprungen und die Replikationsverarbeitungszeit wird somit reduziert. Sie können den Schutz von Speicherpools mehrmals am Tag planen, um den Änderungen an Daten Rechnung zu tragen.

Indem ein Speicherpool geschützt wird, werden keine Ressourcen verwendet, die vorhandene Daten und Metadaten replizieren, wodurch die Serverleistung verbessert wird. Sie müssen Verzeichniscontainerspeicherpools verwenden, wenn nur der Speicherpool geschützt und gesichert werden soll.

Alternative Schutzstrategie: Als Alternative zur Verwendung der Replikation können Sie Daten in Verzeichniscontainerspeicherpools schützen, indem Sie die Daten in Containerkopierspeicherpools kopieren. Daten in Containerkopierspeicherpools werden auf Banddatenträgern gespeichert. Bandkopien, die an einem anderen Standort aufbewahrt werden, stellen zusätzlichen Schutz für die Wiederherstellung nach einem Katastrophenfall in einer replizierten Umgebung bereit.

## Vorgehensweise

---

1. Um den Speicherpoolschutz zu aktivieren, können Sie auch stattdessen den Befehl PROTECT STGPOOL auf dem Quellenserver verwenden, um Datenbereiche in einem Verzeichniscontainerspeicherpool zu sichern. Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen POOL1 zu schützen, geben Sie den folgenden Befehl aus:

```
protect stgpool pool1
```

Im Rahmen der Ausführung des Befehls PROTECT STGPOOL werden beschädigte Speicherbereiche im Zielspeicherpool repariert. Eine Reparatur ist nur möglich, wenn die Speicherbereiche auf dem Zielsystem bereits als beschädigt markiert sind. Beispielsweise

kann vor der Ausgabe des Befehls PROTECT STGPOOL mit einem Befehl AUDIT CONTAINER eine Beschädigung im Zielspeicherpool identifiziert werden.

2. Optional: Wenn beschädigte Speicherbereiche im Zielspeicherpool repariert wurden und Sie mehrere Quellenspeicherpools in einem einzigen Zielspeicherpool schützen, führen Sie die folgenden Schritte aus, um eine vollständige Reparatur zu gewährleisten:
  - a. Geben Sie den Befehl PROTECT STGPOOL für alle Quellenspeicherpools aus, um die Beschädigung möglichst vollständig zu reparieren.
  - b. Geben Sie den Befehl PROTECT STGPOOL erneut für alle Quellenspeicherpools aus. Verwenden Sie bei dieser zweiten Operation den Parameter FORCERECONCILE=YES. Mit diesem Schritt wird sichergestellt, dass alle Reparaturen anderer Quellenpools korrekt für alle Quellenspeicherpools erkannt werden.


## Ergebnisse

Wenn ein Verzeichniscontainerspeicherpool geschützt wird, können Sie den Speicherpool für den Fall, dass eine Beschädigung auftritt, mit dem Befehl REPAIR STGPOOL reparieren.




Einschränkung: Wenn Sie Clientknoten replizieren, den Verzeichniscontainerspeicherpool aber nicht schützen, können Sie den Speicherpool nicht reparieren.

## Nächste Schritte



Führen Sie die folgenden Aktionen aus:

1. Um den Replikationsworkloadstatus anzuzeigen, führen Sie die Anweisungen in Prüfliste für tägliche Überwachungstasks aus.
2.  Wenn der IBM Spectrum Protect-Server Knoten auf einen fernen Server repliziert, prüfen Sie, ob der Datendurchsatz an den fernen Server mithilfe der Technologie von Aspera Fast Adaptive Secure Protocol (FASP) verbessert werden kann. Führen Sie die Anweisungen in Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann aus.

### Zugehörige Verweise:

-  Daten in Verzeichniscontainerspeicherpools reparieren und wiederherstellen
-  AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)
-  PROTECT STGPOOL (Speicherpooldaten schützen)

### Zugehörige Informationen:

-  Häufig gestellte Fragen (FAQs) zu Verzeichniscontainerspeicherpools
-  Häufig gestellte Fragen (FAQs) zu Cloud-Containerspeicherpools

## Replikationseinstellungen ändern

Ändern Sie Replikationseinstellungen im Operations Center. Ändern Sie Einstellungen wie die Anzahl Replikationssitzungen, Replikationsregeln, die Daten, die repliziert werden sollen, den Replikationszeitplan und die Replikationsworkload.

## Informationen zu diesem Vorgang

In den folgenden Szenarios müssen Sie möglicherweise Ihre Replikationseinstellungen ändern:

- Änderungen an Datenprioritäten
- Änderungen an Replikationsregeln
- Erfordernis eines anderen Servers als Zielsever
- Geplante Prozesse, die sich negativ auf die Serverleistung auswirken

## Vorgehensweise

Ändern Sie mithilfe des Operations Center die Replikationseinstellungen.

| Task                           | Prozedur   |
|--------------------------------|--|
| Ändern einer Replikationsregel | <ol style="list-style-type: none"><li>a. Klicken Sie auf der Seite Server auf Details.</li><li>b. Klicken Sie auf der Seite Details auf Merkmale.</li><li>c. Wählen Sie im Abschnitt Replikation die Replikationsregel aus, die angewendet werden soll: Standardregel für Archivierungsdaten, Standardregel für Sicherungsdaten oder Standardregel für speicherverwaltete Daten.</li><li>d. Klicken Sie auf Sichern.</li></ol> |

| Task  | Prozedur   |
|---|--|
| Aufbewahrungsdauer für Replikationsdatensätze angeben | <ul style="list-style-type: none"> <li>a. Klicken Sie auf der Seite Server auf Details.</li> <li>b. Klicken Sie auf der Seite Details auf Merkmale.</li> <li>c. Geben Sie im Abschnitt Replikation im Feld Replikationsprotokoll aufbewahren die Anzahl Tage ein, die Replikationsdatensätze beibehalten werden müssen. Sie können auch das Kontrollkästchen Nicht aufbewahren auswählen, wenn Replikationsdatensätze nicht erforderlich sind.</li> <li>d. Klicken Sie auf Sichern.</li> </ul> |
| Zielreplikationsserver angeben                        | <ul style="list-style-type: none"> <li>a. Klicken Sie auf der Seite Server auf Details.</li> <li>b. Klicken Sie auf der Seite Details auf Merkmale.</li> <li>c. Geben Sie im Abschnitt Replikation den Zielserver an.</li> <li>d. Klicken Sie auf Sichern.</li> </ul>  |
| Replikationsprozess abbrechen                         | <ul style="list-style-type: none"> <li>a. Klicken Sie auf der Seite Server auf Aktive Tasks.</li> <li>b. Wählen Sie den Prozess oder die Sitzung aus, der bzw. die abgebrochen werden soll.</li> <li>c. Klicken Sie auf Abbrechen.</li> </ul>  |

## Unterschiedliche Aufbewahrungsmaßnahmen für den Quellenserver und den Zielserver festlegen

Auf dem Zielreplikationsserver können Sie Maßnahmen festlegen, mit denen die replizierten Clientknotendaten anders als auf dem Quellenserver verwaltet werden. Beispielsweise können Sie auf dem Quellen- und dem Zielserver eine unterschiedliche Anzahl Versionen von Dateien aufbewahren.

### Vorgehensweise

- Überprüfen Sie auf dem Quellenreplikationsserver die Replikationskonfiguration und stellen Sie sicher, dass der Quellenreplikationsserver mit dem Zielreplikationsserver kommunizieren kann, indem Sie den Befehl `VALIDATE REPLICATION` ausgeben. Überprüfen Sie beispielsweise die Konfiguration unter Angabe des Namens eines Clientknotens, der repliziert wird:

```
validate replication node1 verifyconnection=yes
```

- Geben Sie auf dem Quellenreplikationsserver den Befehl `VALIDATE REPLPOLICY` aus, um die Unterschiede zwischen den Maßnahmen auf dem Quellenreplikationsserver und den Maßnahmen auf dem Zielreplikationsserver zu überprüfen. Um beispielsweise die Unterschiede zwischen den Maßnahmen auf dem Quellenserver und den Maßnahmen auf dem Zielserver `CVT_SRV2` anzuzeigen, geben Sie auf dem Quellenserver den folgenden Befehl aus:

```
validate replpolicy cvt_srv2
```

- Aktualisieren Sie die Maßnahmen auf dem Zielserver, falls erforderlich.
 

Tipp: Sie können die Maßnahmen auf dem Zielserver mithilfe des Operations Center ändern. Führen Sie die Anweisungen in Maßnahmen editieren aus.

Um beispielsweise inaktive Dateiversionen auf dem Zielserver für einen kürzeren Zeitraum als auf dem Quellenserver aufzubewahren, reduzieren Sie die Einstellung Sicherungen in den Verwaltungsklassen, die für replizierte Clientdaten gelten.
- Ermöglichen Sie dem Zielreplikationsserver die Verwendung seiner Maßnahmen zur Verwaltung der replizierten Clientknotendaten, indem Sie auf dem Quellenserver den Befehl `SET DISSIMILARPOLICIES` ausgeben. Um beispielsweise die Maßnahmen auf dem Zielreplikationsserver `CVT_SRV2` zu aktivieren, geben Sie auf dem Quellenserver den folgenden Befehl aus:

```
set dissimilarpolicies cvt_srv2 on
```

Bei der nächsten Ausführung des Replikationsprozesses werden die Maßnahmen auf dem Zielreplikationsserver zur Verwaltung der replizierten Clientknotendaten verwendet.

Tipp: Wenn Sie die Replikation mithilfe des Operations Center konfigurieren und die Maßnahmen auf dem Quellen- und dem Zielreplikationsserver nicht übereinstimmen, wird die für den Quellenreplikationsserver angegebene Maßnahme verwendet. Wenn die Maßnahmen auf dem Zielreplikationsserver mithilfe des Befehls `SET DISSIMILARPOLICIES` aktiviert wurden, wird die für den Zielreplikationsserver angegebene Maßnahme verwendet. Wenn der Zielreplikationsserver nicht über die von dem Knoten auf dem Quellenreplikationsserver verwendete Maßnahme verfügt, wird die Maßnahme `STANDARD` verwendet.

#### Zugehörige Verweise:

[EXPORT POLICY \(Maßnahmeninformationen exportieren\)](#)

- ☞ SET DISSIMILARPOLICIES (Maßnahmen auf dem Zielreplikationsserver zum Verwalten replizierter Daten aktivieren)
- ☞ VALIDATE REPLICATION (Replikation für einen Clientknoten überprüfen)
- ☞ VALIDATE REPLPOLICY (Maßnahmen auf dem Zielreplikationsserver überprüfen)

## Server schützen

---

Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.

- Sicherheitskonzepte  
Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.
- Administratoren verwalten  
Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.
- Kennwortanforderungen ändern  
Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.
- IBM Spectrum Protect auf dem System schützen  
Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

## Sicherheitskonzepte

---

Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.

## Transport Layer Security

---

Mithilfe des Protokolls Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) können Sie Transportschichtersicherheit für eine sichere Verbindung zwischen Servern, Clients und Speicheragenten bereitstellen. Wenn Sie Daten zwischen dem Server, dem Client und dem Speicheragenten austauschen, verwenden Sie SSL oder TLS zum Verschlüsseln der Daten.

Tipp: In der gesamten IBM Spectrum Protect-Dokumentation gilt jede Angabe von "SSL" oder zum "Auswählen von SSL" für TLS.

SSL wird von Global Security Kit (GSKit) bereitgestellt, das zusammen mit dem IBM Spectrum Protect-Server installiert wird, der vom Server, vom Client und vom Speicheragenten verwendet wird.

Einschränkung: Sie dürfen die SSL- oder TLS-Protokolle nicht für die Kommunikation mit einer DB2-Datenbankinstanz verwenden, die von IBM Spectrum Protect-Servern verwendet wird.

Jeder Server, Client oder Speicheragent, der SSL ermöglicht, muss ein vertrauenswürdigen selbst signiertes Zertifikat verwenden oder ein eindeutiges Zertifikat anfordern, das von einer Zertifizierungsstelle (CA) signiert ist. Sie können Ihre eigenen Zertifikate verwenden oder Zertifikate bei einer Zertifizierungsstelle (CA) kaufen. Jedes der Zertifikate muss installiert und der Schlüsseldatenbank auf dem IBM Spectrum Protect-Server, -Client oder -Speicheragenten hinzugefügt werden. Das Zertifikat wird von dem SSL-Client oder -Server geprüft, der die SSL-Kommunikation anfordert oder einleitet. Einige CA-Zertifikate sind in der Schlüsseldatenbank standardmäßig vorinstalliert.

SSL wird auf dem IBM Spectrum Protect-Server, -Client und -Speicheragenten unabhängig voneinander konfiguriert.

## Berechtigungsstufen

---

Für jeden IBM Spectrum Protect-Server sind verschiedene Administratorberechtigungsstufen verfügbar, die die Tasks festlegen, die ein Administrator ausführen kann.

Nach der Registrierung muss einem Administrator Berechtigung erteilt werden, indem ihm eine oder mehrere Administratorberechtigungsstufen zugeordnet werden. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen und anderen Administratoren über den Befehl GRANT AUTHORITY Berechtigungsstufen zuordnen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

Ein Administrator kann andere Administrator-IDs registrieren, den IDs Berechtigungsstufen zuordnen, IDs umbenennen, IDs entfernen und IDs für den Server sperren oder entsperren.

Ein Administrator kann den Zugriff auf bestimmte Clientknoten für Rootbenutzer-IDs und Nicht-Rootbenutzer-IDs steuern. Standardmäßig kann eine Nicht-Rootbenutzer-ID keine Daten auf dem Knoten sichern. Ändern Sie mit dem Befehl UPDATE NODE die

Knoteneinstellungen, um Sicherungen zu ermöglichen.

## Kennwörter

Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer beim Zugriff auf den Server ein Kennwort eingeben.

Verwenden Sie LDAP (Lightweight Directory Access Protocol), um striktere Anforderungen für Kennwörter anzuwenden. Weitere Informationen finden Sie in Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1).

Tabelle 1. Merkmale der Kennwortauthentifizierung

| Merkmale                                   | Weitere Informationen  |
|--|--|
| Abhängigkeit von der Groß-/Kleinschreibung | Nicht von der Groß-/Kleinschreibung abhängig.  |
| Standardwert für Kennwortablauf            | 90 Tage.<br><br>Der Ablaufzeitraum beginnt mit der ersten Registrierung einer Administrator-ID oder eines Clientknotens beim Server. Wenn das Kennwort innerhalb dieses Zeitraums nicht geändert wird, muss das Kennwort beim nächsten Zugriff des Benutzers auf den Server geändert werden. |
| Ungültige Kennworteingabeversuche          | Sie können einen Grenzwert für aufeinanderfolgende ungültige Kennworteingabeversuche für alle Clientknoten definieren. Wenn der Grenzwert überschritten wird, sperrt der Server den Knoten.  |
| Kennwortlänge                              | Der Administrator kann eine Mindestlänge angeben.  |

## Sitzungssicherheit

Die Sitzungssicherheit ist die Sicherheitsstufe, die für die Kommunikation zwischen IBM Spectrum Protect-Clientknoten, -Verwaltungsclients und -Servern verwendet wird und mit dem Parameter SESSIONSECURITY festgelegt wird.

Der Parameter SESSIONSECURITY kann auf einen der folgenden Werte gesetzt werden:

- Mit dem Wert STRICT wird die höchste Sicherheitsstufe für die Kommunikation zwischen IBM Spectrum Protect-Servern, -Knoten und -Administratoren durchgesetzt.
- Der Wert TRANSITIONAL gibt an, dass das vorhandene Kommunikationsprotokoll verwendet wird, wenn Sie Ihre IBM Spectrum Protect-Software auf Version 8.1.2 oder höher aktualisieren. Dies ist der Standardwert. Wenn SESSIONSECURITY=TRANSITIONAL angegeben ist, werden strengere Sicherheitseinstellungen automatisch durchgesetzt, da höhere Versionen des TLS-Protokolls verwendet werden, wenn die Software auf Version 8.1.2 oder höher aktualisiert wird. Nachdem ein Knoten, Administrator oder Server die Anforderungen für den Wert STRICT erfüllt, wird die Sitzungssicherheit automatisch in den Wert STRICT geändert und die Entität kann sich nicht mehr unter Verwendung einer Vorgängerversion des Clients oder unter Verwendung früherer TLS-Protokolle authentifizieren.

Weitere Informationen zu den Werten für den Parameter SESSIONSECURITY enthalten die Beschreibungen der folgenden Befehle.

Tabelle 2. Befehle zum Festlegen des Parameters SESSIONSECURITY

| Entität         | Befehl  |
|-----------------|---|
| Clientknoten    | <ul style="list-style-type: none"><li>• REGISTER NODE</li><li>• UPDATE NODE</li></ul>   |
| Administratoren | <ul style="list-style-type: none"><li>• REGISTER ADMIN</li><li>• UPDATE ADMIN</li></ul> |
| Server          | <ul style="list-style-type: none"><li>• DEFINE SERVER</li><li>• UPDATE SERVER</li></ul> |

Administratoren, die sich unter Verwendung des Befehls DSMADMC, des Befehls DSMC oder des Programms dsm authentifizieren, können sich nach der Authentifizierung unter Verwendung von Version 8.1.2 oder höher nicht unter Verwendung einer früheren Version authentifizieren. Die folgenden Tipps liefern Informationen zur Behebung von Authentifizierungsproblemen für Administratoren:  
Tipps:

- Stellen Sie sicher, dass für die gesamte IBM Spectrum Protect-Software, die das Administratorkonto für die Anmeldung verwendet, ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird. Wenn sich ein Administratorkonto über mehrere Systeme

- anmeldet, stellen Sie sicher, dass das Zertifikat des Servers auf jedem System installiert ist.
- Nachdem sich ein Administrator bei einem Server der Version 8.1.2 oder höher unter Verwendung eines Clients der Version 8.1.2 oder höher authentifiziert hat, kann sich der Administrator nur auf Clients oder Servern authentifizieren, die Version 8.1.2 oder höher verwenden. Ein Administratorbefehl kann von jedem beliebigen System ausgegeben werden.
  - Erstellen Sie, falls erforderlich, ein separates Administratorkonto, das nur mit Clients und Servern verwendet wird, die Software der Version 8.1.1 oder früher verwenden.

Setzen Sie die höchste Sicherheitsstufe für die Kommunikation mit dem IBM Spectrum Protect-Server durch, indem Sie sicherstellen, dass alle Knoten, Administratoren und Server die Sitzungssicherheit STRICT verwenden. Mithilfe des Befehls SELECT können Sie feststellen, welche Server, Knoten und Administratoren die Sitzungssicherheit TRANSITIONAL verwenden und für die Verwendung der Sitzungssicherheit STRICT aktualisiert werden sollten.

**Zugehörige Tasks:**

- ☞ Kommunikation schützen

## Administratoren verwalten

Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.

### Vorgehensweise

Führen Sie die folgenden Tasks aus, um Administratoreinstellungen zu ändern.

| Task  | Prozedur   |
|---|--|
| Administrator hinzufügen                        | Um einen Administrator, ADMIN1, mit Systemberechtigung hinzuzufügen und ein Kennwort anzugeben, führen Sie die folgenden Schritte aus: <ol style="list-style-type: none"> <li>Registrieren Sie den Administrator und geben Sie Pa\$#\$twO als Kennwort an, indem Sie den folgenden Befehl ausgeben:               <pre>register admin admin1 Pa\$#\$twO</pre> </li> <li>Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben:               <pre>grant authority admin1 classes=system</pre> </li> </ol> |
| Administratorberechtigung ändern                | Ändern Sie die Berechtigungsstufe für einen Administrator, ADMIN1. <ul style="list-style-type: none"> <li>• Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben:               <pre>grant authority admin1 classes=system</pre> </li> <li>• Entziehen Sie dem Administrator die Systemberechtigung, indem Sie den folgenden Befehl ausgeben:               <pre>revoke authority admin1 classes=system</pre> </li> </ul>  |
| Administratoren entfernen                       | Entfernen Sie einen Administrator, ADMIN1, sodass er nicht mehr auf den IBM Spectrum Protect-Server zugreifen kann, indem Sie den folgenden Befehl ausgeben: <pre>remove admin admin1</pre>  |
| Zugriff auf den Server vorübergehend verhindern | Sperren oder entsperren Sie einen Administrator, indem Sie den Befehl LOCK ADMIN bzw. UNLOCK ADMIN verwenden.  |

## Kennwortanforderungen ändern

Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.



## Informationen zu diesem Vorgang

Indem Sie die Kennwortauthentifizierung durchsetzen und Kennworteinschränkungen verwalten, können Sie Ihre Daten und Ihre Server vor möglichen Sicherheitsrisiken schützen.

## Vorgehensweise

Führen Sie die folgenden Tasks aus, um Kennwortanforderungen für IBM Spectrum Protect-Server zu ändern.

Tabelle 1. Authentifizierungstasks für IBM Spectrum Protect-Server

| Task  | Prozedur   |
|---|--|
| Grenzwert für ungültige Kennworteingabeversuche festlegen | <ol style="list-style-type: none"><li>Wählen Sie auf der Seite Server im Operations Center den Server aus.</li><li>Klicken Sie auf Details und dann auf die Registerkarte Merkmale.</li><li>Geben Sie die Anzahl ungültiger Versuche im Feld Grenzwert für ungültige Anmeldeversuche an.</li></ol> <p>Der Standardwert bei der Installation ist 0.</p>   |
| Mindestlänge für Kennwörter festlegen                     | <ol style="list-style-type: none"><li>Wählen Sie auf der Seite Server im Operations Center den Server aus.</li><li>Klicken Sie auf Details und dann auf die Registerkarte Merkmale.</li><li>Geben Sie die Anzahl Zeichen im Feld Mindestlänge für Kennwort an.</li></ol>   |
| Ablaufzeitraum für Kennwörter festlegen                   | <ol style="list-style-type: none"><li>Wählen Sie auf der Seite Server im Operations Center den Server aus.</li><li>Klicken Sie auf Details und dann auf die Registerkarte Merkmale.</li><li>Geben Sie die Anzahl Tage im Feld Allgemeine Kennwortablaufdauer an.</li></ol>   |
| Kennwortauthentifizierung inaktivieren                    | <p>Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer ein Kennwort eingeben, um auf den Server zugreifen zu können.</p> <p>Sie können die Kennwortauthentifizierung nur für Kennwörter inaktivieren, die mit dem Server (LOCAL) authentifiziert werden. Durch das Inaktivieren der Kennwortauthentifizierung erhöht sich das Sicherheitsrisiko für den Server.</p> |
| Standardauthentifizierungsmethode festlegen               | <p>Geben Sie den Befehl SET DEFAULTAUTHENTICATION aus. Um beispielsweise den Server als die Standardauthentifizierungsmethode zu verwenden, geben Sie den folgenden Befehl aus:</p> <pre>set defaultauthentication local</pre> <p>Um einen Clientknoten für die Authentifizierung mit dem Server zu aktualisieren, schließen Sie AUTHENTICATION=LOCAL in den Befehl UPDATE NODE ein:</p> <pre>update node authentication=local</pre>                 |

### Zugehörige Konzepte:

- IBM Spectrum Protect-Benutzer mithilfe eines LDAP-Servers authentifizieren
- Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1)

## IBM Spectrum Protect auf dem System schützen

Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

## Vorgehensweise

Stellen Sie sicher, dass nicht berechtigte Benutzer nicht auf die Verzeichnisse für die Serverdatenbank und die Serverinstanz zugreifen können. Behalten Sie die Zugriffseinstellungen für diese Verzeichnisse bei, die Sie während der Implementierung konfiguriert haben.

- Benutzerzugriff auf den Server einschränken  
Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.
- Zugriff über Porteinschränkungen einschränken  
Schränken Sie den Zugriff auf den Server ein, indem Sie Porteinschränkungen anwenden.

## Benutzerzugriff auf den Server einschränken

Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

## Vorgehensweise

1. Nachdem Sie einen Administrator mit dem Befehl REGISTER ADMIN registriert haben, legen Sie die Berechtigungsstufe des Administrators mithilfe des Befehls GRANT AUTHORITY fest. Ausführliche Informationen zum Festlegen und Ändern der Berechtigung finden Sie in Administratoren verwalten.
2. Um die Berechtigung eines Administrators zur Ausführung bestimmter Tasks zu steuern, verwenden Sie die beiden folgenden Serveroptionen:
  - a. Über die Serveroption QUERYAUTH können Sie die Berechtigungsstufe auswählen, die ein Administrator haben muss, um Befehle QUERY und SELECT ausgeben zu können. Standardmäßig ist keine Berechtigungsstufe erforderlich. Sie können die Anforderung in eine der Berechtigungsstufen, einschließlich Systemberechtigung, ändern.
  - b. Über die Serveroption REQSYSAUTHOUTFILE können Sie angeben, dass Systemberechtigung für Befehle erforderlich ist, die zur Folge haben, dass der Server Daten in eine externe Datei schreibt. Standardmäßig ist für diese Befehle Systemberechtigung erforderlich.
3. Sie können die Datensicherung auf einem Clientknoten ausschließlich auf Rootbenutzer-IDs oder berechtigte Benutzer beschränken. Um beispielsweise Sicherungen auf die Rootbenutzer-ID zu beschränken, geben Sie den Befehl REGISTER NODE oder UPDATE NODE unter Angabe des Parameters BACKUPINITIATION=root aus:

```
update node backupinitiation=root
```

## Zugriff über Porteinschränkungen einschränken

Schränken Sie den Zugriff auf den Server ein, indem Sie Porteinschränkungen anwenden.

## Informationen zu diesem Vorgang

Gegebenenfalls müssen Sie abhängig von Ihren Sicherheitsanforderungen den Zugriff auf bestimmte Server einschränken. Der IBM Spectrum Protect-Server kann so konfiguriert werden, dass er an vier TCP/IP-Ports empfangsbereit ist: zwei Ports, die für reguläre TCP/IP-Protokolle oder SSL-/TLS-Protokolle verwendet werden können, und zwei Ports, die nur für das SSL-/TLS-Protokoll verwendet werden können.

## Vorgehensweise

Sie können die Serveroptionen wie in Tabelle 1 aufgeführt zur Angabe des erforderlichen Ports festlegen.

Tabelle 1. Serveroptionen und Portzugriff

| Serveroption | Portzugriff  |
|--------------|--|
| TCPSPORT     | Gibt die Nummer des Ports an, dem der TCP/IP-DFV-Treiber des Servers auf Anforderungen von Clientsitzungen warten soll. Dieser Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen empfangsbereit. Der Standardwert ist 1500.  |
| TCPADMINPORT | Gibt die Nummer des Ports an, an dem der TCP/IP-DFV-Treiber des Servers auf Anforderungen von anderen Sitzungen als Clientsitzungen warten soll. Dieser Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen empfangsbereit. Der Standardwert ist der Wert für TCPSPORT.<br><br>Verwenden Sie diese Option, um den Datenverkehr des Verwaltungsclients vom Datenverkehr des regulären Clients, der die Optionen TCPSPORT und SSLTCPSPORT verwendet, zu trennen. |

| Serveroption    | Portzugriff   |
|-----------------|---|
| SSLTCPPORT      | Gibt die SSL-TCP/-IP-Portadresse für einen Server an. Dieser Port ist nur für SSL-fähige Sitzungen empfangsbereit. Ein Standardwert für den Port ist nicht verfügbar.   |
| SSLTCPADMINPORT | Gibt die Portadresse an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen von SSL-fähigen Sitzungen wartet. Ein Standardwert für den Port ist nicht verfügbar.<br><br>Verwenden Sie diese Option, um den Datenverkehr des Verwaltungsclients vom Datenverkehr des regulären Clients, der die Optionen TCPPOINT und SSLTCPPORT verwendet, zu trennen. |

Einschränkungen:

Wenn Sie die Server-Ports, die nur für SSL gelten, (SSLTCPPORT und SSLTCPADMINPORT) angeben, gelten die folgenden Einschränkungen:

- Wenn Sie den Server-Port, der nur für SSL gilt, für den Parameter LLADDRESS im Befehl DEFINE SERVER oder im Befehl UPDATE SERVER angeben, müssen Sie auch den Parameter SSL=YES angeben.
- Wenn Sie den Server-Port, der nur für SSL gilt, für die Clientoption TCPPOINT angeben, müssen Sie auch YES für die SSL-Clientoption angeben.

**Zugehörige Verweise:**

Planung des Firewallzugriffs

## Server stoppen und starten

Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.

### Vorbereitende Schritte

Um den IBM Spectrum Protect-Server stoppen und starten zu können, müssen Sie über System- oder Bedienerberechtigung verfügen.

- **Server stoppen**  
Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.
- **Server für Verwaltungs- oder Rekonfigurationstasks starten**  
Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

## Server stoppen

Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.

### Informationen zu diesem Vorgang

Wenn Sie den Befehl HALT zum Stoppen des Servers ausgeben, werden die folgenden Aktionen ausgeführt:

- Alle Prozesse und Clientknotensitzungen werden abgebrochen.
- Alle aktuellen Transaktionen werden gestoppt. (Die Transaktionen werden rückgängig gemacht, wenn der Server erneut gestartet wird.)

### Vorgehensweise

Um das System vorzubereiten und den Server zu stoppen, führen Sie die folgenden Schritte aus:

1. Verhindern Sie, dass neue Clientknotensitzungen gestartet werden, indem Sie den Befehl DISABLE SESSIONS ausgeben:

```
disable sessions all
```

2. Bestimmen Sie, ob Clientknotensitzungen oder -prozesse aktiv sind, indem Sie die folgenden Schritte ausführen:
  - a. Rufen Sie die Seite Übersicht im Operations Center auf, auf der im Bereich Aktivität die Gesamtzahl Prozesse und Sitzungen angezeigt wird, die derzeit aktiv sind. Wenn die Zahlen erheblich von den Zahlen abweichen, die normalerweise während

- Ihrer täglichen Speicherverwaltungsroutine angezeigt werden, überprüfen Sie mithilfe weiterer Statusanzeiger im Operations Center, ob ein Problem vorliegt.
- b. Zeigen Sie das Diagramm im Bereich Aktivität an, um den Umfang des Datenaustauschs im Netz für die folgenden Perioden zu vergleichen:
- Die laufende Periode, d. h. die letzte 24-Stunden-Periode
  - Die vorherige Periode, d. h. die 24 Stunden vor der laufenden Periode
- Wenn das Diagramm für die vorherige Periode den erwarteten Umfang des Datenaustauschs darstellt, können deutliche Abweichungen in dem Diagramm für die laufende Periode auf ein Problem hindeuten.
- c. Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details. Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, rufen Sie mithilfe von Verwaltungsbefehlen Informationen zu Prozessen ab. Geben Sie den Befehl QUERY PROCESS aus, um Prozesse abzufragen; geben Sie den Befehl QUERY SESSION aus, um Informationen zu Sitzungen abzurufen.
3. Warten Sie, bis die Clientknotensitzungen abgeschlossen sind oder brechen Sie diese ab. Um Prozesse und Sitzungen abzubrechen, führen Sie die folgenden Schritte aus:
- Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details.
  - Klicken Sie auf die Registerkarte Aktive Tasks und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
  - Klicken Sie auf Abbrechen.
  - Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, brechen Sie Sitzungen mithilfe von Verwaltungsbefehlen ab. Geben Sie den Befehl CANCEL SESSION aus, um eine Sitzung abzubrechen; geben Sie den Befehl CANCEL PROCESS aus, um Prozesse abzubrechen.
- Tipp: Wenn der Prozess, der abgebrochen werden soll, auf die Bereitstellung eines Banddatenträgers wartet, wird die Mountainforderung abgebrochen. Wenn Sie beispielsweise einen Befehl EXPORT, IMPORT oder MOVE DATA ausgeben, leitet der Befehl möglicherweise einen Prozess ein, der die Bereitstellung eines Banddatenträgers erfordert. Wenn jedoch ein Banddatenträger durch ein automatisiertes Speicherarchiv bereitgestellt wird, wird die Abbruchoperation unter Umständen erst wirksam, wenn der Bereitstellungsprozess abgeschlossen ist. Abhängig von Ihrer Systemumgebung kann dies mehrere Minuten dauern.
4. Stoppen Sie den Server, indem Sie den Befehl HALT ausgeben:

```
halt
```

## Server für Verwaltungs- oder Rekonfigurationstasks starten

---

Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

### Informationen zu diesem Vorgang

---

Starten Sie den Server im Verwaltungsmodus, indem Sie das Dienstprogramm DSMSERV mit dem Parameter MAINTENANCE ausführen.

Im Verwaltungsmodus sind die folgenden Operationen inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Konsolidierung von Speicherbereich auf dem Server
- Bestandsverfall
- Umlagerung von Speicherpools

Darüber hinaus wird verhindert, dass Clients Sitzungen mit dem Server starten können.

Tipps:

- Sie müssen die Serveroptionsdatei, dsmserve.opt, nicht editieren, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Speicherbereichskonsolidierung, den Bestandsverfall und Umlagerungsprozesse für Speicherpools manuell starten.

### Vorgehensweise

---

Um den Server im Verwaltungsmodus zu starten, geben Sie den folgenden Befehl aus:

```
dsmserve maintenance
```

Tipp: Informationen zum Anzeigen eines Ein Video zum Starten des Servers im Verwaltungsmodus kann über Server im Verwaltungsmodus starten angezeigt werden.




## Nächste Schritte

---

Um Serveroperationen im Produktionsmodus wiederaufzunehmen, führen Sie die folgenden Schritte aus:

1. Fahren Sie den Server herunter, indem Sie den Befehl HALT ausgeben:

```
halt
```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden. Führen Sie die Anweisungen für Ihr Betriebssystem aus:
  -  AIX-BetriebssystemeServerinstanz starten
  -  Linux-BetriebssystemeServerinstanz starten
  -  Windows-BetriebssystemeServerinstanz starten

Operationen, die im Verwaltungsmodus inaktiviert waren, werden wieder aktiviert.

## Durchführung eines Upgrades für den Server planen

---

Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.

### Informationen zu diesem Vorgang

---

Beachten Sie diese Richtlinien:

- Bei der bevorzugten Methode erfolgt das Upgrade für den Server mithilfe des Installationsassistenten. Nachdem Sie den Assistenten gestartet haben, klicken Sie im Fenster IBM Installation Manager auf das Symbol zum Aktualisieren; klicken Sie nicht auf das Symbol zum Installieren oder Ändern!
- Wenn sowohl für die Serverkomponente als auch für die Operations Center-Komponente Upgrades verfügbar sind, wählen Sie die Kontrollkästchen aus, um das Upgrade für beide Komponenten durchzuführen.

### Vorgehensweise




---

1. Überprüfen Sie die Liste der Fixpacks und vorläufigen Fixes. Siehe Technote 1239415.
2. Studieren Sie die Produktverbesserungen, die in der Readme-Datei beschrieben sind.  
Tipp: Wenn Sie die Installationspaketdatei von der IBM Spectrum Protect-Unterstützungsseite abrufen, können Sie auch auf die Readme-Datei zugreifen.
3. Stellen Sie sicher, dass die Version, auf die das Upgrade für Ihren Server durchgeführt wird, mit anderen Komponenten, wie beispielsweise Speicheragenten und Speicherarchivclients, kompatibel ist. Siehe Technote 1302789.
4. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden. Siehe Technote 1053218.
5. Lesen Sie die Upgradeanweisungen. Stellen Sie sicher, dass Sie die Serverdatenbank, die Einheitenkonfigurationsinformationen und die Protokolldatei für Datenträger sichern.

## Nächste Schritte

---

Um ein Fixpack oder einen vorläufigen Fix zu installieren, führen Sie die Anweisungen für Ihr Betriebssystem aus:

-  AIX-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
-  Linux-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
-  Windows-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren

#### Zugehörige Informationen:

 [Upgrade- und Umlagerungsprozess - Häufig gestellte Fragen](#)

## Vorbereitungen für einen Ausfall oder eine Systemaktualisierung

---

Treffen Sie Vorbereitungen in IBM Spectrum Protect, damit Ihr System während eines geplanten Stromausfalls oder einer geplanten Systemaktualisierung in einem konsistenten Zustand verbleibt.

### Informationen zu diesem Vorgang

---

Stellen Sie sicher, dass Sie die regelmäßige Ausführung von Aktivitäten planen, um den Server zu verwalten und zu schützen.

## Vorgehensweise

---

1. Brechen Sie Prozesse und Sitzungen, die aktiv sind, ab, indem Sie die folgenden Schritte ausführen:
  - a. Wählen Sie im Operations Center auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details.
  - b. Klicken Sie auf die Registerkarte Aktive Tasks und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
  - c. Klicken Sie auf Abbrechen.
2. Stoppen Sie den Server, indem Sie den Befehl HALT ausgeben:

halt

Tipp: Sie können den Befehl HALT im Operations Center ausgeben, indem Sie den Mauszeiger über das Symbol für Einstellungen bewegen und auf Command Builder klicken. Wählen Sie dann den Server aus, geben Sie `halt` ein und drücken Sie die Eingabetaste.

## Plan zur Wiederherstellung nach einem Katastrophenfall implementieren

---

Implementieren Sie eine Strategie zur Wiederherstellung nach einem Katastrophenfall, um Ihre Anwendungen in einem Katastrophenfall wiederherstellen und hohe Serververfügbarkeit sicherstellen zu können.

### Informationen zu diesem Vorgang

---

Bestimmen Sie Ihre Anforderungen für die Wiederherstellung nach einem Katastrophenfall, indem Sie die Geschäftsprioritäten für die Clientknotenwiederherstellung und die Systeme, die zum Wiederherstellen von Daten verwendet werden, angeben und prüfen, ob Clientknoten über eine Verbindung zu einem Wiederherstellungsserver verfügen. Verwenden Sie zum Schützen von Daten Replikation und Speicherpoolschutz. Außerdem müssen Sie bestimmen, wie oft Verzeichniscontainerspeicherpools geschützt werden.

- Wiederherstellungsdrilloperationen ausführen  
Planen Sie Drilloperationen für die Wiederherstellung nach einem Katastrophenfall als Vorbereitung für Prüfungen, mit denen die Wiederherstellbarkeit des IBM Spectrum Protect-Servers bestätigt wird, und um sicherzustellen, dass nach einem Ausfall Daten zurückgeschrieben und Operationen wiederaufgenommen werden können. Mithilfe einer Drilloperation können Sie außerdem vor dem Eintreten einer kritischen Situation sicherstellen, dass alle Daten zurückgeschrieben und Operationen wiederaufgenommen werden können.

## Wiederherstellung nach einem Datenverlust oder Systemausfall

---

Mithilfe von IBM Spectrum Protect können Sie Daten wiederherstellen, die bei einem Katastrophenfall oder Systemausfall verloren gegangen sind. Sie können Verzeichniscontainerspeicherpools, Clientdaten und Datenbanken wiederherstellen.

### Vorbereitende Schritte

---

Planen Sie Client- und Server-Workloads, um die beste Leistung für Ihre Speicherumgebung zu erzielen. Geben Sie die Befehle PROTECT STGPOOL und REPLICATE NODE im Rahmen des Zeitplans aus. Schützen Sie den Speicherpool vor dem Replizieren des Clientknotens. Wenn die Knotenreplikation gestartet wird, werden die Datenbereiche, die bereits durch den Speicherpoolschutz repliziert werden, übersprungen und die Replikationsverarbeitungszeit wird somit reduziert.

## Vorgehensweise

---

Verwenden Sie abhängig von der Komponente, die wiederhergestellt werden muss, die folgenden Wiederherstellungsmethoden.

| Wiederherzustellende Komponente | Prozedur | Weitere Informationen |
|---------------------------------|----------|-----------------------|
|---------------------------------|----------|-----------------------|

| <b>Wiederherzustellende Komponente</b> | <b>Prozedur</b>  | <b>Weitere Informationen</b> |
|--|--|------------------------------|
| Verzeichniscontainerspeicherpool       | <p>Um Verzeichniscontainerspeicherpools wiederherzustellen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>a. Suchen Sie in dem Verzeichniscontainerspeicherpool nach beschädigten Datenbereichen, indem Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=SCANALL ausgeben.</li> <li>b. Reparieren Sie beschädigte Datenbereiche in dem Verzeichniscontainerspeicherpool mit dem Befehl REPAIR STGPOOL.<br/>Einschränkung: Sie können einen Speicherpool nur reparieren, wenn der Speicherpool geschützt wird.</li> <li>c. Entfernen Sie beschädigte Datenbereiche, indem Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=REMOVEDAMAGED ausgeben.</li> </ol> | Speicherpools reparieren     |



| Wiederherzustellende Komponente | Prozedur  | Weitere Informationen  |
|---------------------------------|---|--|
| Clientdaten                     | <p>Voraussetzungen:</p> <ul style="list-style-type: none"> <li>• Der Quellenreplikationsserver, der Zielreplikationsserver und der Client müssen Version 7.1 oder höher haben. Wenn einer der Server eine frühere Version hat, wird die automatische Übernahme inaktiviert und Sie müssen die Übernahme manuell ausführen.</li> </ul> <p>Konfigurieren Sie den Client für die automatische Übernahme durch den Zielservers für die Datenwiederherstellung.</p> <p>Wenn der Client für die automatisierte Clientübernahme aktiviert wurde, können Sie die Daten mithilfe der Funktion für die automatische Übernahme wiederherstellen. Überprüfen Sie, ob die Option <code>usereplicationfailover</code> in der Clientoptionsdatei entweder nicht vorhanden ist oder auf <code>yes</code> gesetzt ist. Stellen Sie mithilfe der automatischen Übernahme Daten vom Zielservers wieder her, wenn der Quellenserver aufgrund eines Ausfalls nicht verfügbar ist.</p> <p>Tipp:</p> <ul style="list-style-type: none"> <li>• Geben Sie mit dem Befehl <code>SET FAILOVERHLADDRESS</code> die IP-Adresse für den Replikationsserver während der Übernahme an, wenn die Adresse nicht mit der IP-Adresse übereinstimmt, die für den Replikationsprozess angegeben ist.</li> </ul> | <ul style="list-style-type: none"> <li>• Beschädigte Daten aus einer replizierten Kopie wiederherstellen</li> <li>• <code>SET FAILOVERHLADDRESS</code> (Adresse höherer Ebene für Übernahme definieren)</li> </ul> |



| Wiederherzustellende Komponente | Prozedur  | Weitere Informationen                          |
|---------------------------------|---|--|
| Datenbank                       | <p>Voraussetzungen:</p> <ul style="list-style-type: none"> <li>Um die Datenbank nach einem Katastrophenfall zurückzuschreiben, muss eine Kopie der aktuellen Einheitenkonfigurationsdatei vorhanden sein. Die Einheitenkonfigurationsdatei kann nicht erneut erstellt werden.</li> <li>Stellen Sie sicher, dass eine gesicherte Version der Datenbank vorhanden ist.</li> </ul> <p>Schreiben Sie die IBM Spectrum Protect-Datenbank mit dem neuesten Stand oder mit dem Stand eines bestimmten Zeitpunkts unter Verwendung des Serverdienstprogramms DSMSERV RESTORE DB zurück.</p> | DSMSERV RESTORE DB (Datenbank zurückschreiben) |

- **Datenbank zurückschreiben**  
Unter Umständen müssen Sie die IBM Spectrum Protect-Datenbank nach einem Katastrophenfall zurückschreiben. Sie können die Datenbank mit dem neuesten Stand oder mit dem Stand eines angegebenen Zeitpunkts zurückschreiben. Zum Zurückschreiben der Datenbank benötigen Sie Datenträger mit einer Datenbankgesamt-, -teil- oder -momentaufnahmesicherung.
- **Beschädigte Daten aus einer replizierten Kopie wiederherstellen**  
Wenn ein Quellenreplikationsserver nicht verfügbar ist, können Sie beschädigte Daten aus einer replizierten Kopie, die auf dem Zielreplikationsserver gespeichert ist, wiederherstellen.
- **Speicherpools reparieren**  
Bei einer Katastrophe oder einem Systemausfall können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool reparieren.

#### Zugehörige Verweise:

-  [AUDIT CONTAINER \(Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen\)](#)
-  [DSMSERV RESTORE DB \(Datenbank zurückschreiben\)](#)

## Datenbank zurückschreiben

---

Unter Umständen müssen Sie die IBM Spectrum Protect-Datenbank nach einem Katastrophenfall zurückschreiben. Sie können die Datenbank mit dem neuesten Stand oder mit dem Stand eines angegebenen Zeitpunkts zurückschreiben. Zum Zurückschreiben der Datenbank benötigen Sie Datenträger mit einer Datenbankgesamt-, -teil- oder -momentaufnahmesicherung.

## Vorbereitende Schritte

---

Wenn die Verzeichnisse für die Datenbank und das Wiederherstellungsprotokoll nicht mehr vorhanden sind, erstellen Sie diese erneut, bevor Sie das Serverdienstprogramm DSMSERV RESTORE DB verwenden. Verwenden Sie beispielsweise die folgenden Befehle:

 **AIX-Betriebssysteme**  **Linux-Betriebssysteme**

```
mkdir /tsmdb001
mkdir /tsmdb002
mkdir /tsmdb003
mkdir /activeolog
mkdir /archlog
mkdir /archfaillog
```

 **Windows-Betriebssysteme**

```
mkdir e:\tsm\db001
mkdir f:\tsm\db001
mkdir g:\tsm\db001
mkdir h:\tsm\activeolog
```

```
mkdir i:\tsm\archlog
mkdir j:\tsm\archfaillog
```

Einschränkungen:

- Um die Datenbank mit der neuesten Version zurückzuschreiben, müssen Sie das Archivprotokollverzeichnis lokalisieren. Wenn Sie das Verzeichnis nicht lokalisieren können, kann die Datenbank nur mit dem Stand eines bestimmten Zeitpunkts zurückgeschrieben werden.
- Sie können Secure Sockets Layer (SSL) nicht für Datenbankzurückschreibungsoperationen verwenden.
- Wenn der Release-Level der Datenbanksicherung und der Release-Level des Servers, für den die Zurückschreibung erfolgt, unterschiedlich sind, können Sie die Serverdatenbank nicht zurückschreiben. Wenn Sie beispielsweise einen Server der Version 8.1 verwenden und versuchen, eine Datenbank der Version 7.1 zurückzuschreiben, tritt ein Fehler auf.

## Informationen zu diesem Vorgang

---

Operationen für die Zurückschreibung nach Zeitpunkt werden normalerweise bei der Wiederherstellung nach einem Katastrophenfall oder zum Entfernen der Auswirkungen von Fehlern verwendet, die Inkonsistenzen in der Datenbank zur Folge haben können. Um die Datenbank mit dem Stand wiederherzustellen, den sie zu dem Zeitpunkt hatte, zu dem sie verloren ging, stellen Sie die Datenbank mit der neuesten Version wieder her.

## Vorgehensweise

---

Verwenden Sie das Serverdienstprogramm DSMSERV RESTORE DB, um die Datenbank zurückzuschreiben. Wählen Sie abhängig von der Version der Datenbank, die zurückgeschrieben werden soll, eine der folgenden Methoden aus:

- Zurückschreiben einer Datenbank mit der neuesten Version. Verwenden Sie beispielsweise den folgenden Befehl:

```
dsmserv restore db
```

- Zurückschreiben einer Datenbank mit dem Stand eines bestimmten Zeitpunkts. Um beispielsweise die Datenbank mit einer Sicherungsserie zurückzuschreiben, die am 19. April 2015 erstellt wurde, verwenden Sie den folgenden Befehl:

```
dsmserv restore db todate=04/19/2015
```

## Nächste Schritte

---

Wenn Sie die Datenbank zurückgeschrieben haben und Verzeichniscontainerspeicherpools auf dem Server vorhanden sind, müssen Sie Inkonsistenzen zwischen der Datenbank und dem Dateisystem ermitteln.

1. Wenn Sie die Datenbank mit dem Stand eines bestimmten Zeitpunkts zurückgeschrieben haben und die Wiederverwendung des Verzeichniscontainerspeicherpools nicht verzögert wurde, müssen Sie alle Container prüfen. Um alle Container zu prüfen, geben Sie den folgenden Befehl aus:

```
audit container stgpool
```

2. Wenn der Server keine Container auf dem System identifizieren kann, führen Sie die folgenden Schritte aus, um eine Liste der Container anzuzeigen:

- a. Geben Sie über einen Verwaltungsclient den folgenden Befehl aus:

```
select container_name from containers
```

- b. Geben Sie für das Dateisystem den folgenden Befehl für das Speicherpoolverzeichnis auf dem Quellenserver aus:

Tipp: Das Speicherpoolverzeichnis wird in der Befehlsausgabe angezeigt:

```
 AIX-Betriebssysteme  Linux-Betriebssysteme
```

```
[Root@Quelle]$ ls -lR
```

```
 Windows-Betriebssysteme
```

```
c:\Quellenspeicherpoolverz>Verz /s
```

- c. Vergleichen Sie die für das Dateisystem und den Server aufgelisteten Container.
- d. Geben Sie den Befehl AUDIT CONTAINER unter Angabe des Containers aus, der in der Serverausgabe fehlt. Geben Sie den Parameter ACTION=REMOVEDAMAGED an, um den Container zu löschen.
- e. Um sicherzustellen, dass die Container im Dateisystem gelöscht wurden, überprüfen Sie die angezeigten Nachrichten.  
Tipp: Der IBM Spectrum Protect-Server erkennt keine Container, die nach der letzten Datenbanksicherung erstellt wurden. Löschen Sie die Dateien, die verglichen mit den Dateien auf dem IBM Spectrum Protect-Server zusätzlich in Ihrem lokalen Dateisystem vorhanden sind.

**Zugehörige Tasks:**

☞ Clientknotendaten nach einer Datenbankzurückschreibung replizieren (Version 7.1.1)

**Zugehörige Verweise:**

☞ AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)

☞ DSMSEV RESTORE DB (Datenbank zurückschreiben)

## Beschädigte Daten aus einer replizierten Kopie wiederherstellen

---

Wenn ein Quellenreplikationsserver nicht verfügbar ist, können Sie beschädigte Daten aus einer replizierten Kopie, die auf dem Zielreplikationsserver gespeichert ist, wiederherstellen.

### Vorbereitende Schritte

---

Der Servername, den Sie im Befehl SET REPLSERVER angeben, muss mit dem Namen einer vorhandenen Serverdefinition übereinstimmen. Außerdem muss es sich um den Namen des Servers handeln, der als Zielreplikationsserver verwendet werden soll. Wenn der in diesem Befehl angegebene Servername nicht mit dem Servernamen einer vorhandenen Serverdefinition übereinstimmt, schlägt der Befehl fehl.

Tipp:

- Gehen Sie beim Ändern oder Entfernen eines Zielreplikationsservers mit Sorgfalt vor. Wenn Sie einen Zielreplikationsserver ändern, werden Clientknotendaten, die repliziert werden, an einen anderen Zielreplikationsserver gesendet. Wenn Sie einen Zielreplikationsserver entfernen, werden Clientknotendaten nicht repliziert.

### Vorgehensweise

---

1. Überprüfen Sie den Replikationsstatus der Daten auf dem Zielsystem. Der Replikationsstatus gibt an, ob die neueste Sicherung auf den sekundären Server repliziert wurde.
2. Schreiben Sie Daten von einem Zielreplikationsserver zurück, indem Sie den Quellenreplikationsserver als Zielreplikationsserver festlegen. Wenn beispielsweise der Quellenreplikationsserver als Zielreplikationsserver server1 festgelegt werden soll, geben Sie den folgenden Befehl aus:

```
set replserver server1
```

### Nächste Schritte

---

Wenn Sie die IBM Spectrum Protect-Datenbank auf einen Quellenreplikationsserver zurückschreiben, wird die Replikation automatisch inaktiviert. Bevor Sie die Replikation erneut aktivieren, müssen Sie bestimmen, ob Kopien der Daten, die sich auf dem Zielreplikationsserver befinden, benötigt werden.

**Zugehörige Tasks:**

☞ Clientknotendaten nach einer Datenbankzurückschreibung replizieren (Version 7.1.1)

## Speicherpools reparieren

---

Bei einer Katastrophe oder einem Systemausfall können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool reparieren.

### Vorbereitende Schritte

---

Identifizieren Sie Inkonsistenzen zwischen der Datenbank und dem Verzeichniscontainerspeicherpool mit dem Befehl AUDIT CONTAINER. Indem Sie beschädigte Datenbereiche im Verzeichniscontainerspeicherpool identifizieren, können Sie die zu reparierenden Datenbereiche bestimmen.

Bevor Sie einen Speicherpool reparieren können, müssen Sie mithilfe des Befehls PROTECT STGPOOL sicherstellen, dass der Speicherpool geschützt wird.

### Vorgehensweise

---

1. Verwenden Sie zum Reparieren eines Verzeichniscontainerspeicherpools den Befehl REPAIR STGPOOL. Um beispielsweise den Speicherpool STGPOOL1 zu reparieren, geben Sie den folgenden Befehl aus:

```
repair stgpool stgpool1
```

2. Wenn der beschädigte Speicherpool im Befehl PROTECT STGPOOL für einen oder mehrere Quellenspeicherpools als Zielspeicherpool angegeben ist, geben Sie den Befehl PROTECT STGPOOL für alle Quellenspeicherpools aus.

3. Um sicherzustellen, dass alle beschädigten Daten mithilfe anderer Quellenspeicherpools identifiziert und repariert werden, geben Sie den Befehl PROTECT STGPOOL erneut für alle Quellenspeicherpools unter Angabe des Parameters FORCERECONCILE=YES aus.
4. Um Objekte zu entfernen, die sich auf beschädigte Daten beziehen, geben Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=REMOVEDAMAGED aus.
5. Wenn es sich bei dem beschädigten Speicherpool um einen Zielspeicherpool für die Knotenreplikation von einem oder mehreren Quellenservern handelt, geben Sie den Befehl REPLICATE NODE erneut auf allen Quellenservern aus.
6. Geben Sie, nachdem die Beschädigung repariert wurde, den Befehl PROTECT STGPOOL aus, um sicherzustellen, dass der Speicherpool in einem anderen Verzeichniscontainerspeicherpool geschützt wird.

## Nächste Schritte

---

Stellen Sie durch Ausgabe des Befehls QUERY DAMAGED sicher, dass keine beschädigten Datenbereiche in der Ausgabe angezeigt werden.

### Zugehörige Verweise:

- ☞ Daten in Verzeichniscontainerspeicherpools reparieren und wiederherstellen
- ☞ AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)
- ☞ QUERY DAMAGED (Beschädigte Daten in einem Verzeichniscontainer- oder Cloud-Containerspeicherpool abfragen)
- ☞ REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)

## Bandspeicherlösung

---

Diese Datenschutzlösung stellt Speicher für Banddatenträger bereit, eine flexible und kosteneffiziente Option für die langfristige Aufbewahrung von Daten.

- Planung für eine bandbasierte Datenschutzlösung  
Führen Sie die Planung für eine Datenschutzlösung durch, die Platte-Platte-Band-Sicherungsoperationen und Sicherungsoperationen von Platte auf Band zur Optimierung des Speichers umfasst.
- Implementierung einer bandbasierten Datenschutzlösung  
Implementieren Sie die bandbasierte Lösung, die die Platte-Platte-Band-Sicherung und Plattenstaging zur Optimierung des Speichers verwendet. Durch die Implementierung der Bandspeicherlösung können Sie die langfristige Aufbewahrung von Daten ermöglichen und kostengünstige Skalierbarkeit erzielen.
- Bandspeicherlösung überwachen  
Überwachen Sie nach der Implementierung einer bandbasierten Lösung in IBM Spectrum Protect die Lösung, um ihre korrekte Funktionsweise sicherzustellen. Indem die Lösung täglich und regelmäßig überwacht wird, können Sie bestehende und potenzielle Probleme erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden.
- Operationen für eine Bandspeicherlösung verwalten  
Verwenden Sie diese Informationen, um Operationen für eine Bandspeicherimplementierung für einen IBM Spectrum Protect-Server zu verwalten.

## Planung für eine bandbasierte Datenschutzlösung

---

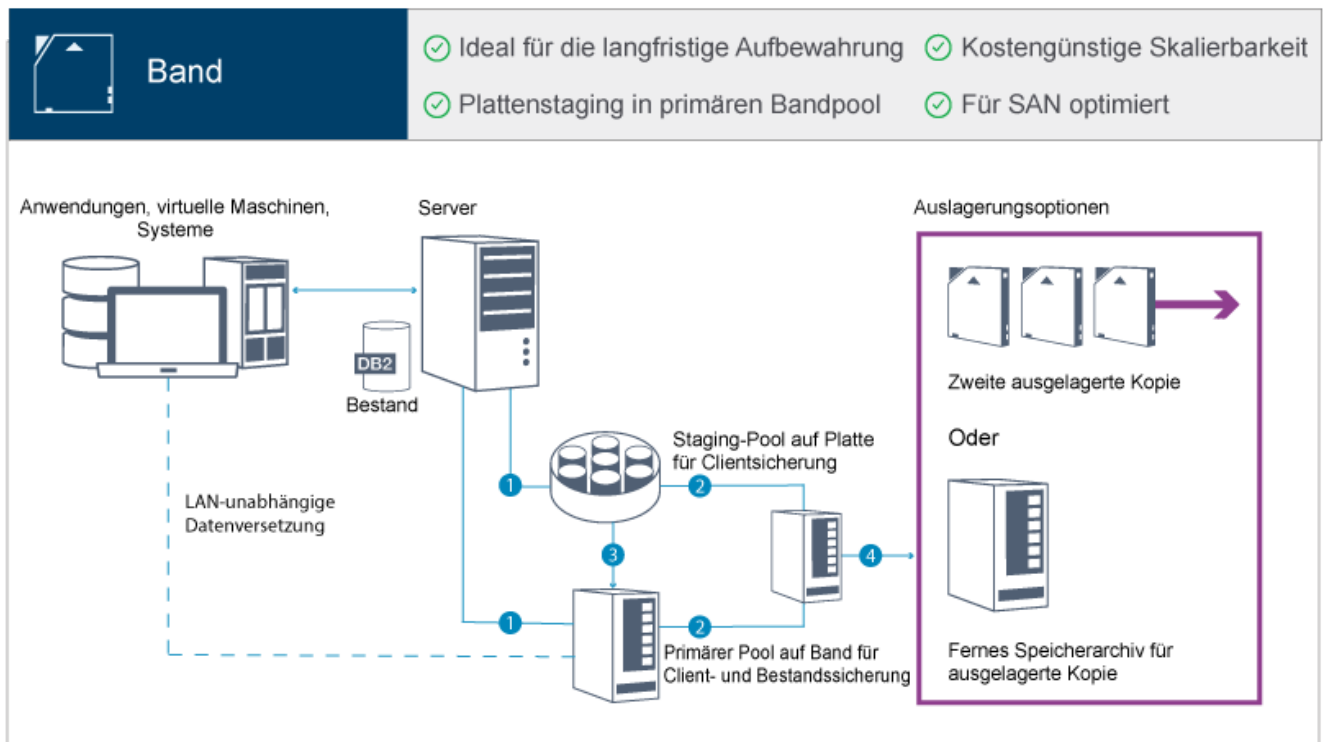
Führen Sie die Planung für eine Datenschutzlösung durch, die Platte-Platte-Band-Sicherungsoperationen und Sicherungsoperationen von Platte auf Band zur Optimierung des Speichers umfasst.

### Planungsroadmap

---

Führen Sie die Planung für die Bandspeicherlösung durch, indem Sie das Architekturlayout in Abbildung 1 überprüfen und dann die Roadmap-Tasks ausführen, die auf die Abbildung folgen.

Abbildung 1. Bandspeicherlösung



Bei dieser Datenschutzkonfiguration verwendet der Server sowohl Platten- als auch Bandspeicherhardware. Es wird Speicherpoolstaging verwendet, bei dem Clientdaten anfänglich in Plattenspeicherpools gespeichert und dann später in Bandspeicherpools umgelagert werden. Für die Wiederherstellung nach einem Katastrophenfall können Banddatenträger an einem anderen Standort gespeichert werden. Auslagerungsoptionen umfassen den physischen Transport einer zweiten Kopie an einen anderen Standort durch einen Kurier oder das Schützen von Kopien an einem anderen Standort durch elektronisches Vaulting in einem fernen Speicherarchiv.

Tipp: Die beschriebene Lösung umfasst keine Knotenreplikation. Wenn die Knotenreplikation jedoch zum Sichern eines Speicherpools von Platte auf Platte verwendet werden soll, müssen Sie sicherstellen, dass die Replikationsoperation abgeschlossen ist, bevor Daten von Platte auf Band umgelagert werden. Sie können die Knotenreplikation auch verwenden, um einen Speicherpool auf einer lokalen Bänderinheit in einem Kopierspeicherpool auf einer lokalen Bänderinheit zu sichern.

Um die Planung für eine bandbasierte Lösung durchzuführen, führen Sie die folgenden Tasks aus:

1. Erfüllen Sie die Systemvoraussetzungen für Hardware und Software.
2. Notieren Sie die Werte für Ihre Systemkonfiguration in den Arbeitsblättern zur Planung.
3. Führen Sie die Planung für den Plattenspeicher durch.
4. Führen Sie die Planung für den Bandspeicher durch.
5. Führen Sie die Planung für die Sicherheit durch.

## Planungsvoraussetzungen für Bänder

Bevor Sie eine Bandspeicherlösung implementieren, lesen Sie die allgemeinen Richtlinien zu Systemvoraussetzungen. Legen Sie fest, ob Daten auf Platte und/oder Band gesichert werden sollen.

### Netzbandbreite

Das Netz muss über genügend Bandbreite für die erwarteten Datenübertragungen zwischen dem Client und dem Server sowie für die standortübergreifenden Zurückschreibungsoperationen verfügen, die für die Wiederherstellung nach einem Katastrophenfall erforderlich sind. Verwenden Sie ein Speicherbereichsnetz (SAN) für Datenübertragungen zwischen dem Server, Platteneinheiten und Bänderheiten. Weitere Informationen finden Sie in Hardwarevoraussetzungen.

### Datenumlagerung

Lagern Sie täglich alle Daten von Platte auf Band um. Geben Sie die Einheitenklasse FILE für plattenbasierte Speicherpools an. Planen Sie die Umlagerung, um zu steuern, wann die Verarbeitung erfolgt. Um die automatische Umlagerung auf der Basis des Umlagerungsschwellenwerts zu verhindern, geben Sie den Wert 100 für den Parameter HIGHMIG und den Wert 0 für den Parameter LOWMIG an, wenn Sie den Befehl DEFINE STGPOOL ausgeben. Es müssen immer mindestens 20 % der Bandlaufwerke für Zurückschreibungsoperationen verfügbar bleiben. Um bis zu 80 % der verfügbaren Bandlaufwerke zu verwenden und den Durchsatz zu verbessern, geben Sie den Parameter MIGPROCESS an.

Berücksichtigen Sie, abhängig vom Typ der Daten, die umgelagert werden, die folgenden Informationen:

- Verwenden Sie Bänder, um Daten von Clients zu sichern, die über große Objekte, wie beispielsweise Datenbanken, verfügen.  
Tipp: Der Hersteller Ihres Bandlaufwerks kann Ihnen Auskunft über die Größe der Datenbank geben, die für das Schreiben auf Band geeignet ist.
- Verwenden Sie Platten, um Daten von Clients zu sichern, die über kleinere Objekte verfügen.
- Um Daten direkt auf Band zu sichern, verwenden Sie die LAN-unabhängige Datenversetzung. Weitere Informationen finden Sie in LAN-unabhängige Datenversetzung konfigurieren.
- Sichern Sie keine virtuellen Maschinen auf Band. Verwenden Sie einen separaten plattenbasierten Speicherpool, der nicht in einen bandbasierten Speicherpool umgelagert wird. Weitere Informationen zur Unterstützung virtueller Maschinen finden Sie in Technote 1239546.


#### Speicherpoolkapazität

Stellen Sie sicher, dass immer genügend Speicherpoolkapazität für 2 Tage mit Clientsicherungen und ein Puffer von 20 % verfügbar ist. Möglicherweise müssen Sie Gesamtsicherungen für einige Tage planen, um sicherzustellen, dass genügend Speicherbereich im Speicherpool vorhanden ist.

#### Bandlaufwerk

Lesen Sie die Herstellerspezifikationen und schätzen Sie die Kapazität eines Bandlaufwerks. Bestimmen Sie die Größe des Speicherbereichs, der für Sicherungs- und Umlagerungsoperationen erforderlich ist. Reservieren Sie 20 % der Bandlaufwerke für Zurückschreibungsoperationen.

#### Zugehörige Verweise:

 [MIGRATE STGPOOL \(Speicherpool in den nächsten Speicherpool umlagern\)](#)

## Systemvoraussetzungen für eine bandbasierte Lösung

Hardware- und Softwarevoraussetzungen werden für eine bandbasierte Speicherlösung mit einer Datenaufnahmerate von 14 TB pro Stunde bereitgestellt.

Lesen Sie die Informationen, um die Hardware- und Softwarevoraussetzungen für Ihre Speicherumgebung zu bestimmen. Unter Umständen müssen Sie auf der Basis Ihrer Systemgröße Anpassungen vornehmen.

- **Hardwarevoraussetzungen**  
Hardwarevoraussetzungen für Ihre IBM Spectrum Protect-Lösung basieren auf der Systemgröße. Wählen Sie funktional entsprechende oder bessere Komponenten als die aufgelisteten aus, um optimale Leistung für Ihre Umgebung zu gewährleisten.
- **Softwarevoraussetzungen**  
Die Dokumentation für die bandbasierte IBM Spectrum Protect-Lösung umfasst Installations- und Konfigurationstasks für IBM® AIX-, Linux- und Microsoft Windows-Betriebssysteme. Die aufgelisteten Softwaremindestvoraussetzungen müssen erfüllt sein.




## Hardwarevoraussetzungen

Hardwarevoraussetzungen für Ihre IBM Spectrum Protect-Lösung basieren auf der Systemgröße. Wählen Sie funktional entsprechende oder bessere Komponenten als die aufgelisteten aus, um optimale Leistung für Ihre Umgebung zu gewährleisten.

Weitere Informationen zur Planung für Platteneinheiten finden Sie in Planung für Plattenspeicher.

Weitere Informationen zur Planung für Bändeinheiten finden Sie in Planung für Bandspeicher.

Die folgende Tabelle enthält Hardwaremindestvoraussetzungen für den Server und Speicher. Wenn Sie logische Partitionen (LPARs) oder Arbeitspartitionen (WPARs) verwenden, passen Sie die Netzvoraussetzungen an, um den Partitionsgrößen Rechnung zu tragen. Die Zahlen in der Tabelle basieren auf einer Datenaufnahmerate von 14 TB pro Stunde.

| Hardwarekomponente | Systemvoraussetzungen  |
|--------------------|--|
| Serverprozessor    |  AIX-Betriebssysteme 8 Prozessorkerne, 3,42 GHz oder schneller<br>Verwenden Sie beispielsweise einen POWER8-prozessorbasierten Server.<br> Linux-Betriebssysteme  Windows-Betriebssysteme 16 Prozessorkerne, 2,0 GHz oder schneller<br>Verwenden Sie beispielsweise einen Intel Xeon-Prozessor. |
| Serverspeicher     | 64 GB Arbeitsspeicher.   |

| Hardwarekomponente | Systemvoraussetzungen  |
|--------------------|--|
| Netz               | <p>Gemäß der folgenden Größe werden etwa 14 TB Daten pro Stunde verwaltet:</p> <ul style="list-style-type: none"> <li>• 10 Gb Ethernet (mindestens vier Ports)</li> <li>• 8 Gb Fibre Channel-Adapter (mindestens vier Ports)</li> </ul> <p>Die Anzahl Ports ist vom Prozentsatz der täglichen Datenaufnahme in Plattenspeicherpools gegenüber Bandspeicher abhängig.</p> <p>Verwenden Sie separate Fibre Channel-Adapter für Band- und Plattendaten.</p>   |
| Speicher           | <p><b>Platte</b></p> <p>Geben Sie auf der Basis des Datenvolumens, das auf Platte geschrieben wird, die Anzahl Platten an, die erforderlich sind.</p> <p>Stellen Sie sicher, dass der Durchsatz der sequenziellen Ein-/Ausgabe des Speicherbereichsnetzes (SAN) mit dem Durchsatz der Ein-/Ausgabe für das Netz (siehe oben) übereinstimmt.</p> <p>Wenn Sie beispielsweise 10 TB Daten in einem 4-Stunden-Fenster sichern müssen, beträgt der Durchsatz ungefähr 700 MB pro Sekunde. In diesem Fall erfordert der Server ein Front-End-Netz (Pfad vom Client zum Server), das einen Mindestdurchsatz von 700 MB pro Sekunde unterstützt. Das Back-End-SAN (Pfad vom Server zur Speichereinheit) muss ebenfalls einen Mindestdurchsatz von 700 MB pro Sekunde unterstützen.</p> <p>Verwenden Sie zur Berechnung der erforderlichen Plattengeschwindigkeit die folgenden Formeln:</p> $\frac{(\text{Gesamtvolumen der täglichen Datenaufnahme} - \text{Volumen der täglichen Datenaufnahme direkt auf Band})}{(\text{Anzahl Stunden für tägliche Clientsicherungsoperationen})} = \text{Megabyte der Datenaufnahme auf Platte pro Stunde}$ $(\text{Megabyte der Datenaufnahme auf Platte pro Stunde}) \div (3600 \text{ Sekunden pro Stunde}) = \text{Megabyte der Datenaufnahme pro Sekunde, die von der Plattentechnologie unterstützt werden müssen}$ <p><b>Band</b></p> <p>Wählen Sie die Bandtechnologie aus, die für Ihre Geschäftsanforderungen am besten geeignet ist. Verwenden Sie beispielsweise IBM Linear Tape-Open-Bandlaufwerke (LTO-Bandlaufwerke) oder IBM TS1150-Bandlaufwerke. Stellen Sie sicher, dass genügend Mountpunkte für Clientsicherungsoperationen und für die Umlagerung vorhanden sind. Weitere Informationen zur Planung für Bandspeicher finden Sie in Planung für Bandspeicher. Eine Liste der unterstützten Bandeinheiten finden Sie im IBM® Support Portal for IBM Spectrum Protect.</p> <p>Tipp: Um die Datenversetzung zu optimieren, verwenden Sie die LAN-unabhängige Datenversetzung.</p> |
| SAN-E/A-Adapter    | <p>Trennen Sie die Platten- und Bandein-/ausgabe voneinander. Weitere Informationen zum Auswählen eines Adapters finden Sie in der Dokumentation für Brocade-Hardwareprodukte und für IBM Storwize-Speicherlösungen.</p> <p><b>Platte</b></p> <p>Verwenden Sie mindestens zwei Adapter.</p> <p><b>Band</b></p> <p>Verwenden Sie mindestens zwei Adapter.</p>   |

## Speicherbedarf für das Operations Center schätzen

Hardwarevoraussetzungen für das Operations Center sind mit Ausnahme des Speicherbereichs für die Datenbank und das Archivprotokoll (Bestand), den das Operations Center zum Speichern von Datensätzen für verwaltete Clients verwendet, in die vorherige Tabelle eingeschlossen.

Wenn Sie nicht planen, das Operations Center auf demselben System wie den IBM Spectrum Protect-Server zu installieren, können Sie die Systemanforderungen separat schätzen. Informationen zum Berechnen der Systemanforderungen für das Operations Center enthält die Technote 1641684 für die Berechnungsfunktion der Systemanforderungen.

Die Verwaltung des Operations Center auf dem IBM Spectrum Protect-Server stellt eine Workload dar, die zusätzlichen Speicherbereich für Datenbankoperationen auf dem Hub-Server und allen Peripherieservern erfordert. Der Speicherbedarf auf dem Hub-Server für das

Archivprotokoll ist höher, wenn der Hub-Server einen oder mehrere Peripherieserver überwacht. Lesen Sie die folgenden Richtlinien, um schätzen zu können, wie viel Speicherbereich Ihr IBM Spectrum Protect-Server erfordert.

#### Speicherbereich in der Datenbank für das Operations Center

Das Operations Center benötigt ungefähr 4,4 GB Speicherbereich in der Datenbank pro 1000 Clients, die auf diesem Server überwacht werden. Diese Berechnung gilt sowohl für Hub-Server als auch für Peripherieserver in einer Konfiguration. Angenommen, ein Hub-Server überwacht 2000 Clients und verwaltet außerdem drei Peripherieserver mit jeweils 1000 Clients. Bei dieser Konfiguration sind insgesamt 5000 Clients auf den vier Servern vorhanden. Jeder der Peripherieserver erfordert 4,4 GB Speicherbereich in der Datenbank. Bei Peripherieservern der IBM Spectrum Protect Version 8.1.2 oder höher erfordert der Hub-Server 8,8 GB Speicherbereich in der Datenbank allein für die Überwachung seiner 2000 Clients:

$$(4,4 \text{ GB} \times 2) = 8,8 \text{ GB}$$

#### Speicherbereich in der Datenbank für verwaltete Daten

*Verwaltete Daten* ist das Datenvolumen, das geschützt wird, einschließlich des Datenvolumens aller aufbewahrten Versionen.

- Bei Clienttypen, die immer inkrementelle Sicherungen ausführen, kann die folgende Formel zum Schätzen des Gesamtvolumens der verwalteten Daten verwendet werden:

$$\text{Front-End-Daten} + (\text{Front-End-Daten} \times \text{Änderungsrate} \times (\text{Aufbewahrungszeitraum} - 1))$$

Wenn Sie beispielsweise 100 TB Front-End-Daten sichern, einen Aufbewahrungszeitraum von 30 Tagen verwenden und eine Änderungsrate von 5 % haben, berechnen Sie das Gesamtvolumen der verwalteten Daten wie folgt:

$$100 \text{ TB} + (100 \text{ TB} \times 0,05 \times (30-1)) = 245 \text{ TB Gesamtvolumen der verwalteten Daten}$$

- Bei Clienttypen, die täglich Gesamtsicherungen ausführen, kann die folgende Formel zum Schätzen des Gesamtvolumens der verwalteten Daten verwendet werden:

$$\text{Front-End-Daten} \times \text{Aufbewahrungszeitraum} \times (1 + \text{Änderungsrate})$$

Wenn Sie beispielsweise 10 TB Front-End-Daten sichern, einen Aufbewahrungszeitraum von 30 Tagen verwenden und eine Änderungsrate von 3 % haben, berechnen Sie das Gesamtvolumen der verwalteten Daten wie folgt:

$$10 \text{ TB} \times 30 \times (1 + 0,03) = 309 \text{ TB Gesamtvolumen der verwalteten Daten}$$

Unstrukturierte Daten; durchschnittliche Objektgröße: 4 MB

Strukturierte Daten; durchschnittliche Objektgröße: 128 MB

Unstrukturierte Daten; Anzahl Objekte =

$$(245 \text{ TB} \times 1024 \times 1024) / 4 \text{ MB} = 64225280$$

Strukturierte Daten; Anzahl Objekte =

$$(309 \text{ TB} \times 1024 \times 1024) / 128 \text{ MB} = 2531328$$

Gesamtzahl Objekte: 66756608

Kosten der verwalteten Daten (1 KB pro Objekt) =

$$(66756608 \text{ KB}) / (1024 \times 1024) = 63,66 \text{ GB}$$

Planen Sie 20 % zusätzlichen Speicherbereich ein, damit Datenbanksysteme nicht 100 % ihrer Kapazität nutzen:

$$\text{Gesamtbedarf des physischen Speicherbereichs in der Datenbank} = (\text{Speicherbereich für verwaltete Daten} + \text{Speicherbereich für das Operations Center}) \times (1,20)$$

In diesem Beispiel würden Sie den Speicherbereich unter Verwendung der folgenden Zahlen berechnen:

$$(66,33 \text{ GB} + 8,4 \text{ GB}) \times 1,20 = 76,41 \text{ GB}$$

#### Speicherbereich für das Archivprotokoll

Das Operations Center verwendet alle 24 Stunden ungefähr 18 GB Speicherbereich für das Archivprotokoll pro Server für jeweils 1000 Clients, die auf diesem Server überwacht werden. Darüber hinaus wird für jeweils 1000 Clients, die auf Peripherieservern überwacht werden, zusätzlicher Speicherbereich für das Archivprotokoll auf dem Hub-Server benötigt. Für Peripherieserver der Version 8.1.2 oder höher beträgt dieses zusätzliche Volumen 1,2 GB Speicherbereich für das Archivprotokoll auf dem Hub-Server pro 100 Clients, die alle 24 Stunden überwacht werden.

Angenommen, ein Hub-Server überwacht 2000 Clients und verwaltet außerdem drei Peripherieserver mit jeweils 1000 Clients. Bei dieser Konfiguration sind insgesamt 5000 Clients auf den vier Servern vorhanden. Sie können den Speicherbereich für das Archivprotokoll für den Hub-Server mithilfe der folgenden Formel berechnen:



$((18 \text{ GB} \times 2) + (1,2 \text{ GB} \times 3)) = 39,6 \text{ GB}$  Speicherbereich für das Archivprotokoll

Diese Schätzungen basieren auf dem Standardintervall von 5 Minuten zur Erfassung von Statusdaten. Wenn Sie das Erfassungsintervall von einmal alle 5 Minuten auf einmal alle 3 Minuten reduzieren, erhöht sich der Speicherbedarf. Die folgenden Beispiele zeigen die ungefähre Erhöhung des Protokollspeicherbedarfs bei einem Erfassungsintervall von einmal alle 3 Minuten für eine Konfiguration, in der Peripherieserver der Version 8.1.2 oder höher überwacht werden:

- Hub-Server: im Bereich von 39,6 GB bis 66 GB
- Jeder Peripherieserver: im Bereich von 18 GB bis 30 GB

Ordnen Sie Speicherbereich für das Archivprotokoll zu, damit das Operations Center ohne Auswirkungen auf Serveroperationen unterstützt werden kann.

## Softwarevoraussetzungen

Die Dokumentation für die bandbasierte IBM Spectrum Protect-Lösung umfasst Installations- und Konfigurationstasks für IBM® AIX-, Linux- und Microsoft Windows-Betriebssysteme. Die aufgelisteten Softwaremindestvoraussetzungen müssen erfüllt sein.

Informationen zu den Softwarevoraussetzungen für IBM lin\_tape-Einheitentreiber finden Sie in der Veröffentlichung IBM Tape Device Drivers Installation and User's Guide.

### AIX-Systeme

| Softwaretyp           | Softwaremindestvoraussetzungen   |
|-----------------------|--|
| Betriebssystem        | IBM AIX 7.1<br><br>Weitere Informationen zu Betriebssystemvoraussetzungen finden Sie in AIX: Systemmindestvoraussetzungen für AIX-Systeme.   |
| Dienstprogramm gunzip | Das Dienstprogramm gunzip muss auf Ihrem System verfügbar sein, bevor Sie die Installation oder das Upgrade für den IBM Spectrum Protect-Server ausführen. Stellen Sie sicher, dass das Dienstprogramm gunzip installiert ist und der Pfad zu diesem Dienstprogramm in der Umgebungsvariablen PATH definiert ist.  |
| Dateisystemtyp        | JFS2-Dateisysteme<br><br>AIX-Systeme können ein großes Volumen an Dateisystemdaten zwischenspeichern, wodurch der Speicherplatz, der für Server- und IBM DB2-Prozesse erforderlich ist, reduziert werden kann. Um beim AIX-Server eine Auslagerung zu verhindern, verwenden Sie die Mountoption rbrw für das JFS2-Dateisystem. Für den Dateisystemcache wird weniger Speicher verwendet und für IBM Spectrum Protect ist mehr Speicher verfügbar.<br><br>Verwenden Sie nicht die Mountoptionen für Dateisysteme, gleichzeitige E/A (CIO = Concurrent I/O) und direkte E/A (DIO = Direct I/O) für Dateisysteme, die die IBM Spectrum Protect-Datenbank, Protokolle oder Speicherpooldatenträger enthalten. Diese Optionen können eine Leistungsverschlechterung vieler Serveroperationen zur Folge haben. IBM Spectrum Protect und DB2 können, wenn dies von Vorteil ist, weiterhin DIO verwenden, IBM Spectrum Protect erfordert die Mountoptionen jedoch nicht, um die Vorteile dieser Verfahren selektiv nutzen zu können. |
| Andere Software       | Korn-Shell (ksh)   |

### Linux-Systeme

| Softwaretyp    | Softwaremindestvoraussetzungen   |
|----------------|--|
| Betriebssystem | Red Hat Enterprise Linux 7 (x86_64)  |
| Bibliotheken   | GNU C-Bibliotheken, Version 2.3.3-98.38 oder höher, die auf dem IBM Spectrum Protect-System installiert sind.<br>Red Hat Enterprise Linux-Server: <ul style="list-style-type: none"><li>• libaio</li><li>• libstdc++.so.6 (32-Bit- und 64-Bit-Pakete sind erforderlich)</li><li>• numactl.x86_64</li></ul> |

| Softwaretyp     | Softwaremindestvoraussetzungen   |
|-----------------|--|
| Dateisystemtyp  | Formatieren Sie datenbankbezogene Dateisysteme mit ext3 oder ext4.<br><br>Verwenden Sie für speicherpoolbezogene Dateisysteme XFS. |
| Andere Software | Korn-Shell (ksh)   |

## Windows-Systeme

| Softwaretyp     | Softwaremindestvoraussetzungen   |
|-----------------|--|
| Betriebssystem  | Microsoft Windows Server 2012 R2 (64-Bit) oder Windows Server 2016   |
| Dateisystemtyp  | NTFS   |
| Andere Software | Windows 2012 R2 oder Windows 2016 mit .NET Framework 3.5 ist installiert und aktiviert.<br><br>Die folgenden Benutzerkontensteuerungsrichtlinien müssen inaktiviert sein: <ul style="list-style-type: none"> <li>Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto</li> <li>Benutzerkontensteuerung: Alle Administratoren im Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen</li> </ul> |

## Arbeitsblätter zur Planung

Verwenden Sie die Arbeitsblätter zur Planung für die Aufzeichnung von Werten, die Sie bei der Konfiguration Ihres Systems und bei der Konfiguration des IBM Spectrum Protect-Servers verwenden. Verwenden Sie die Best-Practice-Standardwerte, die in den Arbeitsblättern aufgeführt sind.

Jedes Arbeitsblatt unterstützt Sie bei den Vorbereitungen für unterschiedliche Teile der Systemkonfiguration mithilfe der Best-Practice-Werte:







### Vorkonfiguration des Serversystems

Führen Sie mithilfe der Arbeitsblätter zur Vorkonfiguration die Planung für die Dateisysteme und Verzeichnisse aus, die erstellt werden sollen, wenn Sie während der Systemkonfiguration Dateisysteme für IBM Spectrum Protect konfigurieren. Alle Verzeichnisse, die Sie für den Server erstellen, müssen leer sein.

### Serverkonfiguration

Verwenden Sie die Arbeitsblätter zur Konfiguration, wenn Sie den Server konfigurieren. Für die meisten Elemente werden Standardwerte vorgeschlagen; andernfalls ist ein entsprechender Hinweis vorhanden.

Tabelle 1. Arbeitsblatt für die Vorkonfiguration eines Serversystems

| Element   | Standardwert  | Eigener Wert | Minimale Verzeichnisgröße  | Weitere Informationen  |
|---|---|--------------|--|--|
| TCP/IP-Portadresse für die Kommunikation mit dem Server | 1500  |              | Nicht zutreffend   | Stellen Sie sicher, dass dieser Port verfügbar ist, wenn Sie das Betriebssystem installieren und konfigurieren.<br><br>Die Portnummer kann eine Zahl zwischen 1024 und 32767 sein. |
| Verzeichnis für die Serverinstanz                       |  AIX-Betriebssysteme<br> Linux-Betriebssysteme<br>/home/tsminst1/tsminst1<br><br> Windows-Betriebssysteme<br>C:\tsminst1 |              |  AIX-Betriebssysteme 50 GB<br><br> Linux-Betriebssysteme<br> Windows-Betriebssysteme 25 GB | Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den DB2-Instanzeigner in Tabelle 2.                          |

| Element                                   | Standardwert  | Eigener Wert | Minimale Verzeichnisgröße  | Weitere Informationen  |
|---|---|--------------|--|--|
| Verzeichnis für Serverinstallation        | <ul style="list-style-type: none"> <li> AIX-Betriebssysteme</li> <li> Linux-Betriebssysteme/</li> <li> Windows-BetriebssystemeC:</li> </ul>  |              |  AIX-Betriebssysteme<br>Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB<br><br> Linux-Betriebssysteme<br> Windows-Betriebssysteme<br>Mindestspeicherbereich, der für das Verzeichnis erforderlich ist: 30 GB |  |
| Verzeichnis für Serverinstallation        | /usr  |              |  AIX-Betriebssysteme<br>Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB  |  |
| Verzeichnis für Serverinstallation        |  AIX-Betriebssysteme/var   |              |  AIX-Betriebssysteme<br>Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB  |  |
| Verzeichnis für Serverinstallation        |  AIX-Betriebssysteme/tmp   |              |  AIX-Betriebssysteme<br>Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB  |  |
| Verzeichnis für Serverinstallation        |  AIX-Betriebssysteme/opt   |              |  AIX-Betriebssysteme<br>Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 10 GB   |  |
| Verzeichnis für die aktive Protokolldatei |  AIX-Betriebssysteme<br> Linux-Betriebssysteme<br>/tsminst1/TSMalog<br><br> Windows-Betriebssysteme<br>C:\tsminst1\TSMalog   |              | 128 GB   | Wenn Sie die aktive Protokolldatei während der Erstkonfiguration des Servers erstellen, setzen Sie die Größe auf 128 GB. |
| Verzeichnis für das Archivprotokoll       |  AIX-Betriebssysteme<br> Linux-Betriebssysteme<br>/tsminst1/TSMarchlog<br><br> Windows-Betriebssysteme<br>C:\tsminst1\TSMarchlog   |              | 3 TB   |  |
| Verzeichnisse für die Datenbank           |  AIX-Betriebssysteme<br> Linux-Betriebssysteme<br>/tsminst1/TSMdbspace00<br>/tsminst1/TSMdbspace01<br>/tsminst1/TSMdbspace02<br>/tsminst1/TSMdbspace03<br><br> Windows-Betriebssysteme<br>C:\tsminst1\TSMdbspace00<br>C:\tsminst1\TSMdbspace01<br>C:\tsminst1\TSMdbspace02<br>C:\tsminst1\TSMdbspace03 |              | Anweisungen zum Berechnen des Speicherbedarfs finden Sie in Hardwarevoraussetzungen.   | Erstellen Sie vier Dateisysteme für die Datenbank.   |















| Element                    | Standardwert  | Eigener Wert | Minimale Verzeichnisgröße  | Weitere Informationen   |
|----------------------------|---|--------------|--|---|
| Verzeichnisse für Speicher |  AIX-Betriebssysteme<br> Linux-Betriebssysteme<br>/tsminst1/TSMfile00<br>/tsminst1/TSMfile01<br>/tsminst1/TSMfile02<br>/tsminst1/TSMfile03<br>...<br> Windows-Betriebssysteme<br>C:\tsminst1\TSMfile00<br>C:\tsminst1\TSMfile01<br>C:\tsminst1\TSMfile02<br>C:\tsminst1\TSMfile03<br>... |              | Ermitteln Sie die minimale Gesamtkapazität für alle Verzeichnisse mithilfe der folgenden Berechnung:<br><br>Prozentsatz der täglich aufgenommenen Daten, die auf Platte geschrieben werden, + 20% = Minimale Gesamtkapazität | Die bevorzugte Methode ist die Definition mindestens eines Verzeichnisses für jede Bandeinheit. |







Tabelle 2. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

| Element   | Standardwert  | Eigener Wert | Weitere Informationen   |
|---|---|--------------|---|
| DB2-Instanzeigner                                   | tsminst1  |              | Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 1 in einen anderen Wert geändert haben, ändern Sie auch den Wert für den DB2-Instanzeigner. |
| Kennwort des DB2-Instanzeigners                     |  AIX-Betriebssysteme<br> Linux-BetriebssystemepasswOrd<br> Windows-Betriebssysteme<br>pAssWOrd |              | Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.             |
| Primärgruppe für den DB2-Instanzeigner              |  AIX-Betriebssysteme<br> Linux-Betriebssystemetsmsrvrs  |              |   |
| Servername  | Der Standardwert für den Servernamen ist der Systemhostname.  |              |   |
| Serverkennwort                                      | passwOrd  |              | Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.                          |
| Administrator-ID: Benutzer-ID für die Serverinstanz | admin   |              |   |
| Kennwort für die Administrator-ID                   | passwOrd  |              | Wählen Sie für das Administratorkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.                   |

| Element                 | Standardwert | Eigener Wert | Weitere Informationen  |
|-------------------------|--------------|--------------|--|
| Startzeit des Zeitplans | 23:00        |              | <p>Die standardmäßige Startzeit des Zeitplans gibt den Anfang der Client-Workload-Phase an, die sich in erster Linie auf die Clientsicherungs- und -archivierungsaktivitäten bezieht. Während der Client-Workload-Phase werden Clientoperationen durch Serverressourcen unterstützt. Normalerweise werden diese Operationen während des nächtlichen Zeitplanfensters ausgeführt.</p> <p>Zeitpläne für Serververwaltungsoperationen beginnen gemäß Definition 10 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen.</p> <p>In diesem Handbuch wird 23:00 Uhr als Startzeit für Clientsicherungsoperationen vorgeschlagen.</p> |

Tabelle 3. Arbeitsblatt für die Bandkonfiguration

| Element                            | Standardwert  | Eigener Wert | Weitere Informationen   |
|------------------------------------|---|--------------|---|
| Dateien für automatische Einheiten | <p>IBM® Einheiten mit einem IBM Banderheitentreiber:</p> <ul style="list-style-type: none"> <li>•  AIX-Betriebssysteme<br/>/dev/smcX</li> <li>•  Linux-Betriebssysteme<br/>/dev/IBMchangerX</li> <li>•  Windows-Betriebssysteme<br/>ChangerX</li> </ul> <p>Einheiten eines anderen Herstellers als IBM mit einem IBM Spectrum Protect-Einheitentreiber:</p> <ul style="list-style-type: none"> <li>•  AIX-Betriebssysteme<br/>/dev/lbX</li> <li>•  Linux-Betriebssysteme<br/>/dev/tsmcsi/lbX</li> <li>•  Windows-Betriebssysteme<br/>lbA.B.C.D</li> </ul> |              | <p>Um die Dateien für Speicherarchiveinheiten manuell zu definieren, verwenden Sie die folgenden Befehle:</p> <ul style="list-style-type: none"> <li>• DEFINE LIBRARY</li> <li>• DEFINE DRIVE</li> <li>• DEFINE PATH</li> </ul> <p>Für SCSI-Einheiten können Sie den Befehl PERFORM LIBACTION verwenden, um alle Laufwerke und zugehörigen Pfade für ein einzelnes Speicherarchiv in einem einzigen Schritt zu definieren. Um diesen Befehl zum Definieren aller Laufwerke und Pfade verwenden zu können, muss die Option SANDISCOVERY unterstützt werden und aktiviert sein.</p> |

| Element       | Standardwert  | Eigener Wert | Weitere Informationen |
|---------------|---|--------------|-----------------------|
| Bandlaufwerke | <p>IBM Einheiten mit einem IBM Bandeinheitentreiber:</p> <ul style="list-style-type: none"> <li>•  AIX-Betriebssysteme<br/>/dev/rmtX</li> <li>•  Linux-Betriebssysteme<br/>/dev/IBMtapeX</li> <li>•  Windows-Betriebssysteme<br/>TapeX</li> </ul> <p>Einheiten eines anderen Herstellers als IBM mit einem IBM Spectrum Protect-Einheitentreiber:</p> <ul style="list-style-type: none"> <li>•  AIX-Betriebssysteme<br/>/dev/mtX</li> <li>•  Linux-Betriebssysteme<br/>/dev/tmscsi/mtX</li> <li>•  Windows-Betriebssysteme<br/>mtA.B.C.D</li> </ul> |              |                       |

## Planung für Plattenspeicher

Wählen Sie die effektivste Speichertechnologie für IBM Spectrum Protect-Komponenten aus, um effiziente Serverleistung und Serveroperationen zu gewährleisten.

Speicherhardwareeinheiten haben unterschiedliche Kapazitäts- und Leistungsmerkmale, die festlegen, wie die Einheiten effizient mit IBM Spectrum Protect verwendet werden können. Die folgenden Richtlinien stellen eine allgemeine Anleitung zur Auswahl der für Ihre Lösung geeigneten Speicherhardware und Konfiguration dar.

Datenbank, aktive Protokolldatei und Archivprotokoll

- Verwenden Sie eine Solid-State-Platte (SSD) oder eine schnelle Platte mit 15.000 Umdrehungen pro Minute für die IBM Spectrum Protect-Datenbank und die aktive Protokolldatei.
- Verwenden Sie beim Erstellen von Arrays für die Datenbank RAID-Stufe 5.
- Verwenden Sie separate Platten für den Speicher für das Archivprotokoll und die Datenbanksicherung.

Speicherpool

Verwenden Sie RAID-Stufe 6 für Speicherpoolarrays, um bei Verwendung von Typen großer Platten Schutz vor dem Ausfall von zwei Laufwerken hinzuzufügen.

- Planung der Speicherarrays  
Bereiten Sie die Konfiguration des Plattenspeichers vor, indem Sie die Planung für RAID-Arrays und Datenträger gemäß der Größe Ihres IBM Spectrum Protect-Systems ausführen.

## Planung für Bandspeicher

Bestimmen Sie, welche Bandeinheiten verwendet werden sollen und wie diese zu konfigurieren sind. Um die Systemleistung zu optimieren, planen Sie die Verwendung schneller Bandeinheiten mit hoher Speicherkapazität. Stellen Sie genügend Bandlaufwerke bereit, um Ihre Geschäftsanforderungen erfüllen zu können.

- Unterstützte Bandeinheiten und Speicherarchive  
Der Server kann eine Vielzahl von Bandeinheiten und Speicherarchiven verwenden. Wählen Sie für Ihre Geschäftsanforderungen geeignete Bandeinheiten und Speicherarchive aus.
- Unterstützte Bandeinheitenkonfigurationen  
Lesen Sie die Informationen zu lokalen Netzen (LAN) und Speicherbereichsnetzen (SAN). Um die Datenversetzung zu optimieren, planen Sie die Konfiguration der LAN-unabhängigen Datenversetzung. Überlegen Sie außerdem, ob die gemeinsame Speicherarchivnutzung verwendet werden soll.
- Erforderliche Definitionen für Bandspeichereinheiten  
Bevor der IBM Spectrum Protect-Server eine Bandeinheit verwenden kann, muss die Einheit für das Betriebssystem und den




Server konfiguriert werden. Bestimmen Sie im Rahmen des Planungsprozesses, welche Definitionen für Ihre Bandspeichereinheiten erforderlich sind.

- Planung der Speicherpoolhierarchie  
Planen Sie die Speicherpoolhierarchie, um sicherzustellen, dass Daten täglich von Platte auf Band umgelagert werden. Bei der Umlagerung wird Speicherbereich auf der Platteneinheit freigegeben und die Daten werden für die langfristige Aufbewahrung auf Band versetzt. Auf diese Weise können Sie die Vorteile der Skalierbarkeit, Kosteneffizienz und Sicherheitsfunktionen von Bandspeicher nutzen.
- Auslagerung von Daten  
Um die Datenwiederherstellung zu erleichtern und in Ihre Strategie zur Wiederherstellung nach einem Katastrophenfall zu integrieren, speichern Sie Bandkopien an einen anderen Standort.

## Unterstützte Bandeinheiten und Speicherarchive

Der Server kann eine Vielzahl von Bandeinheiten und Speicherarchiven verwenden. Wählen Sie für Ihre Geschäftsanforderungen geeignete Bandeinheiten und Speicherarchive aus.

Eine Liste der unterstützten Einheiten und gültigen Einheitenklassenformate finden Sie auf der Website für Ihr Betriebssystem:

-  AIX-Betriebssysteme  Windows-Betriebssysteme Supported devices for AIX and Windows
-  Linux-Betriebssysteme Supported devices for Linux

Weitere Informationen zu Speichereinheiten und Speicherobjekten finden Sie in Typen von Speichereinheiten.

Jede Einheit, die für IBM Spectrum Protect definiert ist, ist einer einzigen *Einheitenklasse* zugeordnet. Die Einheitenklasse gibt den Einheitentyp und die Datenträgerverwaltungsinformationen, wie beispielsweise Aufzeichnungsformat, geschätzte Kapazität und Kennzeichnungspräfixe, an.

Ein *Einheitentyp* kennzeichnet eine Einheit als Mitglied einer Gruppe von Einheiten mit gemeinsamen Datenträgermerkmalen. Beispielsweise gilt der Einheitentyp LTO für alle Generationen von LTO-Bandlaufwerken.

Eine Einheitenklasse für ein Bandlaufwerk muss auch ein Speicherarchiv angeben. Ein *physisches Speicherarchiv* besteht aus einem oder mehreren Laufwerken, die ähnliche Anforderungen in Bezug auf die Bereitstellung von Datenträgern haben. Das heißt, das Laufwerk kann von einem Bediener oder durch einen automatisierten Bereitstellungsmechanismus bereitgestellt werden.

Eine *Speicherarchivobjektdefinition* gibt den Speicherarchivtyp und andere Merkmale an, die diesem Speicherarchivtyp zugeordnet sind.

In der folgenden Tabelle sind die bevorzugten Speicherarchivtypen für eine Bandspeicherlösung in IBM Spectrum Protect Version 8.1.3 aufgelistet.

Tabelle 1. Speicherarchivtypen für eine Bandspeicherlösung in IBM Spectrum Protect 8.1.3

| Speicherarchivtyp | Beschreibung  | Weitere Informationen  |
|-------------------|---|--|
| SCSI              | <p>Ein SCSI-Speicherarchiv wird über eine SCSI-Schnittstelle gesteuert, die entweder direkt über SCSI-Verkabelung oder über ein Speicherbereichsnetz an den Host des Servers angeschlossen ist. Ein Robotermechanismus oder ein anderer Mechanismus handhabt automatisch das Bereitstellen von Banddatenträgern und das Aufheben der Bereitstellung von Banddatenträgern.</p> <p>Wenn Sie unterschiedliche Laufwerktypen für ein SCSI-Speicherarchiv erstellen, erstellen Sie mehrere logische Speicherarchive, die nicht auf verschiedene Typen von Laufwerken aufgeteilt werden können. Ein SCSI-Speicherarchiv kann Laufwerke mit gemischten Technologien enthalten, einschließlich LTO Ultrium- und DLT-Laufwerke. Beispiel:</p> <ul style="list-style-type: none"> <li>• Oracle StorageTek L700-Speicherarchiv</li> <li>• Bandeinheit IBM® 3592</li> </ul> | <p>Speicherarchive für die Verwendung durch einen Server konfigurieren<br/>Es gelten Einschränkungen, wenn Sie verschiedene Generationen von Datenträgern und Laufwerken kombiniert verwenden. Weitere Informationen finden Sie in:</p> <ul style="list-style-type: none"> <li>• Generationen von 3592-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv mischen</li> <li>• LTO-Laufwerke und -Datenträger in einem Speicherarchiv mischen</li> </ul> |

| Speicherarchivtyp | Beschreibung  | Weitere Informationen |
|-------------------|---|-----------------------|
| SHARED            | <p>Gemeinsam genutzte Speicherarchive sind logische Speicherarchive, die durch SCSI-Speicherarchive dargestellt werden. Das Speicherarchiv wird durch den IBM Spectrum Protect-Server gesteuert, der als Speicherarchivmanager konfiguriert ist.</p> <p>IBM Spectrum Protect-Server, die den Speicherarchivtyp SHARED verwenden, sind Speicherarchivclients für den Speicherarchivmanager-Server. Gemeinsam genutzte Speicherarchive referenzieren einen Speicherarchivmanager.</p> |                       |

## Unterstützte Bandeinheitenkonfigurationen

Lesen Sie die Informationen zu lokalen Netzen (LAN) und Speicherbereichsnetzen (SAN). Um die Datenversetzung zu optimieren, planen Sie die Konfiguration der LAN-unabhängigen Datenversetzung. Überlegen Sie außerdem, ob die gemeinsame Speicherarchivnutzung verwendet werden soll.

Wählen Sie die Einheitenkonfiguration aus, die für Ihre Geschäftsanforderungen am besten geeignet ist.

- **LAN-gestützte und LAN-unabhängige Datenversetzung**  
Sie können Daten zwischen Clients und Speichereinheiten, die an ein lokales Netz (LAN) angeschlossen sind, oder Speichereinheiten, die an ein Speicherbereichsnetz (SAN) angeschlossen sind, versetzen; dies wird als LAN-unabhängige Datenversetzung bezeichnet.
- **Gemeinsame Speicherarchivnutzung**  
Sie können die Effizienz Ihrer Bandspeicherlösung optimieren, indem Sie die gemeinsame Speicherarchivnutzung konfigurieren. Bei der gemeinsamen Speicherarchivnutzung können mehrere IBM Spectrum Protect-Server dasselbe Bandarchiv und dieselben Laufwerke in einem Speicherbereichsnetz (SAN) nutzen und die Sicherheits- und Wiederherstellungsleistung sowie die Nutzung der Bandhardware verbessern.
- **LAN-unabhängige Datenversetzung**  
Mit IBM Spectrum Protect wird einem Client über einen Speicheragenten die Funktionalität bereitgestellt, um Daten direkt in einem Bandarchiv in einem Speicherbereichsnetz (SAN) zu sichern und aus ihm zurückzuschreiben. Dieser Typ von Datenversetzung ist auch als LAN-unabhängige Datenversetzung bekannt.
- **Gemischte Einheitentypen in Speicherarchiven**  
IBM Spectrum Protect unterstützt das Mischen unterschiedlicher Einheitentypen in einem einzelnen automatisierten Speicherarchiv, sofern das Speicherarchiv die verschiedenen Datenträger für die unterschiedlichen Einheitentypen unterscheiden kann. Um den Konfigurationsprozess zu vereinfachen, sollten Sie keine unterschiedlichen Einheitentypen in einem Speicherarchiv mischen. Wenn das Mischen von Einheitentypen erforderlich ist, berücksichtigen Sie die Einschränkungen.

## LAN-gestützte und LAN-unabhängige Datenversetzung

Sie können Daten zwischen Clients und Speichereinheiten, die an ein lokales Netz (LAN) angeschlossen sind, oder Speichereinheiten, die an ein Speicherbereichsnetz (SAN) angeschlossen sind, versetzen; dies wird als LAN-unabhängige Datenversetzung bezeichnet.

In einer konventionellen LAN-Konfiguration sind einem einzelnen IBM Spectrum Protect-Server ein oder mehrere Bandarchive zugeordnet. Durch die LAN-unabhängige Datenversetzung wird LAN-Bandbreite für andere Verwendungszwecke verfügbar gemacht und die IBM Spectrum Protect-Serverauslastung verringert.

In einer LAN-Konfiguration müssen Clientdaten, E-Mails, Terminalverbindung, Anwendungsprogramm und Einheitensteuerinformationen von demselben Netz gehandhabt werden. Einheitensteuerinformationen und Clientsicherungs- und -zurückschreibungsdaten fließen über das LAN.

Ein Speicherbereichsnetz (SAN) ist ein dediziertes Speichernetz, das die Systemleistung verbessern kann.

Durch die Verwendung von IBM Spectrum Protect in einem SAN profitieren Sie von den folgenden Funktionen:

- **Gemeinsame Nutzung von Speichereinheiten durch mehrere IBM Spectrum Protect-Server.**  
Einschränkung: Eine Speichereinheit mit dem Einheitentyp GENERICTAPE kann nicht von mehreren Servern gemeinsam genutzt werden.
- **Versetzen von IBM Spectrum Protect-Clientdaten direkt auf Speichereinheiten (LAN-unabhängige Datenversetzung) durch die Konfiguration eines Speicheragenten auf dem Clientsystem.**

In einem SAN können Sie Bandlaufwerke und Speicherarchive, die vom IBM Spectrum Protect-Server unterstützt werden, einschließlich der meisten SCSI-Bandeinheiten, gemeinsam nutzen.



Wenn IBM Spectrum Protect-Server ein SCSI-Bandarchiv gemeinsam nutzen, ist der *Speicherarchivmanager* der Eigner der Einheit und steuert die Einheit. Die Speicheragenten und andere IBM Spectrum Protect-Server, die dieses Speicherarchiv gemeinsam nutzen, sind *Speicherarchivclients*. Ein Speicherarchivclient fordert gemeinsam genutzte Speicherarchivressourcen, wie beispielsweise Laufwerke oder Datenträger, vom Speicherarchivmanager an, verwendet die Ressourcen jedoch unabhängig. Der Speicherarchivmanager koordiniert den Zugriff auf diese Ressourcen. IBM Spectrum Protect-Server, die als Speicherarchivclients definiert sind, kontaktieren den Speicherarchivmanager mithilfe der Kommunikation zwischen Servern und fordern Einheitenservice an. Daten werden über das SAN zwischen den einzelnen Servern und der Speichereinheit versetzt.

Voraussetzung: Wenn Sie einen Speicherarchivmanager-Server definieren, der mit dem IBM Spectrum Protect-Server gemeinsam genutzt wird, muss die Option SANDISCOVERY auf ON gesetzt werden. Standardmäßig ist diese Option auf OFF gesetzt.

IBM Spectrum Protect-Server verwenden die folgenden Funktionen für die gemeinsame Nutzung eines automatisierten Speicherarchivs:

#### Partitionierung des Datenträgerbestands

Der Bestand der Datenträger im gemeinsam genutzten Speicherarchiv wird unter den Servern aufgeteilt. Entweder ist ein einzelner Server Eigner eines bestimmten Datenträgers oder der Datenträger befindet sich im globalen Arbeitsdatenträgerpool. Keiner der Server ist Eigner des Arbeitsdatenträgerpools.

#### Serialisierter Laufwerkzugriff

Es greift jeweils nur ein einziger Server auf das jeweilige Bandlaufwerk zu. Der Laufwerkzugriff erfolgt serialisiert. IBM Spectrum Protect steuert den Laufwerkzugriff, damit Server nicht die Bereitstellung von Datenträgern anderer Server aufheben oder nicht auf Laufwerke schreiben, in denen andere Server ihre Datenträger bereitstellen.

#### Serialisierter Mountzugriff

Der Datenträgerwechsler des Speicherarchivs führt jeweils nur eine einzige Operation zum Bereitstellen (Mountoperation) oder Aufheben der Bereitstellung aus. Der Speicherarchivmanager führt alle Mountoperationen aus, um diese Serialisierung bereitzustellen.

## Gemeinsame Speicherarchivnutzung

---

Sie können die Effizienz Ihrer Bandspeicherlösung optimieren, indem Sie die gemeinsame Speicherarchivnutzung konfigurieren. Bei der gemeinsamen Speicherarchivnutzung können mehrere IBM Spectrum Protect-Server dasselbe Bandarchiv und dieselben Laufwerke in einem Speicherbereichsnetz (SAN) nutzen und die Sicherungs- und Wiederherstellungsleistung sowie die Nutzung der Bandhardware verbessern.

Wenn IBM Spectrum Protect-Server ein Speicherarchiv gemeinsam nutzen, wird ein Server als Speicherarchivmanager konfiguriert, der Speicherarchivoperationen wie Bereitstellung und Aufhebung der Bereitstellung steuert. Der Speicherarchivmanager steuert auch das Eigentumsrecht für Datenträger und den Speicherarchivbestand. Weitere Server werden als Speicherarchivclients konfiguriert und kontaktieren den Speicherarchivmanager mithilfe der Kommunikation zwischen Servern und fordern Ressourcen an.

Speicherarchivclients müssen dieselbe Version oder eine frühere Version wie der Speicherarchivmanager-Server haben. Ein Speicherarchivmanager kann keine Speicherarchivclients unterstützen, die eine höhere Version haben. Weitere Informationen finden Sie in *Storage-agent and library-client compatibility with an IBM Spectrum Protect server* (Kompatibilität des Speicheragenten und des Speicherarchivclients mit einem IBM Spectrum Protect-Server).

## LAN-unabhängige Datenversetzung

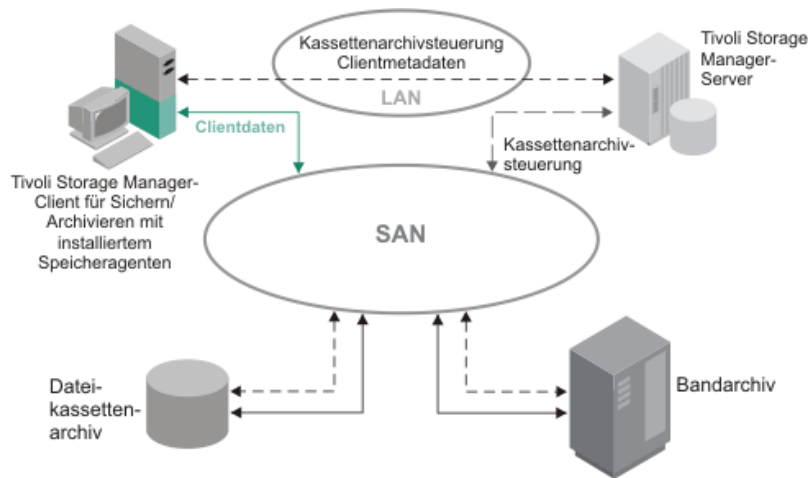
---

Mit IBM Spectrum Protect wird einem Client über einen Speicheragenten die Funktionalität bereitgestellt, um Daten direkt in einem Bandarchiv in einem Speicherbereichsnetz (SAN) zu sichern und aus ihm zurückzuschreiben. Dieser Typ von Datenversetzung ist auch als LAN-unabhängige Datenversetzung bekannt.

Einschränkung: Centera-Speichereinheiten können keine Ziele für LAN-unabhängige Operationen sein.

Abbildung 1 zeigt eine SAN-Konfiguration, bei der ein Client direkt auf ein Bandarchiv zugreift, um Daten zu lesen oder zu schreiben.

Abbildung 1. LAN-unabhängige Datenversetzung



Die LAN-unabhängige Datenversetzung erfordert die Installation eines Speicheragenten auf dem Clientsystem. Der Server verwaltet die Datenbank und das Wiederherstellungsprotokoll und fungiert als Speicherarchivmanager, um Operationen der Einheiten zu steuern. Der Speicheragent auf dem Client handhabt die Datenübertragung zu der Einheit im SAN. Diese Implementierung gibt Bandbreite im LAN frei, die andernfalls für das Versetzen von Clientdaten verwendet würde.

## Gemischte Einheitentypen in Speicherarchiven

IBM Spectrum Protect unterstützt das Mischen unterschiedlicher Einheitentypen in einem einzelnen automatisierten Speicherarchiv, sofern das Speicherarchiv die verschiedenen Datenträger für die unterschiedlichen Einheitentypen unterscheiden kann. Um den Konfigurationsprozess zu vereinfachen, sollten Sie keine unterschiedlichen Einheitentypen in einem Speicherarchiv mischen. Wenn das Mischen von Einheitentypen erforderlich ist, berücksichtigen Sie die Einschränkungen.

Bei Speicherarchiven mit dieser Funktionalität handelt es sich um Modelle, die über integrierte gemischte Laufwerke verfügen oder die das Hinzufügen gemischter Laufwerke unterstützen. Weitere Informationen zu bestimmten Modellen finden Sie in der Dokumentation des Herstellers. Informationen zu Speicherarchiven, die für IBM Spectrum Protect mit gemischten Einheitentypen getestet wurden, finden Sie in den Informationen für Ihr Betriebssystem:

- IBM Spectrum Protect Supported Devices for AIX, HP-UX, Solaris, and Windows
- IBM Spectrum Protect Supported Devices for Linux

Beispielsweise können LTO Ultrium-Laufwerke und IBM TS4500-Laufwerke in einem einzelnen Speicherarchiv vorhanden sein, das für den IBM Spectrum Protect-Server definiert ist.

- Verschiedene Datenträgergenerationen in einem Speicherarchiv  
Der IBM Spectrum Protect-Server erlaubt zwar unterschiedliche Einheitentypen in einem automatisierten Speicherarchiv, das Mischen verschiedener Generationen desselben Laufwerktyps wird jedoch im Allgemeinen nicht unterstützt. Neue Laufwerke können keine Daten mit den älteren Datenträgerformaten schreiben und alte Laufwerke können neue Formate nicht lesen. LTO Ultrium-Laufwerke sind eine Ausnahme von dieser Regel.
- Gemischte Datenträger und Speicherpools  
Sie können die Effizienz Ihrer Bandspeicherlösung optimieren, indem Sie Datenträgerformate in einem Speicherpool nicht mischen. Anstatt Formate zu mischen, ordnen Sie jedes eindeutige Datenträgerformat über seine eigene Einheitenklasse einem separaten Speicherpool zu. Diese Einschränkung gilt auch für LTO-Formate.

## Verschiedene Datenträgergenerationen in einem Speicherarchiv

Der IBM Spectrum Protect-Server erlaubt zwar unterschiedliche Einheitentypen in einem automatisierten Speicherarchiv, das Mischen verschiedener Generationen desselben Laufwerktyps wird jedoch im Allgemeinen nicht unterstützt. Neue Laufwerke können keine Daten mit den älteren Datenträgerformaten schreiben und alte Laufwerke können neue Formate nicht lesen. LTO Ultrium-Laufwerke sind eine Ausnahme von dieser Regel.

Wenn mit der neuen Laufwerktechnologie keine Daten auf Datenträger geschrieben werden können, die von Laufwerken einer älteren Generation formatiert wurden, müssen die älteren Datenträger als schreibgeschützt markiert werden, um Probleme bei Serveroperationen zu verhindern. Außerdem müssen die älteren Laufwerke aus dem Speicherarchiv entfernt werden oder die Definitionen der älteren Laufwerke müssen vom Server entfernt werden. Beispielsweise unterstützt der IBM Spectrum Protect-Server nicht die Verwendung von Oracle StorageTek 9940A-Laufwerken mit 9940B-Laufwerken in Kombination mit anderen Einheitentypen in einem einzelnen Speicherarchiv.

Im Allgemeinen unterstützt IBM Spectrum Protect nicht das Mischen unterschiedlicher Generationen von LTO Ultrium-Laufwerken und -Datenträgern. Die folgenden Kombinationen werden jedoch unterstützt:

- LTO Ultrium Generation 3 (LTO-3) mit LTO Ultrium Generation 4 (LTO-4)
- LTO Ultrium Generation 4 (LTO-4) mit LTO Ultrium Generation 5 (LTO-5)
- LTO Ultrium Generation 5 (LTO-5) mit LTO Ultrium Generation 6 (LTO-6)
- LTO Ultrium Generation 6 (LTO-6) mit LTO Ultrium Generation 7 (LTO-7)

Der Server unterstützt diese Kombinationen, da die verschiedenen Laufwerke Daten von den unterschiedlichen Datenträgern lesen und auf diese schreiben können. Wenn Sie planen, für alle Laufwerke ein Upgrade auf Generation 4 (oder Generation 5, 6 oder 7) durchzuführen, müssen Sie alle vorhandenen LTO Ultrium-Laufwerkdefinitionen und die Pfade, die ihnen zugeordnet sind, löschen. Anschließend können Sie die neuen Laufwerke und Pfade der Generation 4 (oder Generation 5, 6 oder 7) definieren.

Einschränkungen, die für das Mischen von LTO Ultrium-Bandlaufwerken und -Datenträgern gelten

- LTO-5-Laufwerke können nur LTO-3-Datenträger lesen. Wenn Sie LTO-3- und LTO-5-Laufwerke und -Datenträger in einem einzelnen Speicherarchiv mischen, müssen Sie die LTO-3-Datenträger als schreibgeschützt markieren. Sie müssen alle LTO-3-Arbeitsdatenträger entnehmen.
- LTO-6-Laufwerke können nur LTO-4-Datenträger lesen. Wenn Sie LTO-4- und LTO-6-Laufwerke und -Datenträger in einem einzelnen Speicherarchiv mischen, müssen Sie die LTO-4-Datenträger als schreibgeschützt markieren. Sie müssen alle LTO-4-Arbeitsdatenträger entnehmen.
- LTO-7-Laufwerke können nur LTO-5-Datenträger lesen. Wenn Sie LTO-5- und LTO-7-Laufwerke und -Datenträger in einem einzelnen Speicherarchiv mischen, müssen Sie die LTO-5-Datenträger als schreibgeschützt markieren. Sie müssen alle LTO-5-Arbeitsdatenträger entnehmen.

Einschränkungen, die für gemischte Generationen von LTO Ultrium-Bandlaufwerken in einem Speicherarchiv gelten

Sie müssen Bandkassetten einer früheren Generation als das Bandlaufwerk verwenden. Ein Bandlaufwerk einer späteren Generation kann Daten von einer Bandkassette einer früheren Generation lesen und auf diese schreiben. Wenn beispielsweise ein Speicherarchiv über LTO-7- und LTO-6-Bandlaufwerke verfügt, müssen Sie LTO-6-Bandkassetten verwenden. Sowohl die LTO-7- als auch die LTO-6-Bandlaufwerke können Daten von LTO-6-Bandkassetten lesen und auf Bandkassetten dieser Generation schreiben.

Einschränkungen, die für gemischte Generationen von LTO Ultrium-Bandkassetten in einem Speicherarchiv gelten

Sie müssen eine Bandkassette verwenden, die dieselbe Generation wie das Bandlaufwerk hat, oder exakt eine Generation früher. Wenn beispielsweise ein Speicherarchiv über LTO-7-Bandlaufwerke verfügt, können Sie LTO-7-Bandkassetten oder eine Kombination aus LTO-7- und LTO-6-Bandkassetten verwenden. Wenn dieses Speicherarchiv über LTO-7-, LTO-6- und LTO-5-Bandkassetten verfügt, müssen Sie den Zugriffsmodus für die LTO-5-Bandkassetten in READONLY (Lesezugriff) ändern.

Weitere Informationen zum Mischen von LTO Ultrium-Generationen finden Sie in Einheitenklassen LTO definieren.

Wenn Sie IBM Spectrum Protect verwenden, können Sie keine Laufwerke der Laufwerkgenerationen 3592, TS1130, TS1140, TS1150 oder späterer Laufwerkgenerationen mischen. Verwenden Sie eine von drei speziellen Konfigurationen. Ausführliche Informationen finden Sie in Einheitenklassen 3592 definieren.

Wenn Sie planen, Datenträger in einem Speicherarchiv zu verschlüsseln, mischen Sie keine Datenträgergenerationen in dem Speicherarchiv.

## Gemischte Datenträger und Speicherpools

---

Sie können die Effizienz Ihrer Bandspeicherlösung optimieren, indem Sie Datenträgerformate in einem Speicherpool nicht mischen. Anstatt Formate zu mischen, ordnen Sie jedes eindeutige Datenträgerformat über seine eigene Einheitenklasse einem separaten Speicherpool zu. Diese Einschränkung gilt auch für LTO-Formate.

Mehrere Speicherpools und ihre Einheitenklassen verschiedenen Typs können auf dasselbe Speicherarchiv verweisen, das diese wie in Verschiedene Datenträgergenerationen in einem Speicherarchiv beschrieben unterstützen kann.

Sie können eine Migration auf eine neue Generation eines Datenträgertyps innerhalb desselben Speicherpools durchführen, indem Sie die folgenden Schritte ausführen:

1. Ersetzen Sie in dem Speicherarchiv alle älteren Laufwerke durch die Laufwerke der neueren Generation. Die Laufwerke dürfen nicht gemischt werden.
2. Markieren Sie die vorhandenen Datenträger mit den älteren Formaten als schreibgeschützt, wenn das neue Laufwerk diese Bänder im alten Format nicht hinzufügen kann. Wenn das neue Laufwerk auf die vorhandenen Datenträger mit ihrem alten Format schreiben kann, ist dies nicht notwendig; Schritt 1 ist jedoch dennoch erforderlich. Wenn verschiedene Laufwerkgenerationen, die lese- aber nicht schreibkompatibel sind, in demselben Speicherarchiv erforderlich sind, verwenden Sie für jede Laufwerkgeneration einen separaten Speicherpool.






## Erforderliche Definitionen für Bandspeichereinheiten


Bevor der IBM Spectrum Protect-Server eine Bandeinheit verwenden kann, muss die Einheit für das Betriebssystem und den Server konfiguriert werden. Bestimmen Sie im Rahmen des Planungsprozesses, welche Definitionen für Ihre Bandspeichereinheiten erforderlich sind.

Tipp: Mithilfe des Befehls PERFORM LIBACTION können Sie den Prozess zum Hinzufügen von Einheiten zu SCSI- und VTL-Speicherarchiven vereinfachen.

In Tabelle 1 sind die Definitionen, die für die unterschiedlichen Einheitentypen erforderlich sind, zusammengefasst.

Tabelle 1. Erforderliche Definitionen für Speichereinheiten

| Einheit                                 | Einheitentypen   | Erforderliche Definitionen |          |      |                 |
|---|--|----------------------------|----------|------|-----------------|
|   |  | Speicherarchiv             | Laufwerk | Pfad | Einheitenklasse |
| Magnetplatte                            | DISK   | –                          | –        | –    | Ja <sup>1</sup> |
|   | FILE <sup>2</sup>  | –                          | –        | –    | Ja              |
|   |  AIX-Betriebssysteme<br> Windows-Betriebssysteme<br>CENTERA<br> Linux-Betriebssysteme<br>CENTERA <sup>3</sup>   | –                          | –        | –    | Ja              |
| Band                                    | <ul style="list-style-type: none"> <li>• 3590</li> <li>• 3592</li> <li>• DLT</li> <li>• LTO</li> <li>• NAS</li> <li>• VOLSAFE</li> </ul>  AIX-Betriebssysteme<br> Windows-Betriebssysteme<br>GENERICTAPE<br>ECARTRIDGE <sup>4</sup> | Ja                         | Ja       | Ja   | Ja              |
| Austauschbare Datenträger (Dateisystem) | REMOVABLEFILE  | Ja                         | Ja       | Ja   | Ja              |

1. Die Einheitenklasse DISK ist bei der Installation vorhanden und kann nicht geändert werden.
2. FILE-Speicherarchive, -Laufwerke und -Pfade sind für die gemeinsame Nutzung mit Speicheragenten erforderlich.
3.  Linux-Betriebssysteme Der Einheitentyp CENTERA ist nur für Linux x86\_64-Systeme verfügbar.
4. Der Einheitentyp ECARTRIDGE gilt für Oracle StorageTek-Kassettenbandlaufwerke wie beispielsweise 9840- und T10000-Laufwerke.

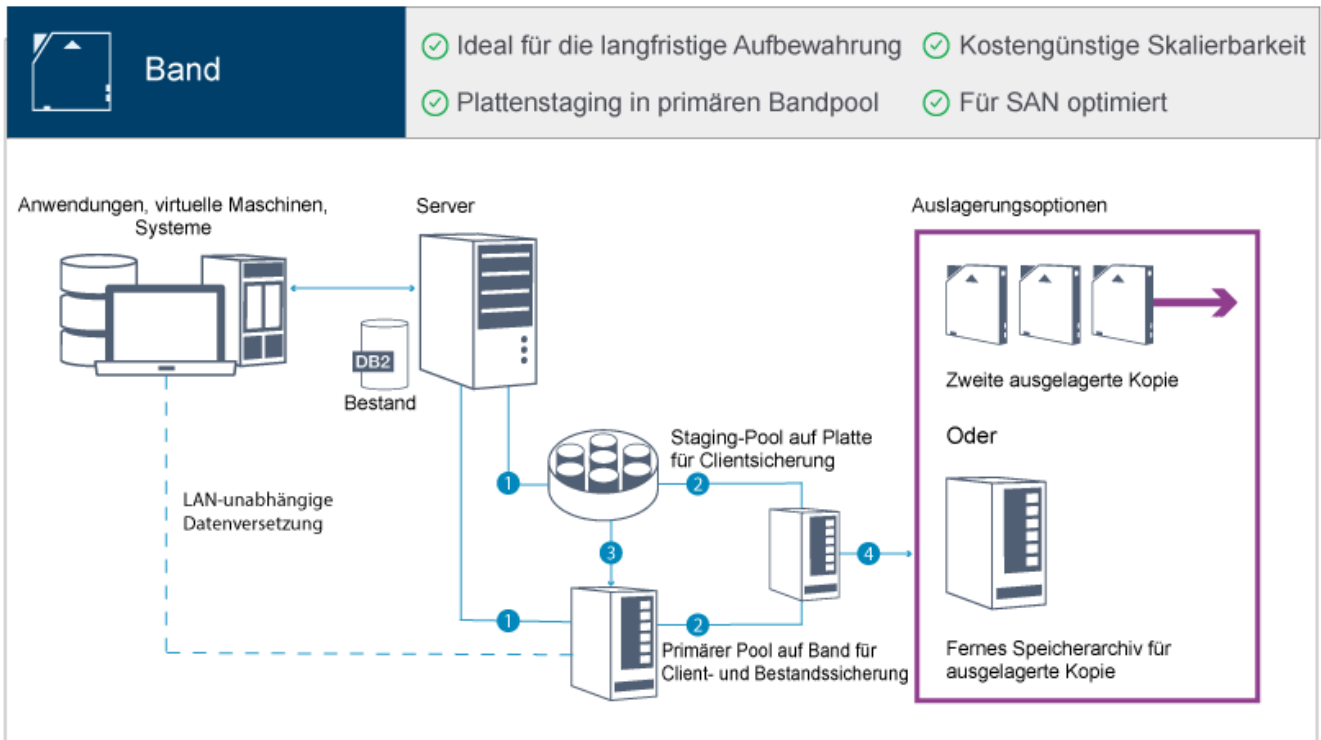
## Planung der Speicherpoolhierarchie

Planen Sie die Speicherpoolhierarchie, um sicherzustellen, dass Daten täglich von Platte auf Band umgelagert werden. Bei der Umlagerung wird Speicherbereich auf der Platteneinheit freigegeben und die Daten werden für die langfristige Aufbewahrung auf Band versetzt. Auf diese Weise können Sie die Vorteile der Skalierbarkeit, Kosteneffizienz und Sicherheitsfunktionen von Bandspeicher nutzen.

### Vorbereitende Schritte

Die Speicherpoolhierarchie unterstützt Sie bei der Verwaltung des Datenflusses. Schauen Sie sich zum besseren Verständnis des Datenflusses Abbildung 1 an.

Abbildung 1. Bandspeicherlösung



Die folgenden Schritte entsprechen den Zahlen in der Abbildung:

1. Der Server empfängt Daten von Clients (Anwendungen, virtuelle Maschinen oder Systeme) und speichert die Daten in primären Speicherpools. Abhängig vom Clienttyp werden die Daten in einem primären Speicherpool auf Platte oder Band gespeichert.
2. Die Daten auf Platte und Band werden in einem Kopierspeicherpool auf Band gesichert.
3. Daten in dem primären Speicherpool auf Platte werden täglich in den primären Speicherpool auf Band umgelagert.
4. Daten aus dem Kopierspeicherpool auf Band werden an einen anderen Standort versetzt werden, um die langfristige Aufbewahrung und die Wiederherstellung nach einem Katastrophenfall zu unterstützen.

## Vorgehensweise

Um die Speicherpoolhierarchie zu planen, beantworten Sie die folgenden Fragen:

- a. Welche Clients sollten Daten auf Platte sichern und welche Clients sollten Daten auf Band sichern?
  - Die bevorzugte Methode ist das Sichern von Clients, die große Objekte wie beispielsweise Datenbanken enthalten, auf Band.
  - Die bevorzugte Methode ist das Sichern aller anderen Clients auf Platte.
  - Clients virtueller Maschinen (VMs) können auf Platte oder Band gesichert werden. Die bevorzugte Methode ist das Sichern eines VM-Clients in einem separaten Plattenspeicherpool, der nicht auf Band umgelagert wird. Wenn ein VM-Client auf Band umgelagert werden muss, erstellen Sie einen kleineren Plattenspeicherpool zum Speichern der VMware-Steuerdateien. Dieser kleinere Plattenspeicherpool darf nicht auf Band umgelagert werden. Weitere Informationen zum Sichern eines VM-Clients auf Band finden Sie in Richtlinien für Banddatenträger und Technote 1239546.

**Tipp:** Wenn viele Clients Daten in einem einzigen Speicherpool sichern müssen, ziehen Sie die Verwendung eines Speicherpools auf Platte in Erwägung, da Sie viele Mountpunkte angeben können. Sie können einen Maximalwert von 999 für den Parameter MAXNUMMP im Befehl REGISTER NODE angeben.

- b. Was ist bei der Angabe der Kapazität plattenbasierter Speicherpools zu beachten?

Planen Sie zumindest genügend Kapazität zum Speichern der Daten von Sicherungsoperationen eines einzelnen Tages ein. Die bevorzugte Methode ist das Planen von genügend Kapazität, um Daten von Sicherungsoperationen zweier Tage zu speichern, zuzüglich eines Puffers von 20 %.

- c. Was ist bei der Angabe der Einheitenklasse für den plattenbasierten Speicherpool zu beachten?

Die bevorzugte Methode ist die Angabe der Einheitenklasse FILE. Setzen Sie den Parameter MOUNTLIMIT auf 4000. Stellen Sie außerdem sicher, dass der Knoten über eine ausreichend große Anzahl Mountpunkte verfügt; diesen Wert können Sie über den Parameter MAXNUMMP im Befehl REGISTER NODE angeben.

- d. Sollte Datendeduplizierung für den Plattenspeicherpool angegeben werden?

Nein, da die Daten nur für einen einzigen Tag auf Platte gespeichert werden, bevor die Daten auf Band umgelagert werden.

e. Sollte die automatische Umlagerung von Daten auf der Basis eines Umlagerungsschwellenwerts angegeben werden?

Nein. Planen Sie stattdessen die tägliche Umlagerung mithilfe des Befehls `MIGRATE STGPOOL`. (Um die automatische Umlagerung auf der Basis des Umlagerungsschwellenwerts zu verhindern, geben Sie den Wert 100 für den Parameter `HIGHMIG` und den Wert 0 für den Parameter `LOWMIG` an, wenn Sie den Befehl `DEFINE STGPOOL` ausgeben.)

f. Sollte eine Umlagerungsverzögerung angegeben werden?

Die bevorzugte Methode ist die Angabe der täglichen Umlagerung von Platte auf Band und nicht die Angabe einer Umlagerungsverzögerung, die weitere Planung erfordert. Weitere Informationen zur Umlagerungsverzögerung finden Sie in Dateien in einer Speicherpoolhierarchie umlagern.

g. Wie kann die Anzahl Bandlaufwerke berechnet werden?

- i. Bestimmen Sie die native Datenübertragungsrate des Laufwerks anhand der Dokumentation des Herstellers. Um eine Schätzung der kontinuierlichen Datenübertragungsrate in Ihrer Speicherumgebung zu ermitteln, subtrahieren Sie 30 % von der nativen Datenübertragungsrate.
- ii. Berechnen Sie die erforderliche Datenaufnahmerate des Servers. Dividieren Sie dann diese Zahl durch die kontinuierliche Datenübertragungsrate einer einzelnen Bänderinheit. Das Ergebnis gibt die minimale Anzahl Laufwerke zur Unterstützung der Datenaufnahme an.
- iii. Berechnen Sie die Anzahl Mountpunkte, die für Clients erforderlich sind, die Daten auf Band sichern, einschließlich der Clients, die mehrere Sitzungen verwenden. Sie können die Mountpunkte über das Fenster zum Durchführen von Sicherungen verteilen; dabei müssen Sie beachten, dass Clients wahrscheinlich große Objekte sichern, die unter Umständen den größten Teil des Fensters in Anspruch nehmen.
- iv. Berechnen Sie die Leistungsanforderungen *und* Mountpunkte, die für Verwaltungstasks, wie beispielsweise Umlagerung von Platte auf Band und Kopieroperationen von Band auf Band, erforderlich sind. Durch die Sicherung von Daten auf Band, können Sie die Umlagerungsverarbeitung vermeiden, durch die Ausführung von Kopieroperationen von Band auf Band verdoppeln sich jedoch die Anforderungen für Bandlaufwerke.
- v. Berechnen Sie die Anzahl zusätzlicher Laufwerke, die gegebenenfalls erforderlich sind:

- Wenn ein Bandlaufwerk nicht korrekt funktioniert, hat das Problem Auswirkungen auf die Anzahl verfügbarer Mountpunkte und die Aufnahmezeit. Ziehen Sie die Bereitstellung von Ersatzlaufwerken in Erwägung. Wenn beispielsweise fünf Bandlaufwerke für normale Operationen erforderlich sind, sollten Sie die Bereitstellung von zwei Ersatzlaufwerken in Erwägung ziehen.
- Für Zurückschreibungs- und Abrufoperationen sind unter Umständen zusätzliche Bandlaufwerke erforderlich, wenn Sie planen, die Operationen gleichzeitig mit Datenaufnahme- und Verwaltungsoperationen auszuführen. Stellen Sie, falls erforderlich, zusätzliche Bandlaufwerke bereit und stellen Sie sicher, dass diese noch nicht verwendet wurden, wenn Sie die Zurückschreibungs- oder Abrufoperationen starten.

h. Welche Alternativen sind für die Optimierung von Zurückschreibungsoperationen verfügbar?

Sie können die Kollokation verwenden, um die Systemleistung zu verbessern und Organisation von Daten zu optimieren. Mithilfe der Kollokation kann die Anzahl Datenträger reduziert werden, auf die zugegriffen werden muss, wenn ein großes Datenvolumen zurückgeschrieben werden muss:

- Für plattenbasierte Speicherpools ist die bevorzugte Methode die Verwendung der Kollokation nach Knoten. Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.
- Für bandbasierte Speicherpools ist die bevorzugte Methode die Verwendung der Kollokation nach Gruppe. Die Kollokation nach Gruppe hat eine Verringerung der nicht genutzten Bandkapazität zur Folge, wodurch mehr kollokierte Daten auf einzelnen Bändern gespeichert werden können.

Weitere Informationen zur Kollokation finden Sie in Operationen durch Aktivierung der Kollokation von Clientdateien optimieren. Wenn Sie ein erfahrener Systemadministrator sind, können Sie weitere Aktionen zur Optimierung von Zurückschreibungsoperationen planen. Siehe Zurückschreibungsoperationen für Clients optimieren, Dateisicherungsmethoden und `MOVE NODEDATA` (Daten nach Knoten in einen Speicherpool mit sequenziellem Zugriff versetzen).

## Auslagerung von Daten

---

Um die Datenwiederherstellung zu erleichtern und in Ihre Strategie zur Wiederherstellung nach einem Katastrophenfall zu integrieren, speichern Sie Bandkopien an einen anderen Standort.

Verwenden Sie die Funktion 'Disaster Recovery Manager' (DRM), um einen Plan zur Wiederherstellung nach einem Katastrophenfall zu konfigurieren und automatisch zu generieren, der die Informationen, Scripts und Prozeduren enthält, die erforderlich sind, um den Server nach einem Katastrophenfall automatisch zurückzuschreiben und Clientdaten wiederherzustellen. Wählen Sie eine der folgenden Optionen für die Auslagerung von Daten als Strategie zur Wiederherstellung nach einem Katastrophenfall aus, um Bandkopien zu schützen:

Vaulting an einem anderen Standort für einen einzelnen Produktionsstandort

Speicherdatenträger, wie beispielsweise Bandkassetten und Datenträger werden an einem anderen Standort durch Vaulting geschützt. Ein Kurier transportiert die Daten von der Speichereinrichtung an dem anderen Standort zum

Wiederherstellungsstandort. Wenn ein Katastrophenfall eintritt, werden die Datenträger wieder an den Produktionsstandort gesendet, nachdem die Hardware und der IBM Spectrum Protect-Server wiederhergestellt wurden.

**Vaulting an einem anderen Standort mit einem Wiederherstellungsstandort**

Ein Kurier transportiert Speicherdatenträger vom Produktionsstandort an eine Speichereinrichtung an einem anderen Standort. Da ein zugeordneter Wiederherstellungsstandort vorhanden ist, können Sie die Wiederherstellungszeit im Vergleich zur Wiederherstellungszeit bei einem einzelnen Produktionsstandort verringern. Diese Option erhöht jedoch die Kosten für die Wiederherstellung nach einem Katastrophenfall, da weitere Hardware und Software verwaltet werden muss. Beispielsweise muss der Wiederherstellungsstandort über kompatible Bandeinheiten und IBM Spectrum Protect-Server-Software verfügen. Bevor der Produktionsstandort wiederhergestellt werden kann, müssen die Hardware und Software am Wiederherstellungsstandort konfiguriert und aktiv sein.

**Elektronisches Vaulting**

Um elektronisches Vaulting als Strategie zur Wiederherstellung nach einem Katastrophenfall verwenden zu können, muss am Wiederherstellungsstandort ein aktiver IBM Spectrum Protect-Server vorhanden sein. Kritische Daten des Produktionsstandorts werden durch elektronisches Vaulting am Wiederherstellungsstandort geschützt. DRM wird auch für das Vaulting nicht kritischer Daten an einem anderen Standort verwendet. Beim elektronischen Vaulting werden kritische Daten schneller und häufiger als bei traditionellen Methoden mittels Kurier ausgelagert. Die Wiederherstellungszeit verkürzt sich, da kritische Daten bereits am Wiederherstellungsstandort gespeichert sind. Da der Wiederherstellungsstandort ständig aktiv ist, sind die Kosten der Strategie zur Wiederherstellung nach einem Katastrophenfall jedoch höher als beim Vaulting an einem anderen Standort.

**Zugehörige Konzepte:**

Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM

## Planung für Sicherheit

---

Planen Sie den Schutz der Sicherheit von Systemen in der IBM Spectrum Protect-Lösung mithilfe von Steuerelementen für Zugriff und Authentifizierung und ziehen Sie das Verschlüsseln von Daten und der Übertragung von Kennwörtern in Erwägung.

- **Planung für Administratorrollen**  
Definieren Sie die Berechtigungsstufen, die Administratoren zugeordnet werden sollen, die Zugriff auf die IBM Spectrum Protect-Lösung haben.
- **Planung für sichere Kommunikation**  
Planen Sie den Schutz der Kommunikation zwischen den IBM Spectrum Protect-Lösungskomponenten.
- **Planung für die Speicherung verschlüsselter Daten**  
Bestimmen Sie, ob Ihr Unternehmen die Verschlüsselung gespeicherter Daten erfordert, und wählen Sie das für Ihre Anforderungen am besten geeignete Verfahren aus.
- **Planung des Firewallzugriffs**  
Bestimmen Sie die definierten Firewalls und die Ports, die offen sein müssen, damit die IBM Spectrum Protect-Lösung funktionsfähig ist.

## Planung für Administratorrollen

---

Definieren Sie die Berechtigungsstufen, die Administratoren zugeordnet werden sollen, die Zugriff auf die IBM Spectrum Protect-Lösung haben.

Sie können Administratoren eine der folgenden Berechtigungsstufen zuordnen:

**Systemberechtigung**

Administratoren mit Systemberechtigung verfügen über die höchste Berechtigungsstufe. Administratoren mit dieser Berechtigungsstufe können jede Task ausführen. Sie können alle Maßnahmendomänen und Speicherpools verwalten und anderen Administratoren Berechtigung erteilen.

**Maßnahmenberechtigung**

Administratoren mit Maßnahmenberechtigung können alle Tasks verwalten, die sich auf die Maßnahmenverwaltung beziehen. Diese Berechtigung kann uneingeschränkt sein oder auf bestimmte Maßnahmendomänen eingeschränkt werden.

**Speicherberechtigung**

Administratoren mit Speicherberechtigung können Speicherressourcen für den Server zuordnen und steuern.

**Bedienberechtigung**

Administratoren mit Bedienberechtigung können den sofortigen Betrieb des Servers und die Verfügbarkeit von Speichermedien wie beispielsweise Bandarchiven und -laufwerken steuern.

Die Szenarios in Tabelle 1 enthalten Beispiele, die zeigen, warum es sinnvoll ist, Administratoren für die Ausführung von Tasks unterschiedliche Berechtigungsstufen zuzuordnen:

Tabelle 1. Szenarios für Administratorrollen

| Szenario  | Typ der zu konfigurierenden Administrator-ID  |
|---|---|
| Ein Administrator in einem kleinen Unternehmen verwaltet den Server und ist für alle Serveraktivitäten verantwortlich.  | <ul style="list-style-type: none"> <li>• Systemberechtigung: 1 Administrator-ID</li> </ul>  |
| Ein Administrator für mehrere Server verwaltet auch das gesamte System. Mehrere andere Administratoren verwalten ihre eigenen Speicherpools.  | <ul style="list-style-type: none"> <li>• Systemberechtigung auf allen Servern: 1 Administrator-ID für den Administrator des gesamten Systems</li> <li>• Speicherberechtigung für bestimmte Speicherpools: 1 Administrator-ID für jeden der anderen Administratoren</li> </ul> |
| Ein Administrator verwaltet 2 Server. Eine andere Person unterstützt ihn bei den Verwaltungstasks. Zwei Assistenten müssen sicherstellen, dass wichtige Systeme gesichert werden. Jeder Assistent ist für die Überwachung der geplanten Sicherungen auf einem der IBM Spectrum Protect-Server verantwortlich. | <ul style="list-style-type: none"> <li>• Systemberechtigung auf beiden Servern: 2 Administrator-IDs</li> <li>• Bedienerberechtigung: 2 Administrator-IDs für die Assistenten mit Zugriff auf den Server, für den die jeweilige Person verantwortlich ist.</li> </ul>          |

**Zugehörige Tasks:**  
Administratoren verwalten

## Planung für sichere Kommunikation

Planen Sie den Schutz der Kommunikation zwischen den IBM Spectrum Protect-Lösungskomponenten.

Bestimmen Sie auf der Basis der Regelungen und Geschäftsanforderungen für Ihr Unternehmen, welche Stufe des Schutzes für Ihre Daten erforderlich ist.

Wenn Ihr Unternehmen ein hohes Maß an Sicherheit für Kennwörter und die Datenübertragung erfordert, planen Sie die Implementierung der sicheren Kommunikation mit dem Protokoll Transport Layer Security (TLS) oder Secure Sockets Layer (SSL).

TLS und SSL stellen sichere Kommunikation zwischen dem Server und dem Client bereit, können sich jedoch auf die Systemleistung auswirken. Um die Systemleistung zu verbessern, verwenden Sie TLS für die Authentifizierung, ohne Objektdaten zu verschlüsseln. Informationen zur Angabe, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, finden Sie in der Beschreibung der Clientoption SSL für die Client/Server-Kommunikation und der Beschreibung des Parameters UPDATE SERVER=SSL für die Kommunikation zwischen Servern. Ab Version 8.1.2 wird TLS standardmäßig für die Authentifizierung verwendet. Wenn Sie sich für die Verwendung von TLS entscheiden, um vollständige Sitzungen zu verschlüsseln, verwenden Sie das Protokoll nur für Sitzungen, für die es erforderlich ist; fügen Sie außerdem auf dem Server Prozessorressourcen hinzu, um den wachsenden Datenaustausch im Netz handhaben zu können. Sie können auch versuchsweise andere Optionen verwenden. Beispielsweise stellen einige Netzeinheiten wie Router und Switches die TLS- oder SSL-Funktion bereit.

Mithilfe von TLS und SSL können Sie einige oder alle der unterschiedlichen möglichen Kommunikationspfade schützen, beispielsweise:

- Operations Center: vom Browser zum Hub-Server; vom Hub-Server zum Peripherieserver
- Vom Client zum Server
- Vom Server zum Server: Knotenreplikation

**Zugehörige Tasks:**  
Sichere Kommunikation mit Transport Layer Security konfigurieren

## Planung für die Speicherung verschlüsselter Daten

Bestimmen Sie, ob Ihr Unternehmen die Verschlüsselung gespeicherter Daten erfordert, und wählen Sie das für Ihre Anforderungen am besten geeignete Verfahren aus.

Tabelle 1. Datenverschlüsselungsverfahren auswählen

| Geschäftsanforderung           | Verschlüsselungsverfahren                  | Weitere Informationen   |
|--------------------------------|--|---|
| Daten auf Clientebene schützen | IBM Spectrum Protect-Clientverschlüsselung | Sie können Daten auf Dateiebene unter Verwendung einer Einschluss-/Ausschlussliste verschlüsseln. Auf diese Weise haben Sie ein hohes Maß an Kontrolle darüber, welche Daten verschlüsselt werden. Auf dem Client sind zusätzliche IT-Ressourcen erforderlich, die sich auf die Leistung von Sicherungs- und Zurückschreibungsprozessen auswirken können. Weitere Informationen zu diesem Verfahren finden Sie in IBM Spectrum Protect-Clientverschlüsselung. |



| Geschäftsanforderung  | Verschlüsselungsverfahren | Weitere Informationen   |
|---|---------------------------|---|
| Daten in Speicherpooldatenträgern auf einem Bandlaufwerk schützen | Anwendungsverfahren       | Wenn Sie das Anwendungsverfahren verwenden, verwaltet IBM Spectrum Protect die Verschlüsselungsschlüssel, um Daten in Speicherpooldatenträgern zu schützen. Sie müssen Sie besonders vorsichtig vorgehen, um Datenbanksicherungen zu schützen, da die Verschlüsselungsschlüssel in der Serverdatenbank gespeichert sind. Ohne Zugriff auf Datenbanksicherungen und zugehörige Verschlüsselungsschlüssel können Sie Ihre Daten nicht zurückschreiben. Sie können dieses Verfahren nicht verwenden, um Datenbanksicherungen, exportierte Daten oder Sicherungsgruppen zu verschlüsseln. Weitere Informationen zum Anwendungsverfahren finden Sie in Verschlüsselungsverfahren für Bänder. |
| Daten auf einem Bandlaufwerk schützen                             | Speicherarchivverfahren   | Wenn Sie das Speicherarchivverfahren verwenden, werden die Verschlüsselungsschlüssel vom Speicherarchiv verwaltet. Sie können sowohl Daten in Speicherpools als auch andere Daten auf einem Bandlaufwerk verschlüsseln. Sie können steuern, welche Datenträger unter Verwendung ihrer Barcodeseriennummern verschlüsselt werden. Weitere Informationen zum Speicherarchivverfahren finden Sie in Verschlüsselungsverfahren für Bänder.  |
| Daten auf einem Bandlaufwerk schützen                             | Systemverfahren           | Wenn Sie das Systemverfahren verwenden, wird die Verschlüsselung von einem Einheitsreiber oder dem AIX-Betriebssystem verwaltet. Dieses Verschlüsselungsverfahren ist nur unter dem Betriebssystem AIX verfügbar. Sie können sowohl Daten in Speicherpools als auch andere Daten auf einem Bandlaufwerk verschlüsseln. Weitere Informationen zum Systemverfahren finden Sie in Verschlüsselungsverfahren für Bänder.  |

## Planung des Firewallzugriffs

Bestimmen Sie die definierten Firewalls und die Ports, die offen sein müssen, damit die IBM Spectrum Protect-Lösung funktionsfähig ist.

In Tabelle 1 sind die Ports beschrieben, die vom Server, vom Client und vom Operations Center verwendet werden.

Tabelle 1. Vom Server, Client und Operations Center verwendete Ports

| Element                        | Standardwert      | Richtung           | Beschreibung   |
|--------------------------------|-------------------|--------------------|--|
| Basisport (TCPPOINT)           | 1500              | Abgehend/Eingehend | Jede Serverinstanz erfordert einen eindeutigen Port. Sie können eine alternative Portnummer angeben. Der mit der Option TCPPOINT angegebene Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen vom Client empfangsbereit. Mithilfe der Option TCPADMINPORT und der Option ADMINONCLIENTPORT können Sie Portwerte für den Datenverkehr des Verwaltungsclients festlegen. |
| Port nur für SSL (SSLTCPPOINT) | Kein Standardwert | Abgehend/Eingehend | Dieser Port wird verwendet, wenn die Kommunikation am Port auf ausschließlich SSL-fähige Sitzungen beschränkt werden soll. Ein Server kann sowohl die SSL-Kommunikation als auch die Nicht-SSL-Kommunikation unterstützen, indem die Option TCPPOINT oder die Option TCPADMINPORT verwendet wird.  |
| SMB                            | 45                | Eingehend/Abgehend | Dieser Port wird von Konfigurationsassistenten verwendet, die unter Verwendung nativer Protokolle mit mehreren Hosts kommunizieren.  |
| SSH                            | 22                | Eingehend/Abgehend | Dieser Port wird von Konfigurationsassistenten verwendet, die unter Verwendung nativer Protokolle mit mehreren Hosts kommunizieren.  |
| SMTP                           | 25                | Abgehend           | Dieser Port wird zum Senden von E-Mail-Alerts vom Server verwendet.  |
| Replikation                    | Kein Standardwert | Abgehend/Eingehend | Der Port und das Protokoll für den Port für abgehende Daten für die Replikation werden mit dem Befehl DEFINE SERVER festgelegt, der zum Konfigurieren der Replikation verwendet wird.<br><br>Bei den Ports für eingehende Daten für die Replikation handelt es sich um die TCP-Ports und SSL-Ports, die für den Quellenserver im Befehl DEFINE SERVER angegeben werden.            |

| Element                               | Standardwert                   | Richtung  | Beschreibung  |
|---------------------------------------|--------------------------------|-----------|---|
| Port für Clientzeitplan               | Client-Port: 1501              | Abgehend  | Der Client ist an dem angegebenen Port empfangsbereit und teilt die Portnummer dem Server mit. Der Server kontaktiert den Client, wenn die servergesteuerte Zeitplanung verwendet wird. Sie können eine alternative Portnummer in der Clientoptionsdatei angeben.   |
| Lange laufende Sitzungen              | Einstellung für KEEPALIVE: YES | Abgehend  | Wenn die Option KEEPALIVE aktiviert ist, werden während Client/Server-Sitzungen Keepalive-Pakete gesendet, um zu verhindern, dass die Firewall-Software lange laufende inaktive Verbindungen schließt.  |
| Operations Center                     | HTTPS: 11090                   | Eingehend | Diese Ports werden für den Web-Browser des Operations Center verwendet. Sie können eine alternative Portnummer angeben.   |
| Port für den Clientverwaltungsservice | Client-Port: 9028              | Eingehend | Wenn Sie planen, IBM Spectrum Protect-Clientverwaltungsservices zu verwenden, muss der Zugriff auf den Port für den Clientverwaltungsservice über das Operations Center möglich sein. Stellen Sie sicher, dass Verbindungen nicht durch Firewalls verhindert werden können. Der Clientverwaltungsservice verwendet den TCP-Port des Servers für den Clientknoten für die Authentifizierung unter Verwendung einer Verwaltungssitzung. |

#### Zugehörige Tasks:

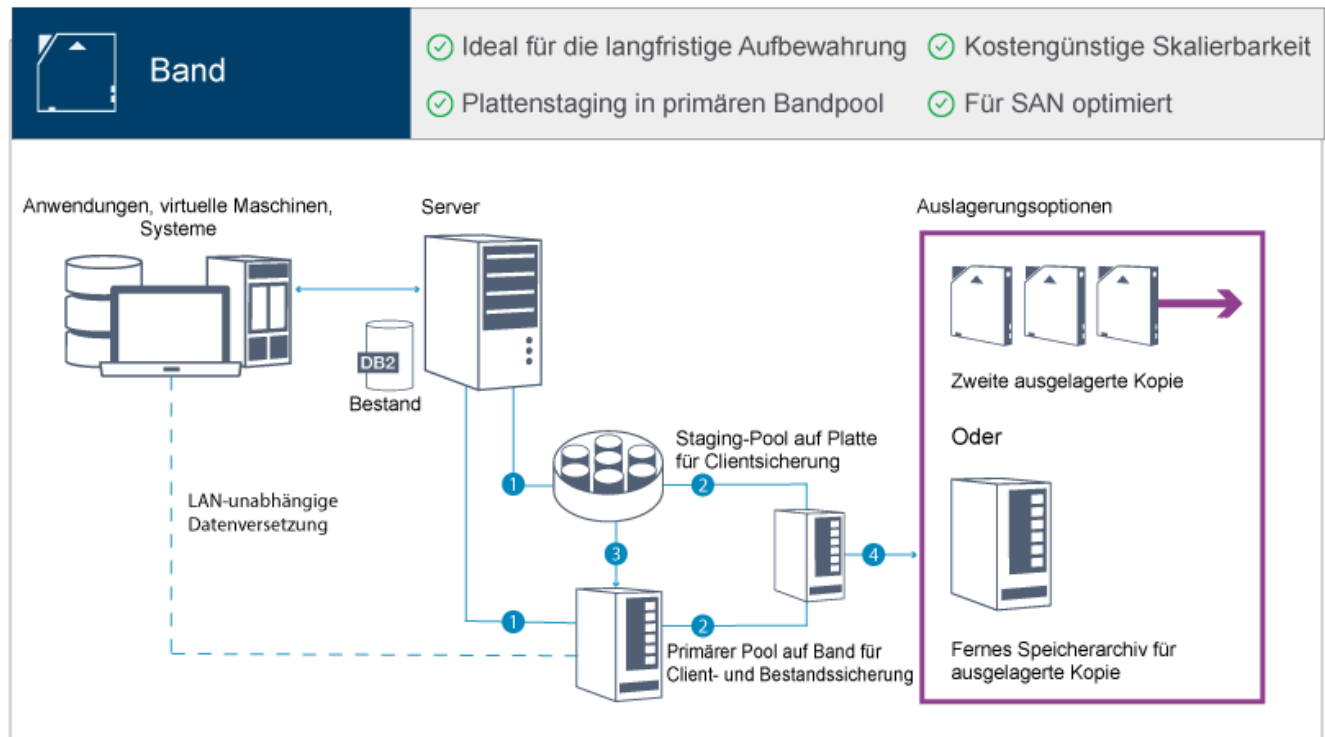
☞ Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen

#### Zugehörige Verweise:

- ☞ Serveroption ADMINONCLIENTPORT
- ☞ DEFINE SERVER (Server für Übertragung zwischen Servern definieren)
- ☞ Serveroption TCPADMINPORT
- ☞ Serveroption TCPPORT

## Implementierung einer bandbasierten Datenschutzlösung

Implementieren Sie die bandbasierte Lösung, die die Platte-Platte-Band-Sicherung und Plattenstaging zur Optimierung des Speichers verwendet. Durch die Implementierung der Bandspeicherlösung können Sie die langfristige Aufbewahrung von Daten ermöglichen und kostengünstige Skalierbarkeit erzielen.



Tipp: Die beschriebene Lösung umfasst keine Knotenreplikation. Wenn die Knotenreplikation jedoch zum Sichern eines Speicherpools von Platte auf Platte verwendet werden soll, müssen Sie sicherstellen, dass die Replikationsoperation abgeschlossen ist, bevor Daten von Platte auf Band umgelagert werden. Sie können die Knotenreplikation auch verwenden, um einen Speicherpool auf einer lokalen Bandoeinheit in einem Kopierspeicherpool auf einer lokalen Bandoeinheit zu sichern.

## Implementierungsroadmap

---

Die folgenden Schritte sind zum Konfigurieren einer bandbasierten Lösung erforderlich.

1. Konfigurieren Sie das System.
2. Installieren Sie den Server und das Operations Center.
3. Konfigurieren Sie den Server und das Operations Center.
4. Schließen Sie Bandeinheiten für den Server an.
5. Konfigurieren Sie Bandarchive für die Verwendung durch den Server.
6. Konfigurieren Sie eine Speicherpoolhierarchie.
7. Installieren und konfigurieren Sie Clients.
8. Konfigurieren Sie die LAN-unabhängige Datenversetzung.
9. Wählen Sie ein Verschlüsselungsverfahren aus und konfigurieren Sie die Verschlüsselung.
10. Konfigurieren Sie Bandspeicheroperationen.
11. Schließen Sie die Implementierung ab.

## System konfigurieren

---

Um das System konfigurieren zu können, müssen Sie zunächst Ihre Plattenspeicherhardware und das Serversystem für IBM Spectrum Protect konfigurieren.

### Informationen zu diesem Vorgang

---

Tipp: Es werden Prozeduren zum Konfigurieren des Servers und des Plattenspeichersystems beschrieben. Erste Schritte zum Konfigurieren von Bandeinheiten finden Sie in Bandeinheiten für den Server anschließen.

- Speicherhardware konfigurieren  
Um Plattenspeicher zu optimieren, prüfen Sie die Richtlinien zum Konfigurieren von Plattenspeicher mithilfe von IBM Spectrum Protect. Stellen Sie dann eine Verbindung zwischen dem Server und den Plattenspeichereinheiten her und führen Sie weitere Konfigurationstasks aus.
- Serverbetriebssystem installieren  
Installieren Sie das Betriebssystem auf dem Serversystem und stellen Sie sicher, dass die Voraussetzungen für den IBM Spectrum Protect-Server erfüllt sind. Passen Sie Betriebssystemeinstellungen gemäß Anweisung an.
- Multipath I/O konfigurieren  
Sie können Multipathing für Plattenspeicher aktivieren und konfigurieren. Die mit Ihrer Hardware zur Verfügung gestellte Dokumentation enthält ausführliche Anweisungen.
- Benutzer-ID für den Server erstellen  
Erstellen Sie die Benutzer-ID, die Eigner der IBM Spectrum Protect-Serverinstanz ist. Sie geben diese Benutzer-ID an, wenn Sie die Serverinstanz im Rahmen der Erstkonfiguration des Servers erstellen.
- Dateisysteme für den Server vorbereiten  
Sie müssen die Dateisystemkonfiguration ausführen, damit der Plattenspeicher vom Server verwendet werden kann.

## Speicherhardware konfigurieren

---

Um Plattenspeicher zu optimieren, prüfen Sie die Richtlinien zum Konfigurieren von Plattenspeicher mithilfe von IBM Spectrum Protect. Stellen Sie dann eine Verbindung zwischen dem Server und den Plattenspeichereinheiten her und führen Sie weitere Konfigurationstasks aus.

### Vorbereitende Schritte

---

Richtlinien zum Konfigurieren von Plattenspeicher finden Sie in Prüfliste für Speicherpools auf FILE- oder DISK-Einheiten.

### Vorgehensweise

---

1. Stellen Sie unter Berücksichtigung der folgenden Richtlinien eine Verbindung zwischen dem Server und den Speichereinheiten her:
  - Verwenden Sie einen Switch oder eine Direktverbindung für Fibre Channel-Verbindungen.
  - Berücksichtigen Sie die Anzahl Ports, die verbunden sind, und die erforderliche Bandbreite.
  - Berücksichtigen Sie die Anzahl Ports auf dem Server und die Anzahl Host-Ports auf dem Plattensystem, die verbunden sind.
2. Stellen Sie sicher, dass die Einheitentreiber und die Firmware für das Serversystem, die Adapter und das Betriebssystem aktuell sind und die empfohlenen Versionen haben.
3. Konfigurieren Sie Speicherarrays. Stellen Sie sicher, dass Sie entsprechend geplant haben, um die optimale Leistung zu gewährleisten. Weitere Informationen finden Sie in Planung für Plattenspeicher.

4. Stellen Sie sicher, dass das Serversystem Zugriff auf Plattendatenträger hat, die erstellt werden. Führen Sie die folgenden Schritte aus:
  - a. Wenn das System mit einem Fibre Channel-Switch verbunden ist, verzonen Sie den Server, um die Platten anzuzeigen.
  - b. Ordnen Sie alle Datenträger zu, um dem Plattensystem mitzuteilen, dass diesem spezifischen Server die Anzeige jeder Platte ermöglicht werden soll.
5. Stellen Sie sicher, dass Band- und Platteneinheiten unterschiedliche HBA-Ports verwenden. Steuern Sie die Band- und Plattene/A mithilfe des Speicherbereichsnetzes (SAN).

#### Zugehörige Tasks:

Multipath I/O konfigurieren

## Serverbetriebssystem installieren

---

Installieren Sie das Betriebssystem auf dem Serversystem und stellen Sie sicher, dass die Voraussetzungen für den IBM Spectrum Protect-Server erfüllt sind. Passen Sie Betriebssystemeinstellungen gemäß Anweisung an.

- Installation auf AIX-Systemen  
Führen Sie die folgenden Schritte aus, um AIX auf dem Serversystem zu installieren.
- Installation auf Linux-Systemen  
Führen Sie die folgenden Schritte aus, um Linux x86\_64 auf dem Serversystem zu installieren.
- Installation auf Windows-Systemen  
Installieren Sie Microsoft Windows Server 2012 Standard Edition auf dem Serversystem und bereiten Sie das System für die Installation und Konfiguration des IBM Spectrum Protect-Servers vor.

## Installation auf AIX-Systemen

---

Führen Sie die folgenden Schritte aus, um AIX auf dem Serversystem zu installieren.

### Vorgehensweise

---

1. Installieren Sie AIX Version 7.1, TL4, SP2 oder höher gemäß den Anweisungen des Herstellers.
2. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Anweisungen zur Installation des Betriebssystems.
3. Öffnen Sie die Datei /etc/hosts und führen Sie die folgenden Aktionen aus:

- Aktualisieren Sie die Datei, um die IP-Adresse und den Hostnamen des Servers einzuschließen. Beispiel:

```
192.0.2.7 server.yourdomain.com server
```

- Überprüfen Sie, ob die Datei einen Eintrag für localhost mit der Adresse 127.0.0.1 enthält. Beispiel:

```
127.0.0.1 localhost
```

4. Aktivieren Sie die AIX-I/O Completion Ports (IOCP), indem Sie den folgenden Befehl eingeben:

```
chdev -l iocp0 -P
```

Die Olson-Zeitzonendefinition kann sich auf die Serverleistung auswirken.

5. Um die Leistung zu optimieren, ändern Sie Ihr Systemzeitonenformat von Olson in POSIX. Verwenden Sie das folgende Befehlsformat zum Aktualisieren der Zeitzoneneinstellung:

```
chtz=Ortszeitzone,Datum/Uhrzeit,Datum/Uhrzeit
```

Beispielsweise würden Sie in Tucson, Arizona, wo die Mountain Standard Time gilt, den folgenden Befehl ausgeben, um das Format in das POSIX-Format zu ändern:

```
chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
```

6. Fügen Sie in .profile des Instanzbenutzers einen Eintrag hinzu, um die folgende Umgebung festzulegen:

```
export MALLOCOPTIONS=multiheap:16
```

7. Legen Sie fest, dass das System vollständige Anwendungskerndateien erstellen soll. Geben Sie den folgenden Befehl aus:

```
chdev -l sys0 -a fullcore=true -P
```

8. Stellen Sie für die Kommunikation mit dem Server und dem Operations Center sicher, dass die folgenden Ports für alle Firewalls, die gegebenenfalls vorhanden sind, offen sind:

- Öffnen Sie für die Kommunikation mit dem Server Port 1500.
- Öffnen Sie für die sichere Kommunikation mit dem Operations Center Port 11090 auf dem Hub-Server.

Wenn Sie nicht die Standardwerte für Ports verwenden, stellen Sie sicher, dass die verwendeten Ports offen sind.

9. Aktivieren Sie TCP-Hochleistungsverbesserungen. Geben Sie den folgenden Befehl aus:

```
no -p -o rfc1323=1
```

10. Um optimalen Durchsatz und optimale Zuverlässigkeit zu gewährleisten, kombinieren Sie vier 10-Gb-Ethernet-Ports durch Bonding miteinander. Verwenden Sie das System Management Interface Tool (SMIT), um die Ports durch Bonding unter Verwendung von Etherchannel zu kombinieren. Beim Testen wurden die folgenden Einstellungen verwendet:

```

mode          8023ad
auto_recovery yes      Automatische Wiederherstellung nach
                    Übernahme aktivieren
backup_adapter NONE    Adapter, der beim Fehlschlagen des
                    gesamten Kanals verwendet wird
hash_mode     src_dst_port  Legt fest, wie der abgehende Adapter
                    ausgewählt wird
interval      long        Legt den Intervallwert für den IEEE-Modus
                    802.3ad fest
mode          8023ad     EtherChannel-Betriebsart
netaddr       0          Mit Ping zu überprüfende Adresse
no_loss_failover yes    Verlustfreie Übernahme nach dem Fehl-
                    schlagen des Pingbefehls aktivieren
num_retries   3          Anzahl Wiederholungen für Pingbefehl vor
                    dem Fehlschlagen
retry_time    1          Wartezeit (in Sekunden) zwischen
                    Pingbefehlen
use_alt_addr  no        Alternative EtherChannel-Adresse
                    aktivieren
use_jumbo_frame no      Jumbo-Frames für Gigabit Ethernet
                    aktivieren

```

11. Überprüfen Sie, ob Benutzerprozessressourcengrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, gemäß den Richtlinien in Tabelle 1 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

Tabelle 1. Benutzergrenzwerte (ulimit-Werte)

| Typ des Benutzergrenzwerts                           | Einstellung | Wert      | Befehl zum Abfragen des Werts |
|--|-------------|-----------|-------------------------------|
| Maximale Größe der erstellten Kerndateien            | core        | Unlimited | ulimit -Hc                    |
| Maximale Größe eines Datensegments für einen Prozess | data        | Unlimited | ulimit -Hd                    |
| Maximale Dateigröße                                  | fsize       | Unlimited | ulimit -Hf                    |
| Maximale Anzahl offener Dateien                      | nofile      | 65536     | ulimit -Hn                    |
| Maximale Prozessorzeit in Sekunden                   | cpu         | Unlimited | ulimit -Ht                    |
| Maximale Anzahl Benutzerprozesse                     | nproc       | 16384     | ulimit -Hu                    |

Wenn einer der Benutzergrenzwerte geändert werden muss, führen Sie die Anweisungen in der Dokumentation für Ihr Betriebssystem aus.

## Installation auf Linux-Systemen

Führen Sie die folgenden Schritte aus, um Linux x86\_64 auf dem Serversystem zu installieren.

### Vorbereitende Schritte

Das Betriebssystem wird auf den internen Festplatten installiert. Konfigurieren Sie die internen Festplatten für die Verwendung eines RAID 1-Hardware-Arrays. Wenn Sie beispielsweise ein kleines System konfigurieren, werden die beiden internen 300-GB-Platten in RAID 1 gespiegelt, sodass es aussieht, als würde dem Installationsprogramm des Betriebssystems eine einzelne 300-GB-Platte zur Verfügung stehen.

### Vorgehensweise

1. Installieren Sie Red Hat Enterprise Linux Version 7.1 oder höher gemäß den Anweisungen des Herstellers. Fordern Sie eine bootfähige DVD an, die Red Hat Enterprise Linux Version 7.1 enthält, und starten Sie Ihr System von dieser DVD. Für Installationsoptionen siehe die folgende Anleitung. Wenn ein Element in der folgenden Liste nicht aufgeführt ist, übernehmen Sie die Standardauswahl unverändert.
  - a. Wählen Sie nach dem Starten der DVD im Menü Install or upgrade an existing system (Installation oder Aktualisierung eines bestehenden Systems) aus.
  - b. Wählen Sie in der Eingangsanzeige Test this media & install Red Hat Enterprise Linux 7.1 (Diese Medien überprüfen & Red Hat Enterprise Linux 7.1 installieren) aus.
  - c. Wählen Sie Ihre Sprache und Tastaturbelegung aus.
  - d. Wählen Sie Ihren Standort aus, um die korrekte Zeitzone festzulegen.
  - e. Wählen Sie Software Selection (Softwareauswahl) und in der nächsten Anzeige Server with GUI (Server mit GUI) aus.
  - f. Klicken Sie auf der Installationszusammenfassungsseite auf Installation Destination (Installationsziel) und überprüfen Sie die folgenden Einträge:
    - Die lokale 300-GB-Platte ist als Installationsziel ausgewählt.
    - Unter 'Other Storage Options' (Weitere Speicheroptionen) ist Automatically configure partitioning (Partitionierung automatisch konfigurieren) ausgewählt.
 Klicken Sie auf Done (Fertig).
  - g. Klicken Sie auf Begin Installation (Installation starten). Legen Sie nach dem Start der Installation das Rootkennwort für Ihr Rootbenutzerkonto fest.

Führen Sie nach dem Abschluss der Installation einen Neustart für das System durch und melden Sie sich als Rootbenutzer an. Geben Sie den Befehl `df` aus, um die Basispartitionierung zu überprüfen. Auf einem Testsystem hatte die Erstpartitionierung beispielsweise das folgende Ergebnis zur Folge:

```
[root@tvapp02]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/mapper/rhel-root  50G  3.0G  48G   6% /
devtmpfs        32G   0    32G   0% /dev
tmpfs           32G   92K   32G   1% /dev/shm
tmpfs           32G   8.8M  32G   1% /run
tmpfs           32G   0    32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home 220G  37M  220G   1% /home
/dev/sda1       497M 124M  373M  25% /boot
```

2. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Anweisungen zur Installation des Betriebssystems. Um optimalen Durchsatz und optimale Zuverlässigkeit zu gewährleisten, sollten Sie das Bonding mehrerer Netzports in Erwägung ziehen. Erstellen Sie dazu eine LACP-Netzverbindung (LACP = Link Aggregation Control Protocol), bei der mehrere untergeordnete Ports in einer einzigen logischen Verbindung aggregiert werden. Die bevorzugte Methode ist die Verwendung des Bondmodus 802.3ad, des Werts 100 für die Einstellung `miimon` und der Angabe `'layer3+4'` für die Einstellung `xmit_hash_policy`. Einschränkung: Um eine LACP-Netzverbindung verwenden zu können, muss ein Netzswitch vorhanden sein, der LACP unterstützt.

Weitere Anweisungen zur Konfiguration von Bonding-Netzverbindungen mit Red Hat Enterprise Linux Version 7 finden Sie unter [Create a Channel Bonding Interface](#).

3. Öffnen Sie die Datei `/etc/hosts` und führen Sie die folgenden Aktionen aus:
  - Aktualisieren Sie die Datei, um die IP-Adresse und den Hostnamen des Servers einzuschließen. Beispiel:

```
192.0.2.7  server.yourdomain.com  server
```

- Überprüfen Sie, ob die Datei einen Eintrag für localhost mit der Adresse 127.0.0.1 enthält. Beispiel:

```
127.0.0.1  localhost
```

4. Installieren Sie Komponenten, die für die Serverinstallation erforderlich sind. Führen Sie die folgenden Schritte aus, um ein YUM-Repository (YUM = Yellowdog Updater, Modified) zu erstellen und die vorausgesetzten Pakete zu installieren.

- a. Stellen Sie die DVD für die Installation von Red Hat Enterprise Linux in einem Systemverzeichnis bereit. Um sie beispielsweise im Verzeichnis `/mnt` bereitzustellen, geben Sie den folgenden Befehl aus:

```
mount -t iso9660 -o ro /dev/cdrom /mnt
```

- b. Überprüfen Sie, ob die DVD bereitgestellt wurde, indem Sie den Befehl `mount` ausgeben. Es sollte eine ähnliche Ausgabe wie in dem folgenden Beispiel angezeigt werden:

```
/dev/sr0 on /mnt type iso9660
```

- c. Wechseln Sie in das YUM-Repository-Verzeichnis, indem Sie den folgenden Befehl ausgeben:

```
cd /etc/yum/repos.d
```

Wenn das Verzeichnis `repos.d` nicht vorhanden ist, erstellen Sie es.

- d. Listen Sie den Verzeichnisinhalt auf:

```
ls rhel-source.repo
```

e. Benennen Sie die ursprüngliche repo-Datei um, indem Sie den Befehl mv ausgeben. Beispiel:

```
mv rhel-source.repo rhel-source.repo.orig
```

f. Erstellen Sie mithilfe eines Texteditors eine neue repo-Datei. Um beispielsweise den Editor vi zu verwenden, geben Sie den folgenden Befehl aus:

```
vi rhel71_dvd.repo
```

g. Fügen Sie der neuen repo-Datei die folgenden Zeilen hinzu. Der Parameter baseurl gibt den Verzeichnismountpunkt an:

```
[rhel71_dvd]
name=DVD Redhat Enterprise Linux 7.1
baseurl=file:///mnt
enabled=1
gpgcheck=0
```

h. Installieren Sie das vorausgesetzte Paket ksh.x86\_64, indem Sie den Befehl yum ausgeben. Beispiel:

```
yum install ksh.x86_64
```

Ausnahme: Sie müssen die Bibliotheken compat-libstdc++-33-3.2.3-69.el6.i686 und libstdc++.i686 für Red Hat Enterprise Linux Version 7.1 nicht installieren.

5. Wenn die Softwareinstallation abgeschlossen ist, können Sie die ursprünglichen YUM-Repository-Werte zurückschreiben, indem Sie die folgenden Schritte ausführen:

a. Heben Sie die Bereitstellung der DVD für die Installation von Red Hat Enterprise Linux auf, indem Sie den folgenden Befehl ausgeben:

```
umount /mnt
```

b. Wechseln Sie in das YUM-Repository-Verzeichnis, indem Sie den folgenden Befehl ausgeben:

```
cd /etc/yum/repos.d
```

c. Benennen Sie die von Ihnen erstellte repo-Datei um:

```
mv rhel71_dvd.repo rhel71_dvd.repo.orig
```

d. Benennen Sie die ursprüngliche Datei wieder in den ursprünglichen Namen um:

```
mv rhel-source.repo.orig rhel-source.repo
```

6. Bestimmen Sie, ob Änderungen an Kernelparametern erforderlich sind. Führen Sie die folgenden Schritte aus:

a. Listen Sie mithilfe des Befehls sysctl -a die Parameterwerte auf.

b. Analysieren Sie die Ergebnisse anhand der Richtlinien in Tabelle 1, um zu bestimmen, ob Änderungen erforderlich sind.

c. Wenn Änderungen erforderlich sind, definieren Sie die Parameter in der Datei /etc/sysctl.conf. Die Dateiänderungen werden angewendet, wenn das System gestartet wird.

Tipp: Passen Sie Kernelparametereinstellungen automatisch an und eliminieren Sie die Notwendigkeit manueller Aktualisierungen dieser Einstellungen. Unter Linux passt die DB2-Datenbanksoftware automatisch die Werte der Kernelparameter für die Interprozesskommunikation (IPC) an und setzt sie auf die bevorzugten Einstellungen. Weitere Informationen zu Kernelparametereinstellungen finden Sie bei Verwendung des Suchbegriffs Linux-Kernelparameter im Produktdokumentation zu IBM DB2 Version 11.1.

Tabelle 1. Optimale Einstellungen für Linux-Kernelparameter

| Parameter  | Beschreibung  |
|--|---|
| kernel.shmmni                                    | Die maximale Anzahl Segmente.   |
| kernel.shmmax                                    | Die maximale Größe eines gemeinsam genutzten Speichersegments (Byte).<br><br>Dieser Parameter muss definiert werden, bevor der IBM Spectrum Protect-Server beim Systemstart automatisch gestartet wird. |
| kernel.shmall                                    | Die maximale Zuordnung von Seiten im gemeinsam genutzten Speicher (Seiten).   |
| kernel.sem                                       | (SEMMSL)  |
| Für den Parameter kernel.sem gibt es vier Werte. | Die maximale Anzahl Semaphore pro Array.  |

| Parameter                 | Beschreibung   |
|---------------------------|--|
|                           | (SEMMNS)<br>Die maximale Anzahl Semaphore pro System.  |
|                           | (SEMOPM)<br>Die maximale Anzahl Operationen pro Semaphoraufwurf.   |
|                           | (SEMMNI)<br>Die maximale Anzahl Arrays.  |
| kernel.msgmni             | Die maximale Anzahl systemweiter Nachrichtenwarteschlangen.  |
| kernel.msgmax             | Die maximale Größe von Nachrichten (Byte).   |
| kernel.msgmnb             | Die standardmäßige maximale Größe der Warteschlange (Byte).  |
| kernel.randomize_va_space | Mit dem Parameter kernel.randomize_va_space wird die Verwendung von Speicher-ASLR für den Kernel konfiguriert. Inaktivieren Sie ASLR, da ASLR Fehler der DB2-Software zur Folge haben kann. Weitere ausführliche Informationen zu Linux-ASLR und DB2 enthält die Technote 1365583. |
| vm.swappiness             | Der Parameter vm.swappiness definiert, ob der Kernel Anwendungsspeicher aus physischem Arbeitsspeicher (RAM) auslagern kann. Weitere Informationen zu Kernelparametern enthält die Produktinformation zu DB2.  |
| vm.overcommit_memory      | Der Parameter vm.overcommit_memory hat Auswirkungen darauf, wie viel virtueller Speicher gemäß dem Kernel zugeordnet werden kann. Weitere Informationen zu Kernelparametern enthält die Produktinformation zu DB2.   |

7. Öffnen Sie Firewall-Ports für die Kommunikation mit dem Server. Führen Sie die folgenden Schritte aus:

a. Legen Sie die von der Netzchnittstelle verwendete Zone fest. Die Zone ist standardmäßig 'public'.

Geben Sie den folgenden Befehl aus:

```
# firewall-cmd --get-active-zones
public
  interfaces: ens4f0
```

b. Um die Standardportadresse für die Kommunikation mit dem Server zu verwenden, öffnen Sie TCP/IP-Port 1500 in der Linux-Firewall.

Geben Sie den folgenden Befehl aus:

```
firewall-cmd --zone=public --add-port=1500/tcp --permanent
```

Wenn ein anderer Wert als der Standardwert verwendet werden soll, können Sie eine Zahl zwischen 1024 und 32767 angeben. Wenn ein anderer Port als der Standardport geöffnet wird, müssen Sie diesen Port bei der Ausführung des Konfigurationsscripts angeben.

c. Wenn Sie planen, dieses System als einen Hub zu verwenden, öffnen Sie Port 11090, den Standardport für die sichere Kommunikation (HTTPS).

Geben Sie den folgenden Befehl aus:

```
firewall-cmd --zone=public --add-port=11090/tcp --permanent
```

d. Laden Sie die Firewalldefinitionen erneut, damit die Änderungen wirksam werden.

Geben Sie den folgenden Befehl aus:

```
firewall-cmd --reload
```

8. Überprüfen Sie, ob Benutzerprozessressourcengrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, gemäß den Richtlinien in Tabelle 2 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

Tabelle 2. Benutzergrenzwerte (ulimit-Werte)

| Typ des Benutzergrenzwerts | Einstellung | Wert | Befehl zum Abfragen des Werts |
|----------------------------|-------------|------|-------------------------------|
|----------------------------|-------------|------|-------------------------------|



| Typ des Benutzergrenzwerts                           | Einstellung | Wert      | Befehl zum Abfragen des Werts |
|--|-------------|-----------|-------------------------------|
| Maximale Größe der erstellten Kerndateien            | core        | Unlimited | ulimit -Hc                    |
| Maximale Größe eines Datensegments für einen Prozess | data        | Unlimited | ulimit -Hd                    |
| Maximale Dateigröße                                  | fsize       | Unlimited | ulimit -Hf                    |
| Maximale Anzahl offener Dateien                      | nofile      | 65536     | ulimit -Hn                    |
| Maximale Prozessorzeit in Sekunden                   | cpu         | Unlimited | ulimit -Ht                    |
| Maximale Anzahl Benutzerprozesse                     | nproc       | 16384     | ulimit -Hu                    |

Wenn einer der Benutzergrenzwerte geändert werden muss, führen Sie die Anweisungen in der Dokumentation für Ihr Betriebssystem aus.

## Installation auf Windows-Systemen

Installieren Sie Microsoft Windows Server 2012 Standard Edition auf dem Serversystem und bereiten Sie das System für die Installation und Konfiguration des IBM Spectrum Protect-Servers vor.

### Vorgehensweise

1. Installieren Sie Windows Server 2016 Standard Edition gemäß den Anweisungen des Herstellers.
2. Ändern Sie die Windows-Kostensteuerungsrichtlinien, indem Sie die folgenden Schritte ausführen.
  - a. Öffnen Sie den Editor für lokale Sicherheitsrichtlinien, indem Sie secpol.msc ausführen.
  - b. Klicken Sie auf Lokale Richtlinien > Sicherheitsoptionen und stellen Sie sicher, dass die folgenden Benutzerkostensteuerungsrichtlinien inaktiviert sind:
    - Administratorbestätigungsmodus für das integrierte Administratorkonto
    - Alle Administratoren im Administratorbestätigungsmodus ausführen
3. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Installationsanweisungen für das Betriebssystem.
4. Wenden Sie Windows-Updates an und aktivieren Sie Zusatzfunktionen (optionale Features), indem Sie die folgenden Schritte ausführen:
  - a. Wenden Sie die neuesten Windows Server 2016-Updates an.
  - b. Installieren und aktivieren Sie das Windows 2012 R2-Feature Microsoft .NET Framework 3.5 über den Windows Server-Manager.
  - c. Aktualisieren Sie, falls erforderlich, die FC- und Ethernet-HBA-Einheitentreiber mit neueren Versionen.
  - d. Installieren Sie den für das verwendete Plattensystem geeigneten Multipath I/O-Treiber.
5. Öffnen Sie den TCP/IP-Standardport (1500) für die Kommunikation mit dem IBM Spectrum Protect-Server. Geben Sie beispielsweise den folgenden Befehl aus:

```
netsh advfirewall firewall add rule name="Sicherungsserver-Port 1500"
dir=in action=allow protocol=TCP localport=1500
```

6. Öffnen Sie auf dem Operations Center-Hub-Server den Standardport für die sichere Kommunikation (HTTPS) mit dem Operations Center. Die Portnummer ist 11090. Geben Sie beispielsweise den folgenden Befehl aus:

```
netsh advfirewall firewall add rule name="Operations Center-Port 11090"
dir=in action=allow protocol=TCP localport=11090
```

## Multipath I/O konfigurieren

Sie können Multipathing für Plattenspeicher aktivieren und konfigurieren. Die mit Ihrer Hardware zur Verfügung gestellte Dokumentation enthält ausführliche Anweisungen.

- AIX-Systeme  
Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.
- Linux-Systeme  
Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.

- Windows-Systeme  
Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.

## AIX-Systeme

---

Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.

### Vorgehensweise

---

1. Bestimmen Sie die Fibre Channel-Portadresse, die für die Hostdefinition auf dem Plattensubsystem verwendet werden muss. Geben Sie den Befehl `lscfg` für jeden Port aus.

- Geben Sie auf kleinen und mittelgroßen Systemen die folgenden Befehle aus:

```
lscfg -vps -l fcs0 | grep "Netzadresse"
lscfg -vps -l fcs1 | grep "Netzadresse"
```

- Geben Sie auf großen Systemen die folgenden Befehle aus:

```
lscfg -vps -l fcs0 | grep "Netzadresse"
lscfg -vps -l fcs1 | grep "Netzadresse"
lscfg -vps -l fcs2 | grep "Netzadresse"
lscfg -vps -l fcs3 | grep "Netzadresse"
```

2. Stellen Sie sicher, dass die folgenden AIX-Dateigruppen installiert sind:

- `devices.common.IBM.mpio.rte`
- `devices.fcp.disk.array.rte`
- `devices.fcp.disk.rte`

3. Geben Sie den Befehl `cfgmgr` aus, damit AIX die Hardware erneut überprüft und verfügbare Platten erkennt. Beispiel:

```
cfgmgr
```

4. Um die verfügbaren Platten aufzulisten, geben Sie den folgenden Befehl aus:

```
lsdev -Ccdisk
```

Es sollte eine ähnliche Ausgabe wie die folgende angezeigt werden:

```
hdisk0 Available 00-00-00 SAS Disk Drive
hdisk1 Available 00-00-00 SAS Disk Drive
hdisk2 Available 01-00-00 SAS Disk Drive
hdisk3 Available 01-00-00 SAS Disk Drive
hdisk4 Available 06-01-02 MPIO IBM 2076 FC Disk
hdisk5 Available 07-01-02 MPIO IBM 2076 FC Disk
...
```

5. Verwenden Sie die Ausgabe des Befehls `lsdev`, um die Einheiten-IDs für jede Platteneinheit zu ermitteln und aufzulisten.

Beispielsweise könnte eine Einheiten-ID `hdisk4` lauten. Sichern Sie die Liste der Einheiten-IDs für die Verwendung bei der Erstellung von Dateisystemen für den IBM Spectrum Protect-Server.

6. Korrelieren Sie die SCSI-Einheiten-IDs zu bestimmten Platten-LUNs aus dem Plattensystem, indem Sie detaillierte Informationen zu allen physischen Datenträgern im System auflisten. Geben Sie den folgenden Befehl aus:

```
lspv -u
```

Auf einem IBM® Storwize-System werden beispielsweise die folgenden Informationen für jede Einheit angezeigt:

```
hdisk4 00f8cf083fd97327 None active
33213600507630081010578000000000003004214503IBMfcp
```

In dem Beispiel ist `6005076300810105780000000000030` die UID für den Datenträger, die von der Storwize-Managementschnittstelle zurückgemeldet wurde.

Um die Plattengröße in Megabyte zu überprüfen und den Wert mit dem für das System aufgelisteten Wert zu vergleichen, geben Sie den folgenden Befehl aus:

```
bootinfo -s hdisk4
```

## Linux-Systeme

---

Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.

1. Editieren Sie die Datei `/etc/multipath.conf`, um Multipathing für Linux-Hosts zu aktivieren. Wenn die Datei `multipath.conf` nicht vorhanden ist, können Sie die Datei erstellen, indem Sie den folgenden Befehl ausgeben:

```
mpathconf --enable
```

Die folgenden Parameter wurden in `multipath.conf` zu Testzwecken auf einem IBM Storwize-System festgelegt:

```
defaults {
    user_friendly_names no
}

devices {
    device {
        vendor "IBM "
        product "2145"
        path_grouping_policy group_by_prio
        user_friendly_names no
        path_selector "round-robin 0"
        prio "alua"
        path_checker "tur"
        failback "immediate"
        no_path_retry 5
        rr_weight uniform
        rr_min_io_rq "1"
        dev_loss_tmo 120
    }
}
```

2. Definieren Sie die Multipath-Option so, dass Multipath zusammen mit dem System gestartet wird. Geben Sie die folgenden Befehle aus:

```
systemctl enable multipathd.service
systemctl start multipathd.service
```

3. Um sicherzustellen, dass Platten für das Betriebssystem sichtbar sind und durch Multipath verwaltet werden, geben Sie den folgenden Befehl aus:

```
multipath -l
```

4. Stellen Sie sicher, dass jede Einheit aufgelistet ist und über so viele Pfade wie erwartet verfügt. Anhand der Größe und Einheiten-ID können Sie die aufgelisteten Platten identifizieren.

Beispielsweise zeigt die folgende Ausgabe, dass einer 2-TB-Platte zwei Pfadgruppen und vier aktive Pfade zugeordnet sind. Die Größe von 2 TB bestätigt, dass die Platte einem Pooldateisystem entspricht. Suchen Sie anhand eines Teils der langen Einheiten-ID-Nummer (in diesem Beispiel 12) in der Managementschnittstelle des Plattensystems nach dem Datenträger.

```
[root@tapsrv01 code]# multipath -l
36005076802810c5098000000000000012 dm-43 IBM,2145
 size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='round-robin 0' prio=0 status=active
|  |- 2:0:1:18 sdcw 70:64 active undef running
|  |- 4:0:0:18 sdgb 131:112 active undef running
`-+- policy='round-robin 0' prio=0 status=enabled
|  |- 1:0:1:18 sdat 66:208 active undef running
|  |- 3:0:0:18 sddy 128:0 active undef running
```

- a. Korrigieren Sie, falls erforderlich, Platten-LUN/Host-Zuordnungen und erzwingen Sie eine erneute Busüberprüfung.  
Beispiel:

```
echo "-- --" > /sys/class/scsi_host/host0/scan
echo "-- --" > /sys/class/scsi_host/host1/scan
echo "-- --" > /sys/class/scsi_host/host2/scan
```

Sie können für eine erneute Überprüfung der Platten-LUN/Host-Zuordnungen auch das System erneut starten.

- b. Stellen Sie sicher, dass Platten jetzt für Multipath I/O verfügbar sind, indem Sie den Befehl `multipath -l` erneut ausgeben.

5. Verwenden Sie die Multipath-Ausgabe, um die Einheiten-IDs für jede Platteneinheit zu ermitteln und aufzulisten.

Beispielsweise ist die Einheiten-ID für Ihre 2-TB-Platte `36005076802810c5098000000000000012`.

Sichern Sie die Liste der Einheiten-IDs für die Verwendung im nächsten Schritt.

Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.

## Vorgehensweise

---

1. Stellen Sie sicher, dass Multipath I/O installiert ist. Installieren Sie, falls erforderlich, weitere anbieterspezifische Multipath-Treiber.
2. Um sicherzustellen, dass Platten für das Betriebssystem sichtbar sind und durch Multipath I/O verwaltet werden, geben Sie den folgenden Befehl aus:

```
c:\Programme\IBM\SDDSM\datapath.exe query device
```

3. Überprüfen Sie die Multipath-Ausgabe und stellen Sie sicher, dass jede Einheit aufgelistet ist und über so viele Pfade wie erwartet verfügt. Anhand der Größe und Einheitenseriennummer können Sie die aufgelisteten Platten identifizieren. Beispielsweise können Sie anhand eines Teils der langen Einheitenseriennummer (in diesem Beispiel 34) in der Managementschnittstelle des Plattensystems nach dem Datenträger suchen. Die Größe von 2 TB bestätigt, dass die Platte einem Speicherpooldateisystem entspricht.

```
DEV#: 4 DEVICE NAME: Disk5 Part0 TYPE: 2145 POLICY: OPTIMIZED
SERIAL: 60050763008101057800000000000034 LUN SIZE: 2.0TB
=====
Path# Adapter/Hard Disk State Mode Select Errors
0 Scsi Port2 Bus0/Disk5 Part0 OPEN NORMAL 0 0
1 Scsi Port2 Bus0/Disk5 Part0 OPEN NORMAL 27176 0
2 Scsi Port3 Bus0/Disk5 Part0 OPEN NORMAL 28494 0
3 Scsi Port3 Bus0/Disk5 Part0 OPEN NORMAL 0 0
```

4. Erstellen Sie unter Verwendung der in der Multipath-Ausgabe im vorherigen Schritt zurückgegebenen Seriennummern eine Liste der Platteneinheiten-IDs.

Beispielsweise ist die Einheiten-ID für Ihre 2-TB-Platte 60050763008101057800000000000034.

Sichern Sie die Liste der Einheiten-IDs für die Verwendung im nächsten Schritt.

5. Um neue Platten online zu schalten und das Lesezugriffsattribut zu löschen, führen Sie diskpart.exe mit den folgenden Befehlen aus. Wiederholen Sie diesen Schritt für jede der Platten:

```
diskpart
select Disk 1
online disk
attribute disk clear readonly
select Disk 2
online disk
attribute disk clear readonly
< ... >
select Disk 49
online disk
attribute disk clear readonly
exit
```

## Benutzer-ID für den Server erstellen

---

Erstellen Sie die Benutzer-ID, die Eigner der IBM Spectrum Protect-Serverinstanz ist. Sie geben diese Benutzer-ID an, wenn Sie die Serverinstanz im Rahmen der Erstkonfiguration des Servers erstellen.

### Informationen zu diesem Vorgang



---

Sie können nur Kleinbuchstaben (a-z), Ziffern (0-9) und das Unterstrichungszeichen (\_) für die Benutzer-ID angeben. Die Benutzer-ID und der Gruppenname müssen den folgenden Regeln entsprechen:

- Die Länge darf 8 Zeichen nicht überschreiten.
- Die Benutzer-ID und der Gruppenname dürfen nicht mit *ibm*, *sql*, *sys* oder einer Ziffer beginnen.
- Die Benutzer-ID und der Gruppenname dürfen nicht *user*, *admin*, *guest*, *public*, *local* oder ein in SQL reserviertes Wortes sein.

## Vorgehensweise

---

1. Erstellen Sie mithilfe von Betriebssystembefehlen eine Benutzer-ID.
  -  AIX-Betriebssysteme  Linux-Betriebssysteme Erstellen Sie eine Gruppe und eine Benutzer-ID im Ausgangsverzeichnis des Benutzers, der Eigner der Serverinstanz ist.

Um beispielsweise die Benutzer-ID `tsminst1` in der Gruppe `tsmsrvrs` mit dem Kennwort `tsminst1` zu erstellen, geben Sie die folgenden Befehle mit einer ID für einen Benutzer mit Verwaltungsaufgaben aus:


#### AIX-Betriebssysteme

```
mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

#### Linux-Betriebssysteme

```
groupadd tsmsrvrs
useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
passwd tsminst1
```

Melden Sie sich von Ihrem System ab und anschließend wieder an. Wechseln Sie zu dem von Ihnen erstellten Benutzerkonto. Verwenden Sie ein interaktives Anmeldeprogramm, wie beispielsweise Telnet, damit Sie zur Eingabe des Kennworts aufgefordert werden und es, falls erforderlich, ändern können.

-  Windows-Betriebssysteme Erstellen Sie eine Benutzer-ID und fügen Sie dann die neue ID der Gruppe 'Administratoren' hinzu. Um beispielsweise die Benutzer-ID `tsminst1` zu erstellen, geben Sie den folgenden Befehl aus:

```
net user tsminst1 * /add
```

Fügen Sie, nachdem Sie für den neuen Benutzer ein Kennwort erstellt und bestätigt haben, die Benutzer-ID der Gruppe 'Administratoren' hinzu, indem Sie die folgenden Befehle ausgeben:

```
net localgroup Administratoren tsminst1 /add
net localgroup DB2ADMNS tsminst1 /add
```

2. Melden Sie die neue Benutzer-ID ab.

## Dateisysteme für den Server vorbereiten

---

Sie müssen die Dateisystemkonfiguration ausführen, damit der Plattenspeicher vom Server verwendet werden kann.

- Dateisysteme auf AIX-Systemen vorbereiten  
Sie müssen Datenträgergruppen, logische Datenträger und Dateisysteme für den Server mithilfe von AIX Logical Volume Manager erstellen.
- Dateisysteme auf Linux-Systemen vorbereiten  
Sie müssen ext4- oder xfs-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.
- Dateisysteme auf Windows-Systemen vorbereiten  
Sie müssen NTFS-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

## Dateisysteme auf AIX-Systemen vorbereiten

---

Sie müssen Datenträgergruppen, logische Datenträger und Dateisysteme für den Server mithilfe von AIX Logical Volume Manager erstellen.

### Vorgehensweise

---

1. Erhöhen Sie die Warteschlangenlänge und die maximale Übertragungsgröße für alle verfügbaren `hdiskX`-Platten. Geben Sie für jede Platte die folgenden Befehle aus:

```
chdev -l hdisk4 -a max_transfer=0x100000
chdev -l hdisk4 -a queue_depth=32
chdev -l hdisk4 -a reserve_policy=no_reserve
chdev -l hdisk4 -a algorithm=round_robin
```

Sie dürfen diese Befehle nicht für interne Betriebssystemplatten, beispielsweise `hdisk0`, ausführen.

2. Erstellen Sie Datenträgergruppen für die IBM Spectrum Protect-Datenbank, die aktive Protokolldatei, das Archivprotokoll, die Datenbanksicherung und den Speicherpool. Geben Sie den Befehl `mkvg` unter Angabe der Einheiten-IDs für die entsprechenden zuvor ermittelten Platten aus.

Wenn beispielsweise die Einheitennamen `hdisk4`, `hdisk5` und `hdisk6` Datenbankplatten entsprechen, schließen Sie diese in die Datenbankdatenträgergruppe ein.

Systemgröße: Die folgenden Befehle basieren auf einer Konfiguration für ein mittelgroßes System. Für kleine und große Systeme müssen Sie die Syntax wie erforderlich anpassen.

```

mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
mkvg -S -y tsmactlog hdisk5
mkvg -S -y tsmarchlog hdisk6
mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49

```

- Bestimmen Sie die Namen der physischen Datenträger und die Anzahl freier physischer Partitionen, die beim Erstellen logischer Datenträger verwendet werden sollen. Geben Sie den Befehl `lsvg` für jede Datenträgergruppe aus, die Sie im vorherigen Schritt erstellt haben.

Beispiel:

```
lsvg -p tsmdb
```

Die Ausgabe sieht ähnlich wie die folgende aus. Die Spalte *FREE PPs* gibt die freien physischen Partitionen an:

```

tsmdb:
PV_NAME  PV STATE  TOTAL PPs  FREE PPs  FREE DISTRIBUTION
hdisk4   active    1631      1631      327..326..326..326..326
hdisk5   active    1631      1631      327..326..326..326..326
hdisk6   active    1631      1631      327..326..326..326..326

```

- Erstellen Sie mit dem Befehl `mklv` logische Datenträger in jeder Datenträgergruppe. Die Datenträgergröße, die Datenträgergruppe und die Einheitenamen sind, abhängig von der Größe Ihres Systems und Variationen in Ihrer Plattenkonfiguration, unterschiedlich.

Um beispielsweise die Datenträger für die IBM Spectrum Protect-Datenbank auf einem mittelgroßen System zu erstellen, geben Sie die folgenden Befehle aus:

```

mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4

```

- Formatieren Sie Dateisysteme auf jedem logischen Datenträger mit dem Befehl `crfs`.

Um beispielsweise die Dateisysteme für die Datenbank auf einem mittelgroßen System zu formatieren, geben Sie die folgenden Befehle aus:

```

crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes

```

- Führen Sie für alle neu erstellten Dateisysteme einen Mount durch, indem Sie den folgenden Befehl eingeben:

```
mount -a
```

- Listen Sie alle Dateisysteme auf, indem Sie den Befehl `df` ausgeben. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Überprüfen Sie außerdem den verfügbaren Speicherbereich.

Das folgende Beispiel der Befehlsausgabe zeigt, dass der Umfang des belegten Speicherbereichs normalerweise 1 % beträgt:

```

tapsrv07> df -g /tsminst1/*
Filesystem      GB blocks  Free    %Used  Iused  %Iused  Mounted on
/dev/tsmact00   195.12    194.59  1%      4       1%      /tsminst1/TSMalog

```

- Überprüfen Sie, ob die in Benutzer-ID für den Server erstellen erstellte Benutzer-ID Schreib-/Lesezugriff auf die Verzeichnisse für den Server hat.

## Dateisysteme auf Linux-Systemen vorbereiten

Sie müssen ext4- oder xfs-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

### Vorgehensweise

- Verwenden Sie die zuvor generierte Liste der Einheiten-IDs und geben Sie den Befehl `mkfs` aus, um für jede LUN-Speichereinheit ein Dateisystem zu erstellen und zu formatieren. Geben Sie die Einheiten-ID im Befehl an. Siehe die folgenden Beispiele.

Formatieren Sie für die Datenbank ext4-Dateisysteme:

```
mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c50980000000000012
```

Formatieren Sie für Speicherpool-LUNs xfs-Dateisysteme:

```
mkfs -t xfs /dev/mapper/3600507630081010578000000000002c3
```

Abhängig davon, wie viele verschiedene Einheiten vorhanden sind, können Sie den Befehl mkfs bis zu 50 Mal ausgeben.

2. Erstellen Sie Mountpunktverzeichnisse für Dateisysteme.

Geben Sie den Befehl mkdir für jedes Verzeichnis aus, das erstellt werden muss. Verwenden Sie die in den Arbeitsblättern zur Planung verwendeten Verzeichniswerte.

Um beispielsweise das Serverinstanzverzeichnis unter Verwendung des Standardwerts zu erstellen, geben Sie den folgenden Befehl aus:

```
mkdir /tsminst1
```

Wiederholen Sie den Befehl mkdir für jedes Dateisystem.

3. Fügen Sie in der Datei /etc/fstab für jedes Dateisystem einen Eintrag hinzu, damit für die Dateisysteme beim Serverstart automatisch ein Mount durchgeführt wird.

Beispiel:

```
/dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
```

4. Führen Sie für die Dateisysteme, die der Datei /etc/fstab hinzugefügt wurden, einen Mount durch, indem Sie den Befehl mount -a ausgeben.

5. Listen Sie alle Dateisysteme auf, indem Sie den Befehl df ausgeben. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Überprüfen Sie außerdem den verfügbaren Speicherbereich. Das folgende Beispiel für ein IBM® Storwize-System zeigt, dass der Umfang des belegten Speicherbereichs normalerweise 1 % beträgt:

```
[root@tapsrv04 ~]# df -h /tsminst1/*
Filesystem                                Size  Used Avail Use% Mounted on
/dev/mapper/36005076300810105780000000000003 134G  188M 132G   1%  /tsminst1/TSMalog
```

6. Überprüfen Sie, ob die in Benutzer-ID für den Server erstellen erstellte Benutzer-ID Schreib-/Lesezugriff auf die Verzeichnisse für den IBM Spectrum Protect-Server hat.

## Dateisysteme auf Windows-Systemen vorbereiten

---

Sie müssen NTFS-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

### Vorgehensweise

---

1. Erstellen Sie Mountpunktverzeichnisse für Dateisysteme.

Geben Sie den Befehl md für jedes Verzeichnis aus, das erstellt werden muss. Verwenden Sie die in den Arbeitsblättern zur Planung verwendeten Verzeichniswerte. Um beispielsweise das Serverinstanzverzeichnis unter Verwendung des Standardwerts zu erstellen, geben Sie den folgenden Befehl aus:

```
md c:\tsminst1
```

Wiederholen Sie den Befehl md für jedes Dateisystem.

2. Erstellen Sie für jede Platten-LUN, die einem Verzeichnis unter dem Serverinstanzverzeichnis zugeordnet ist, unter Verwendung des Windows-Datenträgermanagers (Volume-Manager) einen Datenträger.

Rufen Sie Server-Manager > Datei- und Speicherdienste auf und führen Sie die folgenden Schritte für jede Platte aus, die der im vorherigen Schritt erstellten LUN-Zuordnung entspricht:

- Schalten Sie die Platte online.
- Initialisieren Sie die Platte mit dem GPT-Basistyp, dem Standardwert.
- Erstellen Sie einen einfachen Datenträger, der den gesamten Speicherbereich auf der Platte belegt. Formatieren Sie das Dateisystem mit NTFS und ordnen Sie einen Kennsatz zu, der den Zweck des Datenträgers angibt, wie beispielsweise TSMfile00. Ordnen Sie den neuen Datenträger keinem Laufwerksbuchstaben zu. Ordnen Sie den Datenträger stattdessen einem Verzeichnis unter dem Instanzverzeichnis zu, wie beispielsweise C:\tsminst1\TSMfile00.  
Tipp: Legen Sie den Datenträgerkennsatz und die Bezeichnungen für Verzeichniszuordnungen auf der Basis der Größe der aufgelisteten Platte fest.

3. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Listen Sie alle Dateisysteme auf, indem Sie den Befehl mountvol ausgeben; überprüfen Sie dann die Ausgabe. Beispiel:

```
\\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
C:\tsminst1\TSMdbspace00\
```

4. Starten Sie nach dem Abschluss der Plattenkonfiguration das System erneut.

## Nächste Schritte

---

Mithilfe von Windows Explorer können Sie den Umfang des freien Speicherbereichs für jeden Datenträger prüfen.

## Server und das Operations Center installieren

---

Verwenden Sie den grafisch orientierten Assistenten von IBM® Installation Manager, um die Komponenten zu installieren.

- Installation auf AIX- und Linux-Systemen  
Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.
- Installation auf Windows-Systemen  
Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.

## Installation auf AIX- und Linux-Systemen

---

Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.


## Vorbereitende Schritte

---

Überprüfen Sie, ob das Betriebssystem auf die erforderliche Sprache gesetzt ist. Standardmäßig entspricht die Sprache für das Betriebssystem der Sprache für den Installationsassistenten.

## Vorgehensweise

---

1.  Überprüfen Sie, ob die erforderlichen RPM-Dateien auf Ihrem System installiert sind.

Ausführliche Informationen finden Sie in Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren.

2. Überprüfen Sie vor dem Herunterladen des Installationspakets, ob genügend Speicherbereich zum Speichern der Installationsdateien vorhanden ist, wenn die Dateien aus dem Produktpaket extrahiert werden. Informationen zum Speicherbedarf enthält das Downloaddokument unter Technote 4042992.
3. Rufen Sie Passport Advantage auf und laden Sie die Paketdatei in ein leeres Verzeichnis Ihrer Wahl herunter.
4. Stellen Sie sicher, dass für das Paket die Berechtigung zur Ausführung festgelegt ist. Ändern Sie, falls erforderlich, die Dateiberechtigungen, indem Sie den folgenden Befehl ausgeben:

```
chmod a+x Paketname.bin
```

5. Extrahieren Sie das Paket, indem Sie den folgenden Befehl ausgeben:

```
./Paketname.bin
```

Dabei ist *Paketname* der Name der Downloaddatei.

6.  Stellen Sie sicher, dass der folgende Befehl aktiviert ist, damit die Assistenten korrekt ausgeführt werden:

```
lsuser
```

Standardmäßig ist der Befehl aktiviert.

7. Wechseln Sie in das Verzeichnis, in das die ausführbare Datei gestellt wurde.
8. Starten Sie den Installationsassistenten, indem Sie den folgenden Befehl ausgeben:

```
./install.sh
```

Wenn Sie die zu installierenden Pakete auswählen, wählen Sie sowohl den Server als auch das Operations Center aus.

## Nächste Schritte

---

- Wenn während des Installationsprozesses Fehler auftreten, werden die Fehler in Protokolldateien aufgezeichnet, die im Protokollverzeichnis von IBM Installation Manager gespeichert sind.  
  
Um Installationsprotokolldateien in Installation Manager anzuzeigen, klicken Sie auf Datei > Protokoll anzeigen. Um diese Protokolldateien in Installation Manager zu erfassen, klicken Sie auf Hilfe > Daten zur Fehleranalyse exportieren.
- Rufen Sie nach der Installation des Servers, aber vor der Anpassung des Servers für Ihre Verwendung die IBM Spectrum Protect-Unterstützungssite auf. Klicken Sie auf Support und Downloads und wenden Sie alle zutreffenden Fixes an.



- Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren  
RPM-Dateien sind für den grafisch orientierten Assistenten von IBM Installation Manager erforderlich.

## Installation auf Windows-Systemen

---

Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.

### Vorbereitende Schritte

---

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Überprüfen Sie, ob das Betriebssystem auf die erforderliche Sprache gesetzt ist. Standardmäßig entspricht die Sprache für das Betriebssystem der Sprache für den Installationsassistenten.
- Stellen Sie sicher, dass die Benutzer-ID, die während der Installation verwendet werden soll, für einen Benutzer mit der Berechtigung eines lokalen Administrators gilt.

### Vorgehensweise

---

1. Überprüfen Sie vor dem Herunterladen des Installationspakets, ob genügend Speicherbereich zum Speichern der Installationsdateien vorhanden ist, wenn die Dateien aus dem Produktpaket extrahiert werden. Informationen zum Speicherbedarf enthält das Downloaddokument unter Technote 4042993.
2. Rufen Sie Passport Advantage auf und laden Sie die Paketdatei in ein leeres Verzeichnis Ihrer Wahl herunter.
3. Wechseln Sie in das Verzeichnis, in das die ausführbare Datei gestellt wurde.
4. Doppelklicken Sie auf die ausführbare Datei, um die Datei in das aktuelle Verzeichnis zu extrahieren.
5. Starten Sie in dem Verzeichnis, in das die Installationsdateien extrahiert wurden, den Installationsassistenten, indem Sie auf die Datei `install.bat` doppelklicken. Wenn Sie die zu installierenden Pakete auswählen, wählen Sie sowohl den Server als auch das Operations Center aus.

### Nächste Schritte

---

- Wenn während des Installationsprozesses Fehler auftreten, werden die Fehler in Protokolldateien aufgezeichnet, die im Protokollverzeichnis von IBM® Installation Manager gespeichert sind.

Um Installationsprotokolldateien in Installation Manager anzuzeigen, klicken Sie auf Datei > Protokoll anzeigen. Um diese Protokolldateien in Installation Manager zu erfassen, klicken Sie auf Hilfe > Daten zur Fehleranalyse exportieren.

- Rufen Sie nach der Installation des Servers, aber vor der Anpassung des Servers für Ihre Verwendung die IBM Spectrum Protect-Unterstützungssite auf. Klicken Sie auf Support und Downloads und wenden Sie alle zutreffenden Fixes an.

## Server und das Operations Center konfigurieren

---

Nachdem Sie die Komponenten installiert haben, führen Sie die Konfiguration für den IBM Spectrum Protect-Server und das Operations Center aus.

- Serverinstanz konfigurieren  
Verwenden Sie den IBM Spectrum Protect-Assistenten für die Serverinstanzkonfiguration, um die Erstkonfiguration für den Server auszuführen.
- Client für Sichern/Archivieren installieren  
Installieren Sie als Best Practice den IBM Spectrum Protect-Client für Sichern/Archivieren auf dem Serversystem, sodass der Verwaltungsbefehlszeilenclient und der Scheduler verfügbar sind.
- Optionen für den Server festlegen  
Überprüfen Sie die Serveroptionsdatei, die mit dem IBM Spectrum Protect-Server installiert wird, um sicherzustellen, dass die korrekten Werte für Ihr System festgelegt sind.
- Sicherheitskonzepte  
Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.
- Operations Center konfigurieren  
Führen Sie nach der Installation des Operations Center die folgenden Konfigurationsschritte aus, um mit der Verwaltung Ihrer Speicherumgebung zu beginnen.
- Produktlizenz registrieren  
Verwenden Sie zum Registrieren Ihrer Lizenz für das Produkt IBM Spectrum Protect den Befehl `REGISTER LICENSE`.
- Datenaufbewahrungsregeln für Ihr Unternehmen definieren  
Nachdem Sie einen Verzeichniscontainerspeicherpool für die Datenduplizierung erstellt haben, aktualisieren Sie die

Serverstandardmaßnahme für die Verwendung des neuen Speicherpools. Die Seite Services im Operations Center wird vom Assistenten Speicherpool hinzufügen zur Ausführung dieser Task geöffnet.

- Zeitpläne für Serververwaltungsaktivitäten definieren  
Erstellen Sie Zeitpläne für jede Serververwaltungsoperation, indem Sie den Befehl DEFINE SCHEDULE im Command Builder des Operations Center verwenden.
- Clientzeitpläne definieren  
Erstellen Sie mithilfe des Operations Center Zeitpläne für Clientoperationen.

## Serverinstanz konfigurieren

---

Verwenden Sie den IBM Spectrum Protect-Assistenten für die Serverinstanzkonfiguration, um die Erstkonfiguration für den Server auszuführen.


### Vorbereitende Schritte

---

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

 AIX-Betriebssysteme  Linux-Betriebssysteme

- Auf dem System, auf dem IBM Spectrum Protect installiert wurde, muss der X Window System-Client vorhanden sein. Außerdem muss ein X Window System-Server auf Ihrem Desktop ausgeführt werden.
- Für das System muss das Secure Shell-Protokoll (SSH-Protokoll) aktiviert sein. Stellen Sie sicher, dass der Port auf den Standardwert 22 gesetzt ist und dass der Port nicht durch eine Firewall blockiert wird. Sie müssen die Kennwortauthentifizierung in der Datei `sshd_config` im Verzeichnis `/etc/ssh/` aktivieren. Stellen Sie außerdem sicher, dass der SSH-Dämonservice über die Zugriffsberechtigungen verfügt, um mithilfe des Werts `localhost` eine Verbindung zum System herstellen zu können.
- Sie müssen sich mit der Benutzer-ID, die Sie für die Serverinstanz erstellt hatten, unter Verwendung des SSH-Protokolls bei IBM Spectrum Protect anmelden können. Wenn Sie den Assistenten verwenden, müssen Sie diese Benutzer-ID und das Kennwort für den Zugriff auf dieses System angeben.
- Wenn Sie in den vorhergehenden Schritten Änderungen an den Einstellungen vorgenommen haben, starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.

 Windows-Betriebssysteme Überprüfen Sie, ob der Remoteregistrierungsdienst gestartet wurde, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie auf Start > Verwaltung > Dienste. Wählen Sie im Fenster Dienste Remoteregistrierung aus. Wurde der Dienst nicht gestartet, klicken Sie auf Starten.
2. Stellen Sie sicher, dass die Ports 137, 139 und 445 nicht durch eine Firewall blockiert sind:
  - a. Klicken Sie auf Start > Systemsteuerung > Windows-Firewall.
  - b. Wählen Sie Erweiterte Einstellungen aus.
  - c. Wählen Sie Eingehende Regeln aus.
  - d. Wählen Sie Neue Regel aus.
  - e. Erstellen Sie eine Portregel für die TCP-Ports 137, 139 und 445, um Verbindungen für Domänennetze und private Netze zu ermöglichen.
3. Konfigurieren Sie die Benutzerkontensteuerung, indem Sie auf die Optionen für die lokale Sicherheitsrichtlinie zugreifen und die folgenden Schritte ausführen:
  - a. Klicken Sie auf Start > Verwaltung > Lokale Sicherheitsrichtlinie. Erweitern Sie Lokale Richtlinien > Sicherheitsoptionen.
  - b. Falls noch nicht bereits aktiviert, aktivieren Sie das integrierte Administratorkonto, indem Sie Konten: Administratorkontostatus > Aktivieren > OK auswählen.
  - c. Falls noch nicht bereits inaktiviert, inaktivieren Sie die Benutzerkontensteuerung für alle Windows-Administratoren, indem Sie Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen > Inaktivieren > OK auswählen.
  - d. Falls noch nicht bereits inaktiviert, inaktivieren Sie die Benutzerkontensteuerung für das integrierte Administratorkonto, indem Sie Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto > Inaktivieren > OK auswählen.
4. Wenn Sie in den vorhergehenden Schritten Änderungen an den Einstellungen vorgenommen haben, starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.

### Informationen zu diesem Vorgang




---



Der Assistent kann gestoppt und erneut gestartet werden, der Server ist jedoch erst betriebsbereit, wenn der gesamte Konfigurationsprozess abgeschlossen ist.


### Vorgehensweise

---

1. Starten Sie die lokale Version des Assistenten.

-   Öffnen Sie das Programm dsmsicfgx im Verzeichnis /opt/tivoli/tsm/server/bin. Dieser Assistent kann nur als Rootbenutzer ausgeführt werden.
  -  Klicken Sie auf Start > Alle Programme > IBM Spectrum Protect > Konfigurationsassistent.
2. Führen Sie die Anweisungen aus, um die Konfiguration auszuführen. Verwenden Sie die während der IBM Spectrum Protect-Systemkonfiguration aufgezeichneten Informationen (siehe Arbeitsblätter zur Planung), um Verzeichnisse und Optionen im Assistenten anzugeben.

  Legen Sie im Fenster Serverinformationen fest, dass der Server automatisch unter Verwendung der Instanzbenutzer-ID gestartet werden soll, wenn das System bootet.

 Mithilfe des Konfigurationsassistenten wird festgelegt, dass der Server automatisch gestartet werden soll, wenn ein Warmstart durchgeführt wird.

## Client für Sichern/Archivieren installieren

Installieren Sie als Best Practice den IBM Spectrum Protect-Client für Sichern/Archivieren auf dem Serversystem, sodass der Verwaltungsbefehlszeilenclient und der Scheduler verfügbar sind.

### Vorgehensweise

Um den Client für Sichern/Archivieren zu installieren, führen Sie die Installationsanweisungen für Ihr Betriebssystem aus.

- UNIX- und Linux-Clients für Sichern/Archivieren installieren
- Windows-Client für Sichern/Archivieren installieren

## Optionen für den Server festlegen

Überprüfen Sie die Serveroptionsdatei, die mit dem IBM Spectrum Protect-Server installiert wird, um sicherzustellen, dass die korrekten Werte für Ihr System festgelegt sind.

### Vorgehensweise

1. Wechseln Sie in das Serverinstanzverzeichnis und öffnen Sie die Datei dsmserv.opt.
2. Überprüfen Sie die Werte in der folgenden Tabelle und Ihre Serveroptionseinstellungen auf der Basis der Systemgröße.

| Serveroption       | Wert  |
|--------------------|---|
| ACTIVELOGDIRECTORY | Während der Konfiguration angegebener Verzeichnispfad |
| ACTIVELOGSIZE      | 131072  |
| ARCHLOGCOMPRESS    | No  |
| ARCHLOGDIRECTORY   | Während der Konfiguration angegebener Verzeichnispfad |
| COMMMETHOD         | TCPIP   |
| COMMTIMEOUT        | 3600  |
| DEVCONFIG          | devconf.dat   |
| EXPINTERVAL        | 0   |
| IDLETIMEOUT        | 60  |
| MAXSESSIONS        | 500   |
| NUMOPENVOLSALLOWED | 20  |
| TCPADMINPORT       | 1500  |
| TCPPORT            | 1500  |
| VOLUMEHISTORY      | volhist.dat   |

Aktualisieren Sie, falls erforderlich, Serveroptionseinstellungen in Übereinstimmung mit den Werten in der Tabelle. Um Aktualisierungen durchzuführen, schließen Sie die Datei dsmserv.opt und definieren Sie die Optionen mit dem Befehl SETOPT in der Verwaltungsbefehlszeilenschnittstelle.

Um beispielsweise die Option IDLETIMEOUT mit 60 zu aktualisieren, geben Sie den folgenden Befehl aus:

```
setopt idletimeout 60
```

3. Um für den Server, die Clients und das Operations Center die sichere Kommunikation zu konfigurieren, überprüfen Sie die Optionen in der folgenden Tabelle.

| Serveroption        | Alle Systemgrößen  |
|---------------------|--|
| SSLDISABLELEGACYTLS | YES  |
| SSLFIPSMODE         | NO   |
| SSLTCPPORT          | Geben Sie die SSL-Portnummer an. Der TCP/IP-DFV-Treiber des Servers wartet an diesem Port auf Anforderungen für SSL-fähige Sitzungen vom Client. |
| SSLTCPADMINPORT     | Geben Sie die Adresse des Ports an, an dem der Server auf Anforderungen von SSL-fähigen Sitzungen des Verwaltungsbefehlszeilenclients wartet.    |
| SSLTLS12            | YES  |

Wenn einer der Optionswerte aktualisiert werden muss, editieren Sie die Datei dmserv.opt unter Verwendung der folgenden Anleitungen:

- Entfernen Sie den Stern am Anfang einer Zeile, um eine Option zu aktivieren.
- Geben Sie in jeder Zeile nur eine einzige Option und den für die Option angegebenen Wert ein.
- Wenn eine Option in mehreren Einträgen in der Datei vorkommt, verwendet der Server den letzten Eintrag.

Sichern Sie Ihre Änderungen und schließen Sie die Datei. Wenn Sie die Datei dmserv.opt direkt editieren, müssen Sie den Server erneut starten, damit die Änderungen wirksam werden.

## Sicherheitskonzepte

Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.

### Transport Layer Security

Mithilfe des Protokolls Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) können Sie Transportschichtsicherheit für eine sichere Verbindung zwischen Servern, Clients und Speicheragenten bereitstellen. Wenn Sie Daten zwischen dem Server, dem Client und dem Speicheragenten austauschen, verwenden Sie SSL oder TLS zum Verschlüsseln der Daten.

**Tipp:** In der gesamten IBM Spectrum Protect-Dokumentation gilt jede Angabe von "SSL" oder zum "Auswählen von SSL" für TLS.

SSL wird von Global Security Kit (GSKit) bereitgestellt, das zusammen mit dem IBM Spectrum Protect-Server installiert wird, der vom Server, vom Client und vom Speicheragenten verwendet wird.

**Einschränkung:** Sie dürfen die SSL- oder TLS-Protokolle nicht für die Kommunikation mit einer DB2-Datenbankinstanz verwenden, die von IBM Spectrum Protect-Servern verwendet wird.

Jeder Server, Client oder Speicheragent, der SSL ermöglicht, muss ein vertrauenswürdiges selbst signiertes Zertifikat verwenden oder ein eindeutiges Zertifikat anfordern, das von einer Zertifizierungsstelle (CA) signiert ist. Sie können Ihre eigenen Zertifikate verwenden oder Zertifikate bei einer Zertifizierungsstelle (CA) kaufen. Jedes der Zertifikate muss installiert und der Schlüsseldatenbank auf dem IBM Spectrum Protect-Server, -Client oder -Speicheragenten hinzugefügt werden. Das Zertifikat wird von dem SSL-Client oder -Server geprüft, der die SSL-Kommunikation anfordert oder einleitet. Einige CA-Zertifikate sind in der Schlüsseldatenbank standardmäßig vorinstalliert.

SSL wird auf dem IBM Spectrum Protect-Server, -Client und -Speicheragenten unabhängig voneinander konfiguriert.

### Berechtigungsstufen

Für jeden IBM Spectrum Protect-Server sind verschiedene Administratorberechtigungsstufen verfügbar, die die Tasks festlegen, die ein Administrator ausführen kann.

Nach der Registrierung muss einem Administrator Berechtigung erteilt werden, indem ihm eine oder mehrere Administratorberechtigungsstufen zugeordnet werden. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen und anderen Administratoren über den Befehl GRANT AUTHORITY Berechtigungsstufen zuordnen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

Ein Administrator kann andere Administrator-IDs registrieren, den IDs Berechtigungsstufen zuordnen, IDs umbenennen, IDs entfernen und IDs für den Server sperren oder entsperren.

Ein Administrator kann den Zugriff auf bestimmte Clientknoten für Rootbenutzer-IDs und Nicht-Rootbenutzer-IDs steuern. Standardmäßig kann eine Nicht-Rootbenutzer-ID keine Daten auf dem Knoten sichern. Ändern Sie mit dem Befehl UPDATE NODE die Knoteneinstellungen, um Sicherungen zu ermöglichen.

## Kennwörter

Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer beim Zugriff auf den Server ein Kennwort eingeben.

Verwenden Sie LDAP (Lightweight Directory Access Protocol), um strikere Anforderungen für Kennwörter anzuwenden. Weitere Informationen finden Sie in Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1).

Tabelle 1. Merkmale der Kennwortauthentifizierung

| Merkmale                                   | Weitere Informationen  |
|--|--|
| Abhängigkeit von der Groß-/Kleinschreibung | Nicht von der Groß-/Kleinschreibung abhängig.  |
| Standardwert für Kennwortablauf            | 90 Tage.<br>Der Ablaufzeitraum beginnt mit der ersten Registrierung einer Administrator-ID oder eines Clientknotens beim Server. Wenn das Kennwort innerhalb dieses Zeitraums nicht geändert wird, muss das Kennwort beim nächsten Zugriff des Benutzers auf den Server geändert werden. |
| Ungültige Kennworteingabeversuche          | Sie können einen Grenzwert für aufeinanderfolgende ungültige Kennworteingabeversuche für alle Clientknoten definieren. Wenn der Grenzwert überschritten wird, sperrt der Server den Knoten.  |
| Kennwortlänge                              | Der Administrator kann eine Mindestlänge angeben.  |

## Sitzungssicherheit

Die Sitzungssicherheit ist die Sicherheitsstufe, die für die Kommunikation zwischen IBM Spectrum Protect-Clientknoten, -Verwaltungsclients und -Servern verwendet wird und mit dem Parameter SESSIONSECURITY festgelegt wird.

Der Parameter SESSIONSECURITY kann auf einen der folgenden Werte gesetzt werden:

- Mit dem Wert STRICT wird die höchste Sicherheitsstufe für die Kommunikation zwischen IBM Spectrum Protect-Servern, -Knoten und -Administratoren durchgesetzt.
- Der Wert TRANSITIONAL gibt an, dass das vorhandene Kommunikationsprotokoll verwendet wird, wenn Sie Ihre IBM Spectrum Protect-Software auf Version 8.1.2 oder höher aktualisieren. Dies ist der Standardwert. Wenn SESSIONSECURITY=TRANSITIONAL angegeben ist, werden strengere Sicherheitseinstellungen automatisch durchgesetzt, da höhere Versionen des TLS-Protokolls verwendet werden, wenn die Software auf Version 8.1.2 oder höher aktualisiert wird. Nachdem ein Knoten, Administrator oder Server die Anforderungen für den Wert STRICT erfüllt, wird die Sitzungssicherheit automatisch in den Wert STRICT geändert und die Entität kann sich nicht mehr unter Verwendung einer Vorgängerversion des Clients oder unter Verwendung früherer TLS-Protokolle authentifizieren.

Weitere Informationen zu den Werten für den Parameter SESSIONSECURITY enthalten die Beschreibungen der folgenden Befehle.

Tabelle 2. Befehle zum Festlegen des Parameters SESSIONSECURITY

| Entität         | Befehl  |
|-----------------|---|
| Clientknoten    | <ul style="list-style-type: none"><li>• REGISTER NODE</li><li>• UPDATE NODE</li></ul>   |
| Administratoren | <ul style="list-style-type: none"><li>• REGISTER ADMIN</li><li>• UPDATE ADMIN</li></ul> |
| Server          | <ul style="list-style-type: none"><li>• DEFINE SERVER</li><li>• UPDATE SERVER</li></ul> |

Administratoren, die sich unter Verwendung des Befehls DSMADMC, des Befehls DSMC oder des Programms dsm authentifizieren, können sich nach der Authentifizierung unter Verwendung von Version 8.1.2 oder höher nicht unter Verwendung einer früheren Version authentifizieren. Die folgenden Tipps liefern Informationen zur Behebung von Authentifizierungsproblemen für Administratoren:  
Tipps:

- Stellen Sie sicher, dass für die gesamte IBM Spectrum Protect-Software, die das Administratorkonto für die Anmeldung verwendet, ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird. Wenn sich ein Administratorkonto über mehrere Systeme anmeldet, stellen Sie sicher, dass das Zertifikat des Servers auf jedem System installiert ist.

- Nachdem sich ein Administrator bei einem Server der Version 8.1.2 oder höher unter Verwendung eines Clients der Version 8.1.2 oder höher authentifiziert hat, kann sich der Administrator nur auf Clients oder Servern authentifizieren, die Version 8.1.2 oder höher verwenden. Ein Administratorbefehl kann von jedem beliebigen System ausgegeben werden.
- Erstellen Sie, falls erforderlich, ein separates Administratorkonto, das nur mit Clients und Servern verwendet wird, die Software der Version 8.1.1 oder früher verwenden.

Setzen Sie die höchste Sicherheitsstufe für die Kommunikation mit dem IBM Spectrum Protect-Server durch, indem Sie sicherstellen, dass alle Knoten, Administratoren und Server die Sitzungssicherheit STRICT verwenden. Mithilfe des Befehls SELECT können Sie feststellen, welche Server, Knoten und Administratoren die Sitzungssicherheit TRANSITIONAL verwenden und für die Verwendung der Sitzungssicherheit STRICT aktualisiert werden sollten.

- Sichere Kommunikation mit Transport Layer Security konfigurieren  
Um Daten zu verschlüsseln und die sichere Kommunikation in Ihrer Umgebung zu ermöglichen, ist Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) auf dem IBM Spectrum Protect-Server und dem Client für Sichern/Archivieren aktiviert. Kommunikationsanforderungen zwischen dem Server und dem Client werden mithilfe eines SSL-Zertifikats geprüft.

#### Zugehörige Tasks:

 Kommunikation schützen

## Operations Center konfigurieren

---

Führen Sie nach der Installation des Operations Center die folgenden Konfigurationsschritte aus, um mit der Verwaltung Ihrer Speicherumgebung zu beginnen.

### Vorbereitende Schritte

---

Wenn Sie zum ersten Mal die Verbindung zum Operations Center herstellen, müssen Sie die folgenden Informationen angeben:

- Verbindungsinformationen für den Server, der als Hub-Server festgelegt werden soll
- Anmeldeberechtigungs-nachweise für eine Administrator-ID, die für diesen Server definiert ist

### Vorgehensweise

---

1. Legen Sie den Hub-Server fest. Geben Sie in einem Web-Browser die folgende Adresse ein:

```
https://Hostname:sicherer_Port/oc
```

Erläuterungen:

- *Hostname* gibt den Namen des Computers an, auf dem das Operations Center installiert ist.
- *Sicherer\_Port* gibt die Portnummer an, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet.

Wenn beispielsweise der Hostname `tsm.storage.mylocation.com` lautet und der standardmäßige sichere Port für das Operations Center (Port 11090) verwendet wird, ist die Adresse wie folgt:

```
https://tsm.storage.mylocation.com:11090/oc
```

Wenn Sie sich zum ersten Mal beim Operations Center anmelden, führt Sie ein Assistent durch eine Erstkonfiguration, um einen neuen Administrator mit Systemberechtigung auf dem Server zu konfigurieren.

2. Konfigurieren Sie die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server, indem Sie das Protokoll Secure Sockets Layer (SSL) konfigurieren.

Führen Sie die Anweisungen in Kommunikation zwischen dem Operations Center und dem Hub-Server schützen aus.

3. Optional: Um einen täglichen E-Mail-Bericht mit einer Zusammenfassung des Systemstatus zu empfangen, konfigurieren Sie Ihre E-Mail-Einstellungen im Operations Center.

Führen Sie die Anweisungen in Systemstatus mithilfe von E-Mail-Berichten verfolgen aus.

- Kommunikation zwischen dem Operations Center und dem Hub-Server schützen  
Um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server zu ermöglichen, fügen Sie das TLS-Zertifikat des Hub-Servers der Truststore-Datei des Operations Center hinzu.

## Produktlizenz registrieren

---

Verwenden Sie zum Registrieren Ihrer Lizenz für das Produkt IBM Spectrum Protect den Befehl REGISTER LICENSE.

## Informationen zu diesem Vorgang


---

Lizenzen werden in Registrierungszertifikatsdateien gespeichert, die Lizenzinformationen für das Produkt enthalten. Die Registrierungszertifikatsdateien befinden sich auf den Installationsmedien und werden während der Installation auf den Server gestellt. Wenn Sie das Produkt registrieren, werden die Lizenzen in einer NODELOCK-Datei im aktuellen Verzeichnis gespeichert.

## Vorgehensweise

---

Registrieren Sie eine Lizenz, indem Sie den Namen der Registrierungszertifikatsdatei angeben, die die Lizenz enthält. Um den Command Builder des Operations Center für diese Task zu verwenden, führen Sie die folgenden Schritte aus.


1. Öffnen Sie das Operations Center.
2. Öffnen Sie den Command Builder des Operations Center, indem Sie den Mauszeiger über das Symbol für Einstellungen  bewegen und auf Command Builder klicken.
3. Geben Sie den Befehl REGISTER LICENSE aus. Um beispielsweise eine IBM Spectrum Protect-Basislizenz zu registrieren, geben Sie den folgenden Befehl aus:

```
register license file=tsmbasic.lic
```

## Nächste Schritte

---

Sichern Sie die Installationsmedien, die Ihre Registrierungszertifikatsdateien enthalten. Möglicherweise müssen Sie Ihre Lizenz erneut registrieren, wenn beispielsweise eine der folgenden Bedingungen erfüllt ist:

- Der Server wird auf einen anderen Computer versetzt.
- Die NODELOCK-Datei ist beschädigt. Der Server speichert Lizenzinformationen in der NODELOCK-Datei, die sich in dem Verzeichnis befindet, von dem aus der Server gestartet wird.
-  Linux-Betriebssysteme Sie ändern den Prozessorchip, der dem Server zugeordnet ist, auf dem der Server installiert ist.

## Datenaufbewahrungsregeln für Ihr Unternehmen definieren

---

Nachdem Sie einen Verzeichniscontainerspeicherpool für die Datenduplizierung erstellt haben, aktualisieren Sie die Serverstandardmaßnahme für die Verwendung des neuen Speicherpools. Die Seite Services im Operations Center wird vom Assistenten Speicherpool hinzufügen zur Ausführung dieser Task geöffnet.

## Vorgehensweise

---

1. Wählen Sie auf der Seite Services im Operations Center die Domäne STANDARD aus und klicken Sie auf Details.
2. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen. Die Seite Maßnahmengruppen gibt den Namen der aktiven Maßnahmengruppe an und listet alle Verwaltungsklassen für diese Maßnahmengruppe auf.
3. Klicken Sie auf die Umschaltfläche Konfigurieren und führen Sie die folgenden Änderungen durch:
  - Ändern Sie das Sicherungsziel für die Verwaltungsklasse STANDARD in den Verzeichniscontainerspeicherpool.
  - Ändern Sie den Wert für die Spalte 'Sicherungen' in Keine Begrenzung.
  - Ändern Sie den Aufbewahrungszeitraum. Setzen Sie den Wert für die Spalte 'Zusätzliche Sicherungen aufbewahren' abhängig von Ihren Geschäftsanforderungen auf 30 Tage oder mehr.
4. Sichern Sie Ihre Änderungen und klicken Sie erneut auf die Umschaltfläche Konfigurieren, damit die Maßnahmengruppe nicht mehr editierbar ist.
5. Aktivieren Sie die Maßnahmengruppe, indem Sie auf Aktivieren klicken.

## Zeitpläne für Serververwaltungsaktivitäten definieren

---

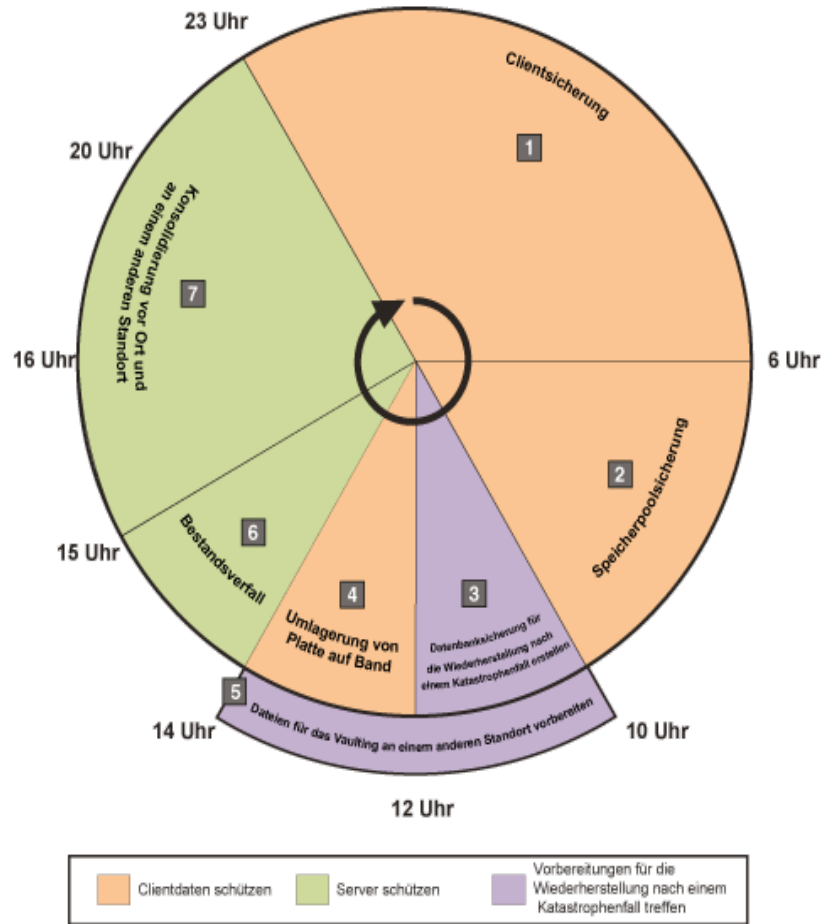
Erstellen Sie Zeitpläne für jede Serververwaltungsoperation, indem Sie den Befehl DEFINE SCHEDULE im Command Builder des Operations Center verwenden.

## Informationen zu diesem Vorgang

---

Planen Sie die Ausführung von Serververwaltungsoperationen im Anschluss an Clientsicherungsoperationen. Sie können das Timing von Zeitplänen steuern, indem Sie die Startzeit in Kombination mit der Dauer für jede Operation definieren.

Die folgende Abbildung zeigt ein Beispiel für die Planung von Verwaltungsoperationen.  
Abbildung 1. Tagesplan der Serveroperationen für eine Bandspeicherlösung



Die folgende Tabelle zeigt die Planung von Serververwaltungsprozessen in Kombination mit dem Clientsicherungszeitplan für eine Bandspeicherlösung.

| Operation  | Zeitplan  |
|--|---|
| Clientsicherung  | Startet um 23 Uhr.  |
| Speicherpoolsicherung  | Startet um 6 Uhr.   |
| Verarbeitung für die Datenbank und die Dateien zur Wiederherstellung nach einem Katastrophenfall | <ul style="list-style-type: none"> <li>Die Datenbanksicherungsoperation startet um 10 Uhr bzw. 11 Stunden nach dem Start der Clientsicherungsoperation. Dieser Prozess wird bis zum Abschluss ausgeführt.</li> <li>Die Sicherungsoperationen für Einheitenkonfigurationsinformationen und das Datenträgerprotokoll starten um 17 Uhr bzw. 7 Stunden nach dem Start der Datenbanksicherungsoperation.</li> <li>Das Löschen des Datenträgerprotokolls startet um 20 Uhr bzw. 10 Stunden nach dem Start der Datenbanksicherungsoperation.</li> </ul> |
| Vorbereitung der Dateien für das Vaulting an einem anderen Standort                              | Startet um 10 Uhr zu demselben Zeitpunkt wie die Verarbeitung für die Datenbank und die Dateien zur Wiederherstellung nach einem Katastrophenfall.  |
| Umlagerung von Platte auf Band   | Startet um 12 Uhr bzw. 2 Stunden nach dem Start der Datenbanksicherungsoperation.   |
| Bestandsverfall  | Startet um 14 Uhr bzw. 15 Stunden nach dem Start der Clientsicherungsoperation. Dieser Prozess wird bis zum Abschluss ausgeführt.   |
| Speicherbereichskonsolidierung   | Startet um 15 Uhr bzw. 16 Stunden nach dem Start der Clientsicherungsoperation.   |

## Vorgehensweise



Erstellen Sie nach dem Konfigurieren der Einheitenklasse für die Datenbanksicherungsoperationen Zeitpläne für Datenbanksicherungsoperationen und andere erforderliche Verwaltungsoperationen mithilfe des Befehls DEFINE SCHEDULE. Abhängig von der Größe Ihrer Umgebung müssen Sie die Startzeiten für jeden Zeitplan in dem Beispiel gegebenenfalls anpassen.

1. Definieren Sie eine Einheitenklasse für die Sicherungsoperation, bevor Sie den Zeitplan für Datenbanksicherungen erstellen. Erstellen Sie mit dem Befehl DEFINE DEVCLASS eine Einheitenklasse mit dem Namen LTOTAPE:

```
define devclass ltotape devtype=lto library=ltolib
```

2. Legen Sie die Einheitenklasse für automatische Datenbanksicherungen fest. Geben Sie mit dem Befehl SET DBRECOVERY die im vorhergehenden Schritt für die Datenbanksicherung erstellte Einheitenklasse an. Wenn beispielsweise die Einheitenklasse den Namen LTOTAPE hat, geben Sie den folgenden Befehl aus:

```
set dbrecovery ltotape
```

3. Erstellen Sie mithilfe des Befehls DEFINE SCHEDULE Zeitpläne für die Verwaltungsoperationen. Die folgende Tabelle enthält die erforderlichen Operationen und Beispiele der Befehle.

| Operation                 | Beispielbefehle und weitere Informationen  |
|---------------------------|--|
| Sichern von Speicherpools | <p>Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP STGPOOL.<br/>Geben Sie beispielsweise den folgenden Befehl aus, um einen Sicherungszeitplan für einen primären Speicherpool mit dem Namen PRIMARY_POOL zu erstellen. Der Pool wird in einem Kopierspeicherpool mit dem Namen COPYSTG gesichert:</p> <pre>define schedule BACKUPSTGPOOL type=administrative cmd="backup stgpool primary_pool copystg" active=yes starttime=06:00 period=1</pre> |
| Sichern der Datenbank     | <p>Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP DB.<br/>Geben Sie beispielsweise den folgenden Befehl aus, um einen Sicherungszeitplan zu erstellen, der die neue Einheitenklasse verwendet:</p> <pre>define schedule DBBACKUP type=admin cmd="backup db devclass=ltotape type=full numstreams=3 wait=yes compress=yes" active=yes desc="Datenbank sichern." startdate=today starttime=10:00:00 duration=45 durunits=minutes</pre>             |
| Replizieren von Knoten    | <p>Verwenden Sie wahlweise die Knotenreplikation, um Clientdaten zu schützen, indem Sie die Daten auf einem sekundären Server sichern. Anweisungen finden Sie in Clientdaten auf einen anderen Server replizieren. Stellen Sie sicher, dass die Knotenreplikation abgeschlossen ist, bevor Umlagerungsoperationen beginnen.</p>  |

| Operation  | Beispielbefehle und weitere Informationen   |
|--|---|
| Tägliches Umlagern von Daten von Platte auf Band                   | <p>Erstellen Sie einen Zeitplan für die Speicherpoolumlagerung. Wenn beispielsweise ein Plattenspeicherpool mit dem Namen DISKPOOL vorhanden ist und der nächste Speicherpool der Speicherpool mit dem Namen TAPEPOOL ist, können Sie die Speicherpoolumlagerung planen, indem Sie den folgenden Befehl ausgeben:</p> <pre>define schedule stgpool_migration type=administrative cmd="migrate stgpool diskpool lomig=0" active=yes description="Plattenspeicherpool in Bandpool umlagern" startdate=today starttime=12:00 duration=2 durunits=hours period=1 perunits=days</pre> <p>Um den Durchsatz zu maximieren, können Sie die Anzahl paralleler Prozesse angeben, die für die Umlagerung von Dateien verwendet werden soll, indem Sie die folgenden Schritte ausführen:</p> <ol style="list-style-type: none"> <li>Stellen Sie für den Bandspeicherpool sicher, dass die Kollokation aktiviert ist. Um zu überprüfen, ob die Kollokation aktiviert ist, führen Sie den Befehl QUERY STGPOOL aus. Stellen Sie sicher, dass der Wert GROUP, NODE oder FILESPACE im Feld COLLOCATE angegeben ist. Wenn der Wert GROUP, NODE oder FILESPACE nicht angegeben ist, verwenden Sie den Befehl UPDATE STGPOOL, um abhängig von Ihrer Systemkonfiguration COLLOCATE=GROUP, COLLOCATE=NODE oder COLLOCATE=FILESPACE anzugeben.</li> <li>Geben Sie für den Plattenspeicherpool mithilfe des Befehls DEFINE STGPOOL oder UPDATE STGPOOL einen Wert für den Parameter MIGPROCESS an. Wenn beispielsweise 12 Bandlaufwerke vorhanden sind, geben Sie MIGPROCESS=10 an. Auf diese Weise werden maximal 10 Bandlaufwerke für Umlagerungsprozesse verwendet. Zwei Laufwerke sind für andere Tasks, wie beispielsweise Zurückschreibungs-, Datenbanksicherungs- und Clientsicherungsoperationen, reserviert.</li> </ol> |
| Vorbereiten von Dateien für das Vaulting an einem anderen Standort | <ol style="list-style-type: none"> <li>Versetzen Sie Banddatenträger an einen anderen Standort, indem Sie die Anweisungen in Sicherungsdатenträger versetzen ausführen.</li> <li>Erstellen Sie die Plandatei zur Wiederherstellung nach einem Katastrophenfall, indem Sie den Befehl PREPARE auf dem Quellenserver ausgeben: <pre>prepare</pre> </li> <li>Stellen Sie sicher, dass alle Datenträger, die für die Wiederherstellung nach einem Katastrophenfall erforderlich sind, in die Wiederherstellungsplandatei eingeschlossen sind. Weitere Informationen finden Sie in Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM.</li> </ol>  |
| Sichern der Einheitenkonfigurationsinformationen                   | <p>Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP DEVCONFIG:</p> <pre>define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Einheitenkonfigurationsdatei sichern." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>   |
| Sichern des Datenträgerprotokolls                                  | <p>Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP VOLHISTORY:</p> <pre>define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Datenträgerprotokoll sichern." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>   |

| Operation  | Beispielbefehle und weitere Informationen   |
|--|---|
| Entfernen älterer Versionen von Datenbanksicherungen, die nicht mehr erforderlich sind | <p>Erstellen Sie einen Zeitplan für die Ausführung des Befehls DELETE VOLHISTORY:</p> <pre>define schedule DELVOLHIST type=admin cmd="delete volhistory   type=dbb todate=today-6 totime=now" active=yes desc="Alte Datenbanksicherungen entfernen." startdate=today starttime=20:00:00 duration=45 durunits=minutes</pre>  |
| Entfernen von Objekten, deren zulässige Aufbewahrungsdauer überschritten wurde         | <p>Erstellen Sie einen Zeitplan für die Ausführung des Befehls EXPIRE INVENTORY.</p> <p>Legen Sie für den Parameter RESOURCE auf der Basis der Systemgröße, die Sie konfigurieren, einen Wert fest, der mit der Anzahl Prozesskerne, die für Ihr System angegeben wurden, übereinstimmt.</p> <p>Geben Sie beispielsweise den folgenden Befehl aus, um einen Zeitplan mit dem Namen EXPINVENTORY zu erstellen:</p> <pre>define schedule EXPINVENTORY type=admin cmd="expire inventory   wait=yes resource=8 duration=120" active=yes desc="Verfallene Objekte entfernen." startdate=today starttime=14:00:00 duration=1 durunits=hours</pre>   |
| Konsolidieren von Speicherbereich  | <p>Erstellen Sie einen Zeitplan für die Ausführung des Befehls RECLAIM STGPOOL.</p> <p>Geben Sie beispielsweise den folgenden Befehl aus, um einen Zeitplan mit dem Namen RECLAIM zu erstellen:</p> <pre>define schedule RECLAIM type=admin cmd="reclaim stgpool   tapepool duration=60" startdate=today starttime=15:00:00 duration=5 durunits=hours</pre> <p>Tipp: Um den Durchsatz zu maximieren, können Sie die Anzahl paralleler Prozesse angeben, die für die Konsolidierung von Speicherbereich verwendet werden soll. Aktualisieren Sie den Bandspeicherpool mithilfe des Befehls UPDATE STGPOOL und geben Sie einen Wert für den Parameter RECLAIMPROCESS an. Wenn beispielsweise 12 Bandlaufwerke vorhanden sind, geben Sie RECLAIMPROCESS=5 an. Da für jeden Konsolidierungsprozess zwei Laufwerke verwendet werden, beträgt die Gesamtzahl Laufwerke, die für die Konsolidierung verwendet werden kann, 10. Zwei Laufwerke sind für Sicherungsoperationen reserviert.</p> |

## Nächste Schritte

Nachdem Sie Zeitpläne für die Serververwaltungstasks erstellt haben, können Sie diese im Operations Center anzeigen, indem Sie die folgenden Schritte ausführen:

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Server.
  2. Klicken Sie auf Verwaltung.
- Sicherungsdatenträger versetzen  
Für die Wiederherstellung nach einem Katastrophenfall benötigen Sie Datenbanksicherungsdatenträger, Kopierspeicherpooldatenträger und weitere Dateien. Um auf einen Katastrophenfall vorbereitet zu sein, müssen Sie tägliche Tasks ausführen.

### Zugehörige Verweise:

- [UPDATE STGPOOL \(Speicherpool aktualisieren\)](#)
- [DEFINE SCHEDULE \(Zeitplan für einen Verwaltungsbefehl definieren\)](#)

### Zugehörige Informationen:

- [DEFINE STGPOOL \(Datenträger in einem Speicherpool definieren\)](#)

## Clientzeitpläne definieren

---

Erstellen Sie mithilfe des Operations Center Zeitpläne für Clientoperationen.

### Vorgehensweise

---

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Clients.
2. Klicken Sie auf Zeitpläne.
3. Klicken Sie auf +Zeitplan.
4. Führen Sie die Schritte im Assistenten Zeitplan erstellen aus. Definieren Sie auf der Basis der in Zeitpläne für Serververwaltungsaktivitäten geplanten Serververwaltungsaktivitäten für Clientsicherungszeitpläne eine Startzeit von 22:00 Uhr.

## Bandeinheiten für den Server anschließen

---



Bevor der Server eine Bandeinheit verwenden kann, müssen Sie die Einheit an Ihr Serversystem anschließen und den entsprechenden Bandeinheitentreiber installieren.

### Informationen zu diesem Vorgang

---

Um die Systemleistung zu optimieren, verwenden Sie schnelle Bandeinheiten mit hoher Speicherkapazität. Stellen Sie genügend Bandlaufwerke bereit, um Ihre Geschäftsanforderungen erfüllen zu können.

Schließen Sie Bandeinheiten an ihren eigenen Hostbusadapter (HBA) an, der nicht mit anderen Einheitentypen, wie beispielsweise Platte, gemeinsam genutzt wird. IBM® Bandlaufwerke haben einige spezielle Anforderungen in Bezug auf HBAs und zugehörige Treiber.

-  Linux-BetriebssystemeAutomatisierte Speicherarchiveinheit an das System anschließen  
Sie können eine automatisierte Speicherarchiveinheit an Ihr System anschließen, um Ihre Daten auf Bändern zu speichern.
- Bandeinheitentreiber auswählen  
Um Bandeinheiten mit IBM Spectrum Protect verwenden zu können, müssen Sie den entsprechenden Bandeinheitentreiber installieren.
-  Linux-BetriebssystemeGerätedateinamen für Bandeinheiten  
Ein Gerätedateiname für eine Bandeinheit ist für den IBM Spectrum Protect-Server für die Arbeit mit Bandeinheiten, Datenträgerwechslern oder Einheiten für austauschbare Datenträger erforderlich.
- Bandeinheitentreiber installieren und konfigurieren  
Sie können Bandeinheiten erst mit IBM Spectrum Protect verwenden, nachdem der korrekte Bandeinheitentreiber installiert wurde.

## Automatisierte Speicherarchiveinheit an das System anschließen

---

Sie können eine automatisierte Speicherarchiveinheit an Ihr System anschließen, um Ihre Daten auf Bändern zu speichern.

### Informationen zu diesem Vorgang

---

Berücksichtigen Sie die folgenden Einschränkungen, bevor Sie eine automatisierte Speicherarchiveinheit anschließen:



- Angeschlossene Einheiten müssen sich an ihrem eigenen Hostbusadapter (HBA) befinden.
- Ein HBA darf nicht mit anderen Einheitentypen, wie beispielsweise einer Platte, gemeinsam genutzt werden. .
- Bei Mehrfach-FC-HBAs müssen sich angeschlossene Einheiten an ihren eigenen Ports befinden. Diese Ports dürfen nicht mit anderen Einheitentypen gemeinsam genutzt werden.
- IBM® Bandlaufwerke haben einige spezielle Anforderungen in Bezug auf HBA und zugehörige Treiber. Weitere Informationen zu Einheiten finden Sie auf der Website für Ihr Betriebssystem:
  - Website mit den von IBM Spectrum Protect unterstützten Einheiten für AIX
  - Website mit den von IBM Spectrum Protect unterstützten Einheiten für Linux und Windows

### Vorgehensweise

---

Um den Fibre Channel-Adapter (FC-Adapter) verwenden zu können, führen Sie die folgenden Schritte aus:

1. Installieren Sie den FC-Adapter und die zugehörigen Treiber.
2. Installieren Sie die geeigneten Einheitentreiber für die angeschlossenen Datenträgerwechsler.

-   Speicherarchivmodus festlegen  
Damit der IBM Spectrum Protect-Server auf ein SCSI-Speicherarchiv zugreifen kann, muss die Bandeinheit für den entsprechenden Modus definiert werden.

**Zugehörige Konzepte:**

Bandeinheitentreiber auswählen

## Bandeinheitentreiber auswählen

---

Um Bandeinheiten mit IBM Spectrum Protect verwenden zu können, müssen Sie den entsprechenden Bandeinheitentreiber installieren.

- IBM Bandeinheitentreiber  
IBM® Einheitentreiber sind für die meisten IBM Bandeinheiten mit Kennsätzen verfügbar.
- IBM Spectrum Protect-Bandeinheitentreiber  
Bandeinheitentreiber werden vom IBM Spectrum Protect-Server bereitgestellt.

**Zugehörige Verweise:**

Bandeinheitentreiber installieren und konfigurieren

## IBM Bandeinheitentreiber

---

IBM® Einheitentreiber sind für die meisten IBM Bandeinheiten mit Kennsätzen verfügbar.

Sie können IBM Bandeinheitentreiber von der Website für Fix Central herunterladen:

1. Rufen Sie die Website für Fix Central unter Website für Fix Central auf.
2. Klicken Sie auf Produkt auswählen.
3. Wählen Sie System Storage im Menü für die Produktgruppe aus.
4. Wählen Sie Tape systems im Menü für System Storage aus.
5. Wählen Sie Tape drivers and software im Menü für Tape systems aus.
6. Wählen Sie Tape device drivers im Menü für Tape drivers and software aus. Zusätzlich zu Bandtreibern erhalten Sie auch Zugriff auf Tools wie das IBM Tape Diagnostic Tool (ITDT).
7. Wählen Sie Ihr Betriebssystem im Menü Plattform aus.

Die aktuelle Liste der Einheiten und Betriebssystemversionen, die von IBM Bandeinheitentriibern unterstützt werden, finden Sie auf der Website mit den von IBM Spectrum Protect unterstützten Einheiten unter Supported devices for AIX and Windows.



Die aktuelle Liste der Bandeinheiten und Betriebssystemversionen, die von IBM Bandeinheitentriibern unterstützt werden, finden Sie auf der Website mit den von IBM Spectrum Protect unterstützten Einheiten unter Supported devices for Linux.

IBM Bandeinheitentreiber unterstützen nur einige Linux-Kernel-Level. Informationen zu unterstützten Kernel-Leveln finden Sie in Website für Fix Central.

## IBM Spectrum Protect-Bandeinheitentreiber

---

Bandeinheitentreiber werden vom IBM Spectrum Protect-Server bereitgestellt.

Ein IBM Spectrum Protect-Bandeinheitentreiber wird mit dem Server installiert.



Sie können den generischen SCSI-Bandeinheitentreiber, der vom IBM® AIX-Betriebssystem bereitgestellt wird, verwenden, um mit Bandeinheiten zu arbeiten, die nicht vom IBM Spectrum Protect-Einheitentreiber unterstützt werden. Wenn der generische SCSI-Bandeinheitentreiber unter AIX verwendet wird, muss die Einheitenklasse GENERICTAPE auf den Einheitentyp gesetzt werden, der im Befehl DEFINE DEVCLASS angegeben ist.

Bei den folgenden Bandeinheiten können Sie auswählen, ob der IBM Spectrum Protect-Bandeinheitentreiber oder der native Einheitentreiber für Ihr Betriebssystem installiert werden soll:

- ECART
- LTO (nicht von IBM)

Alle über SCSI angeschlossenen Speicherarchive, die Bandlaufwerke aus der Liste enthalten, müssen den IBM Spectrum Protect-Wechslertrieberr verwenden.

Bandeinheitentreiber anderer Hardwareanbieter können verwendet werden, wenn sie der Einheitenklasse GENERICTAPE zugeordnet sind. Generische Einheitentreiber werden in Einheitenklassen WORM (Write Once Read Many) nicht unterstützt.

#### Linux-Betriebssysteme


Sie können den IBM Spectrum Protect-Durchgriffseinheitentreiber verwenden. IBM Spectrum Protect-Durchgriffseinheitentreiber erfordern den generischen Linux-SCSI-Einheitentreiber (sg) zusammen mit dem Linux-Betriebssystem für die Installation der Kernel.

Sie können beispielsweise den IBM Spectrum Protect-Durchgriffseinheitentreiber für die folgenden Bandeinheiten installieren:

- ECART
- LTO (nicht von IBM)

Alle über SCSI angeschlossenen Speicherarchive, die Bandlaufwerke enthalten, die in der Liste nicht mit IBM gekennzeichnet sind, müssen ebenfalls den IBM Spectrum Protect-Durchgriffseinheitentreiber verwenden.

Sie können den generischen SCSI-Bandeinheitentreiber (st), der vom Linux-Betriebssystem bereitgestellt wird, nicht verwenden. Demzufolge wird der Einheitentyp GENERICTAPE für den Befehl DEFINE DEVCLASS nicht unterstützt.

 Windows-Betriebssysteme Sie können einen durch Windows Hardware Quality Labs (WHQL) zertifizierten nativen Treiber anstelle des IBM Spectrum Protect-Einheitentreibers auswählen. Der durch die Windows Hardware Qualification Labs (WHQL) zertifizierte native Einheitentreiber kann nur für Einheiten verwendet werden, die keinen IBM Kennsatz haben, sowie für Bandlaufwerke eines anderen Herstellers als IBM. Für den durch die Windows Hardware Qualification Labs zertifizierten nativen Einheitentreiber können Sie entweder den IBM Spectrum Protect-SCSI-Durchgriffseinheitentreiber oder den nativen Windows-Bandeinheitentreiber auswählen. Wenn der SCSI-Durchgriffseinheitentreiber verwendet wird, darf die Einheitenklasse im Befehl DEFINE DEVCLASS nicht GENERICTAPE lauten. Wenn der native Einheitentreiber verwendet wird, muss die Einheitenklasse GENERICTAPE lauten.

## Gerätedateinamen für Bandeinheiten

Ein Gerätedateiname für eine Bandeinheit ist für den IBM Spectrum Protect-Server für die Arbeit mit Bandeinheiten, Datenträgerwechslern oder Einheiten für austauschbare Datenträger erforderlich.

#### AIX-Betriebssysteme

Wenn eine Einheit erfolgreich konfiguriert wird, wird der Name einer logischen Datei zurückgegeben. In Tabelle 1 ist der Name der Einheit, der auch als Gerätedateiname bezeichnet wird, aufgeführt, der dem Laufwerk oder Speicherarchiv entspricht. Sie können den Betriebssystembefehl SMIT verwenden, um den Gerätedateinamen für die Einheit abzurufen. In den Beispielen gibt x eine ganze Zahl größer-gleich 0 an.

Tabelle 1. Beispiele für Einheiten

| Einheit  | Beispiel für Einheit | Name der logischen Datei |
|--|----------------------|--------------------------|
| Bandlaufwerke, die vom IBM Spectrum Protect-Einheitentreiber verwendet werden können           | /dev/mtx             | mtx                      |
| Bandlaufwerke, die vom IBM Bandeinheitentreiber verwendet werden können                        | /dev/rmtx            | rmtx                     |
| Bandlaufwerke, die vom generischen IBM AIX-Bandeinheitentreiber verwendet werden können        | /dev/rmtx            | rmtx                     |
| Speicherarchiveinheiten, die vom IBM Spectrum Protect-Einheitentreiber verwendet werden können | /dev/lbx             | lbx                      |
| Speicherarchiveinheiten, die vom IBM Bandeinheitentreiber verwendet werden können              | /dev/smcx            | smcx                     |

#### Linux-Betriebssysteme

Wenn eine Einheit erfolgreich konfiguriert wird, wird der Name einer logischen Datei zurückgegeben. In Tabelle 2 ist der Name der Einheit, der auch als Gerätedateiname bezeichnet wird, aufgeführt, der dem Laufwerk oder Speicherarchiv entspricht. In den Beispielen gibt x eine ganze Zahl größer-gleich 0 an.

Tabelle 2. Beispiele für Einheiten

| Einheit   | Beispiel für Einheit | Name der logischen Datei |
|---|----------------------|--------------------------|
| Bandlaufwerke, die vom IBM Spectrum Protect-Durchgriffseinheitentreiber verwendet werden können | /dev/tmscsi/mtx      | mtx                      |
| Bandlaufwerke, die vom IBM lin_tape-Einheitentreiber verwendet werden können                    | /dev/IBMtapex        | IBMtapex                 |

| Einheit  | Beispiel für Einheit | Name der logischen Datei |
|--|----------------------|--------------------------|
| Speicherarchivseinheiten, die vom IBM Spectrum Protect-Durchgriffseinheitentreiber verwendet werden können | /dev/sgscsi/lbx      | lbx                      |
| Speicherarchivseinheiten, die vom IBM lin_tape-Einheitentreiber verwendet werden können                    | /dev/IBMchangerx     | IBMchangerx              |

#### Windows-Betriebssysteme

Wenn eine Einheit erfolgreich konfiguriert wird, wird der Name einer logischen Datei zurückgegeben. In Tabelle 3 ist der Name der Einheit, der auch als Gerätedateiname bezeichnet wird, aufgeführt, der dem Laufwerk oder Speicherarchiv entspricht. In den Beispielen geben *a*, *b*, *c*, *d* und *x* jeweils eine ganze Zahl größer-gleich 0 an; dabei gilt Folgendes:

- *a* gibt die Ziel-ID an.
- *b* gibt die Nummer der logischen Einheit (LUN) an.
- *c* gibt die SCSI-Bus-ID an.
- *d* gibt die Port-ID an.




Tabelle 3. Beispiele für Einheiten

| Einheit   | Beispiel für Einheit | Konvertierter Einheitenname |
|---|----------------------|-----------------------------|
| Bandlaufwerke, die vom IBM Spectrum Protect-Einheitentreiber unterstützt werden                       | <i>mta.b.c.d</i>     | <i>mta.b.c.d</i>            |
| Bandlaufwerke, die vom IBM Spectrum Protect-Durchgriffseinheitentreiber unterstützt werden            | <i>mta.b.c.d</i>     | <i>mta.b.c.d</i>            |
| Bandlaufwerke, die vom IBM Einheitentreiber unterstützt werden  | Tapex                | <i>mta.b.c.d</i>            |
| Speicherarchivseinheiten, die vom IBM Spectrum Protect-Einheitentreiber unterstützt werden            | <i>lba.b.c.d</i>     | <i>lba.b.c.d</i>            |
| Speicherarchivseinheiten, die vom IBM Spectrum Protect-Durchgriffseinheitentreiber unterstützt werden | <i>lba.b.c.d</i>     | <i>lba.b.c.d</i>            |
| Speicherarchivseinheiten, die vom IBM Einheitentreiber unterstützt werden                             | Changerx             | <i>lba.b.c.d</i>            |

## Bandeneinheitentreiber installieren und konfigurieren

Sie können Bandeneinheiten erst mit IBM Spectrum Protect verwenden, nachdem der korrekte Bandeneinheitentreiber installiert wurde.

IBM Spectrum Protect unterstützt alle Einheiten, die von IBM® Bandeneinheitentreibern unterstützt werden. IBM Spectrum Protect unterstützt jedoch nicht alle Betriebssystemversionen, die von IBM Bandeneinheitentreiber unterstützt werden.


- IBM Einheitentreiber für IBM Bandeneinheiten installieren und konfigurieren  
Installieren und Konfigurieren Sie einen IBM Bandeneinheitentreiber, um eine IBM Bandeneinheit verwenden zu können.
-  AIX-Betriebssysteme Bandeneinheitentreiber auf AIX-Systemen konfigurieren  
Lesen Sie die Anweisungen zum Installieren und Konfigurieren von Bandeneinheitentreibern anderer Hersteller als IBM auf AIX-Systemen.
-  Linux-Betriebssysteme Bandeneinheitentreiber auf Linux-Systemen konfigurieren  
Lesen Sie die folgenden Abschnitte, wenn Sie Bandeneinheitentreiber auf Linux-Systemen installieren und konfigurieren.
-  Windows-Betriebssysteme Bandeneinheitentreiber auf Windows-Systemen konfigurieren  
Lesen Sie die Anweisungen zum Installieren und Konfigurieren von Treibern für Bandeneinheiten und Speicherarchive auf Windows-Systemen.

## IBM Einheitentreiber für IBM Bandeneinheiten installieren und konfigurieren

Installieren und Konfigurieren Sie einen IBM® Bandeneinheitentreiber, um eine IBM Bandeneinheit verwenden zu können.

### Informationen zu diesem Vorgang

Anweisungen zum Installieren und Konfigurieren von IBM Bandeneinheitentreibern finden Sie in der Veröffentlichung *IBM Tape Device Drivers Installation and User's Guide*.

 AIX-Betriebssysteme Nachdem Sie die Installationsprozedur wie im Handbuch *IBM Tape Device Drivers Installation and User's Guide* beschrieben ausgeführt haben, werden, abhängig von dem Einheitentreiber, der installiert wird, unterschiedliche Nachrichten

ausgegeben. Wenn Sie den Einheitentreiber für ein IBM Bandlaufwerk oder Speicherarchiv installieren, werden die folgenden Nachrichten zurückgegeben:

```
rmtx Verfügbar
```

oder

```
smcx Verfügbar
```


Notieren Sie den Wert von x, der vom IBM Bandedeinheitentreiber zugeordnet wird. Um den Gerätedateinamen Ihrer Einheit zu bestimmen, geben Sie einen der folgenden Befehle aus:

- Für Bandlaufwerke: `ls -l /dev/rmt*`
- Für Bandarchive: `ls -l /dev/smc*`

Der Dateiname kann weitere Zeichen am Ende haben, um verschiedene Betriebsmerkmale anzugeben, die aber von IBM Spectrum Protect nicht benötigt werden. Verwenden Sie für IBM Einheitentreiber den Basisdateinamen im Parameter DEVICE des Befehls DEFINE PATH, um eine Einheit einem Laufwerk (/dev/rmtx) oder einem Speicherarchiv (/dev/smcx) zuzuordnen.

Nachdem Sie den Einheitentreiber installiert haben, können Sie mithilfe von SMIT (System Management Interface Tool) Bandlaufwerke und Bandarchive anderer Hersteller als IBM konfigurieren. Führen Sie die folgenden Schritte aus:

1. Führen Sie das Programm SMIT aus.
2. Klicken Sie auf Devices.
3. Klicken Sie auf IBM Spectrum Protect Devices.
4. Klicken Sie auf Fibre Channel SAN Attached devices.
5. Klicken Sie auf Discover Devices Supported by IBM Spectrum Protect. Warten Sie, bis der Erkennungsprozess abgeschlossen ist.
6. Kehren Sie zum Menü Fibre Channel SAN Attached devices zurück und klicken Sie auf List Attributes of a Discovered Device.

 Nachdem Sie die Installationsprozedur wie im Handbuch *IBM Tape Device Drivers Installation and User's Guide* beschrieben ausgeführt haben, werden, abhängig von dem Einheitentreiber, der installiert wird, unterschiedliche Nachrichten ausgegeben. Wenn Sie den Einheitentreiber für eine IBM LTO- oder 3592-Einheit installieren, werden die folgenden Nachrichten zurückgegeben:

```
IBMtapex Verfügbar
```

oder


```
IBMChangerx Verfügbar
```

Notieren Sie den Wert von x, der vom IBM Bandedeinheitentreiber zugeordnet wird. Um den Gerätedateinamen Ihrer Einheit zu bestimmen, geben Sie einen der folgenden Befehle aus:

- Für Bandlaufwerke: `ls -l /dev/IBMtape*`
- Für Bandarchive: `ls -l /dev/IBMChange*`

Der Dateiname kann weitere Zeichen am Ende haben, um verschiedene Betriebsmerkmale anzugeben, die aber von IBM Spectrum Protect nicht benötigt werden. Verwenden Sie für IBM Einheitentreiber den Basisdateinamen im Parameter DEVICE des Befehls DEFINE PATH, um eine Einheit einem Laufwerk (/dev/IBMtapex) oder einem Speicherarchiv (/dev/IBMChangerx) zuzuordnen.

Einschränkung: Der Einheitentyp dieser Klasse darf nicht GENERICTAPE lauten.

 Für Windows-Betriebssysteme stellt IBM Spectrum Protect zwei Einheitentreiber zur Verfügung:

**Durchgriffseinheitentreiber**

Wenn der Hersteller der Bandedeinheit einen SCSI-Einheitentreiber bereitstellt, installieren Sie den IBM Spectrum Protect-Durchgriffseinheitentreiber.

**SCSI-Einheitentreiber für Bandedeinheiten**


Wenn der Hersteller der Bandedeinheit keinen SCSI-Einheitentreiber bereitstellt, installieren Sie den IBM Spectrum Protect-SCSI-Einheitentreiber für Bandedeinheiten. Der Name der Treiberdatei ist tsm SCSI64.sys.

Anweisungen zum Installieren und Konfigurieren von IBM Bandedeinheitentribern finden Sie in der Veröffentlichung *IBM Tape Device Drivers Installation and User's Guide*. Nach der Installation des IBM Bandedeinheitentreibers gibt der Server einen Gerätedateinamen TapeX für IBM Bandlaufwerke und ChangerY für IBM Datenträgerwechsler an. Für einen IBM Spectrum Protect-SCSI-Einheitentreiber oder einen IBM Spectrum Protect-Durchgriffseinheitentreiber können Sie den Windows-Betriebssystembefehl regedit ausgeben, um den Namen der Treiberdatei für die Einheit zu überprüfen. Der IBM Spectrum Protect-Server stellt auch ein Dienstprogramm zur Überprüfung der Einheit für das Windows-Betriebssystem zur Verfügung. Das Dienstprogramm tsm d1st ist im Serverpaket enthalten. Um das Dienstprogramm zu verwenden, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass die Anwendungsprogrammierschnittstelle (API) des Hostbusadapters installiert ist.
2. Um Einheitsdaten aus dem Hostsystem abzurufen, geben Sie Folgendes ein:


```
tsmd1st
```



-  Linux-Betriebssysteme Multipath I/O-Zugriff mit IBM Bandeinheiten  
Multipath I/O ist ein Verfahren, das unterschiedliche Pfade für den Zugriff auf dieselbe physische Einheit verwendet, beispielsweise über mehrere Hostbusadapter (HBA) oder Switches. Mithilfe des Multipathverfahrens kann sichergestellt werden, dass kein Single Point of Failure auftritt.

**Zugehörige Konzepte:**

Multipath I/O-Zugriff mit IBM Bandeinheiten

 AIX-Betriebssysteme

## Bandeneinheitentreiber auf AIX-Systemen konfigurieren





---

Lesen Sie die Anweisungen zum Installieren und Konfigurieren von Bandeneinheitentriibern anderer Hersteller als IBM® auf AIX-Systemen.

### Informationen zu diesem Vorgang

---

Anweisungen zum Installieren und Konfigurieren von IBM Bandeneinheitentriibern finden Sie in der Veröffentlichung *IBM Tape Device Drivers Installation and User's Guide*.

-  AIX-Betriebssysteme SCSI- und Fibre Channel-Einheiten  
Die Menüs und Eingabeaufforderungen zur Definition von IBM Spectrum Protect-Einheiten in SMIT ermöglichen die Verwaltung von Einheiten, die über SCSI und Fibre Channel (FC) angeschlossen sind.
-  AIX-Betriebssysteme IBM Spectrum Protect-Einheitentreiber für Datenträgerwechsler konfigurieren  
Verwenden Sie die folgende Prozedur, um IBM Spectrum Protect-Einheitentreiber für Datenträgerwechsler für Speicherarchive anderer Hersteller zu konfigurieren.
-  AIX-Betriebssysteme IBM Spectrum Protect-Einheitentreiber für Bandlaufwerke konfigurieren  
Verwenden Sie die folgende Prozedur, um IBM Spectrum Protect-Einheitentreiber für Bandlaufwerke für Speicherarchive anderer Hersteller zu konfigurieren.
-  AIX-Betriebssysteme An ein Fibre Channel-SAN angeschlossene Einheiten konfigurieren  
Um eine an ein Fibre Channel-SAN angeschlossene Einheit zu konfigurieren, führen Sie die Prozedur aus.

 AIX-Betriebssysteme

## SCSI- und Fibre Channel-Einheiten

---

Die Menüs und Eingabeaufforderungen zur Definition von IBM Spectrum Protect-Einheiten in SMIT ermöglichen die Verwaltung von Einheiten, die über SCSI und Fibre Channel (FC) angeschlossen sind.

Das Hauptmenü von IBM Spectrum Protect verfügt über zwei Optionen:

Über SCSI angeschlossene Einheiten

Verwenden Sie diese Option, um SCSI-Einheiten zu konfigurieren, die mit einem SCSI-Adapter im Host verbunden sind.

Über Fibre Channel-SAN-angeschlossene Einheiten

Verwenden Sie diese Option, um Einheiten zu konfigurieren, die mit einem Fibre Channel-Adapter (FC-Adapter) im Host verbunden sind. Wählen Sie eines der folgenden Attribute aus:

Attribute einer erkannten Einheit auflisten

Listet Attribute einer Einheit auf, die der aktuellen ODM-Datenbank bekannt ist.

- FC Port ID:  
24-Bit FC Port ID(N(L)\_Port oder F(L)\_Port). Dies ist die Adress-ID, die innerhalb der zugeordneten Topologie, in der die Einheit verbunden ist, eindeutig ist. In den Switch- oder Fabric-Umgebungen kann sie durch den Switch anhand der oberen 2 Byte, die nicht null sind, bestimmt werden. In einer Private Arbitrated Loop ist dies die Arbitrated Loop Physical Address (AL\_PA), wobei die oberen 2 Byte null sind. Wenden Sie sich an Ihren Fibre Channel-Hersteller, um zu bestimmen, wie eine AL\_PA oder eine Port-ID zugeordnet wird.
- Mapped LUN ID:  
Ein FC-zu-SCSI-Brückenmodul (auch als Umsetzer, Router oder Gateway bezeichnet). Informationen zur Zuordnung von LUNs erhalten Sie von Ihrem Brückenhersteller. Zugeordnete LUN-IDs sollten nicht geändert werden.
- WW Name:  
Der weltweite Name (WWN) des Ports, an den die Einheit angeschlossen ist. Dies ist die eindeutige 64-Bit-Kennung, die von Herstellern von Fibre Channel-Komponenten wie Brücken oder nativen Fibre Channel-Einheiten zugeordnet

wird. Wenden Sie sich an Ihren Fibre Channel-Hersteller, um den WWN eines Ports zu bestimmen.

- Product ID:

Die Produkt-ID einer Einheit. Wenden Sie sich an Ihren Einheitenhersteller, um die Produkt-ID zu bestimmen.

#### Von IBM Spectrum Protect unterstützte Einheiten erkennen

Mit dieser Option werden Einheiten in einem Fibre Channel-SAN, die von IBM Spectrum Protect unterstützt werden, erkannt und verfügbar gemacht. Wenn eine Einheit einer vorhandenen SAN-Umgebung hinzugefügt oder aus einer vorhandenen SAN-Umgebung entfernt wird, müssen Sie mithilfe dieser Option eine erneute Erkennung für die Einheiten ausführen. Einheiten müssen zunächst erkannt werden, damit aktuelle Werte der Einheitenattribute mit der Option Attribute einer erkannten Einheit auflisten angezeigt werden. Unterstützte Einheiten in einem Fibre Channel-SAN sind Bandlaufwerke und Datenträgerwechsler. Der IBM Spectrum Protect-Einheitentreiber ignoriert alle anderen Einheitentypen, wie beispielsweise Platte.

#### Alle definierten Einheiten entfernen

Mit dieser Option werden alle an ein Fibre Channel-SAN angeschlossenen IBM Spectrum Protect-Einheiten mit dem Status `DEFINED` in der ODM-Datenbank entfernt. Falls erforderlich, müssen Sie für Einheiten eine erneute Erkennung ausführen, indem Sie die Option `Von IBM Spectrum Protect unterstützte Einheiten erkennen` auswählen, nachdem alle definierten Einheiten entfernt wurden.

#### Einheit entfernen

Mit dieser Option wird eine einzelne an ein Fibre Channel-SAN angeschlossene IBM Spectrum Protect-Einheit mit dem Status `DEFINED` in der ODM-Datenbank entfernt. Falls erforderlich, müssen Sie für die Einheit eine erneute Erkennung ausführen, indem Sie die Option `Von IBM Spectrum Protect unterstützte Einheiten erkennen` auswählen, nachdem eine definierte Einheit entfernt wurde.



AIX-Betriebssysteme

## IBM Spectrum Protect-Einheitentreiber für Datenträgerwechsler konfigurieren

Verwenden Sie die folgende Prozedur, um IBM Spectrum Protect-Einheitentreiber für Datenträgerwechsler für Speicherarchive anderer Hersteller zu konfigurieren.

### Vorgehensweise

Führen Sie das Programm SMIT aus, um den Einheitentreiber für jeden Datenträgerwechsler oder Robotermechanismus zu konfigurieren:

1. Wählen Sie Devices aus.
2. Wählen Sie IBM Spectrum Protect Devices aus.
3. Wählen Sie Library/MediumChanger aus.
4. Wählen Sie Add a Library/MediumChanger aus.
5. Wählen Sie den IBM Spectrum Protect-SCSI-LB für jedes von IBM Spectrum Protect unterstützte Speicherarchiv aus.
6. Wählen Sie den übergeordneten Adapter aus, mit dem die Einheit verbunden wird. Diese Nummer wird im Format 00-0X aufgelistet; dabei gibt X die Steckplatznummer der SCSI-Adapterkarte an.
7. Geben Sie, wenn Sie dazu aufgefordert werden, die Verbindungsadresse der Einheit ein, die Sie installieren. Die Verbindungsadresse ist eine zweistellige Zahl. Die erste Ziffer ist die SCSI-ID (der Wert, der auf dem Arbeitsblatt notiert wurde). Die zweite Ziffer ist die Nummer der logischen SCSI-Einheit (LUN), die - sofern nicht anders angegeben - normalerweise null ist. Die SCSI-ID und die LUN müssen durch ein Komma (,) voneinander getrennt werden. Beispielsweise hat die Verbindungsadresse 4,0 eine SCSI-ID=4 und eine LUN=0.
8. Klicken Sie auf DO.

Sie erhalten eine Nachricht (Name einer logischen Datei) in der Form `lbX Verfügbar`. Notieren Sie den Wert von X; dabei handelt es sich um eine Zahl, die automatisch vom System zugeordnet wird. Verwenden Sie diese Informationen, um das Feld Einheitenname auf Ihrem Arbeitsblatt auszufüllen.

Wenn die Nachricht beispielsweise `lb0 Verfügbar` lautet, enthält das Feld Einheitenname auf dem Arbeitsblatt den Wert `/dev/lb0`. Verwenden Sie immer das Präfix `/dev/` mit dem von SMIT zur Verfügung gestellten Namen.



AIX-Betriebssysteme

## IBM Spectrum Protect-Einheitentreiber für Bandlaufwerke konfigurieren

Verwenden Sie die folgende Prozedur, um IBM Spectrum Protect-Einheitentreiber für Bandlaufwerke für Speicherarchive anderer Hersteller zu konfigurieren.

## Vorgehensweise

---

Wichtig: IBM Spectrum Protect kann *tar*- oder *dd*-Bänder nicht überschreiben, *tar* oder *dd* kann jedoch IBM Spectrum Protect-Bänder überschreiben.

Einschränkung: Bandlaufwerke können nur gemeinsam genutzt werden, wenn das Laufwerk nicht definiert oder der Server nicht gestartet ist. Der Befehl MKSYSE funktioniert nicht, wenn sowohl IBM Spectrum Protect als auch AIX dasselbe Laufwerk oder dieselben Laufwerke gemeinsam nutzen. Um den nativen Bandeinheitentreiber des Betriebssystems mit einem SCSI-Laufwerk verwenden zu können, muss die Einheit zuerst für AIX und dann für IBM Spectrum Protect konfiguriert werden. Ihre AIX-Dokumentation enthält Informationen zu diesen nativen Einheitentreibern.

Führen Sie das Programm SMIT aus, um den Einheitentreiber für jedes Laufwerk (einschließlich Laufwerke in Speicherarchiven) wie folgt zu konfigurieren:

1. Wählen Sie Devices aus.
2. Wählen Sie IBM Spectrum Protect Devices aus.
3. Wählen Sie Tape Drive aus.
4. Wählen Sie Add a Tape Drive aus.
5. Wählen Sie den IBM Spectrum Protect-SCSI-MT für jedes unterstützte Bandlaufwerk aus.
6. Wählen Sie den Adapter aus, mit dem die Einheit verbunden wird. Diese Nummer wird im Format 00-0X aufgelistet; dabei gibt X die Steckplatznummer der SCSI-Adapterkarte an.
7. Geben Sie, wenn Sie dazu aufgefordert werden, die Verbindungsadresse der Einheit ein, die Sie installieren. Die Verbindungsadresse ist eine zweistellige Zahl. Die erste Ziffer ist die SCSI-ID (der Wert, der auf dem Arbeitsblatt notiert wurde). Die zweite Ziffer ist die Nummer der logischen SCSI-Einheit (LUN), die - sofern nicht anders angegeben - normalerweise null ist. Die SCSI-ID und die LUN müssen durch ein Komma (,) voneinander getrennt werden. Beispielsweise hat die Verbindungsadresse 4,0 eine SCSI-ID=4 und eine LUN=0.
8. Klicken Sie auf DO. Sie erhalten eine Nachricht:

Wenn Sie den Einheitentreiber für eine Bandeinheit (kein IBM® Bandlaufwerk) konfigurieren, erhalten Sie eine Nachricht (Name einer logischen Datei) in der Form *mtX Verfügbar*. Notieren Sie den Wert von X; dabei handelt es sich um eine Zahl, die automatisch vom System zugeordnet wird. Verwenden Sie diese Informationen, um das Feld Einheitenname auf dem Arbeitsblatt auszufüllen.

Wenn die Nachricht beispielsweise *mt0 Verfügbar* lautet, enthält das Feld Einheitenname auf dem Arbeitsblatt den Wert */dev/mt0*. Verwenden Sie immer das Präfix */dev/* mit dem von SMIT zur Verfügung gestellten Namen.

 AIX-Betriebssysteme

## An ein Fibre Channel-SAN angeschlossene Einheiten konfigurieren

---

Um eine an ein Fibre Channel-SAN angeschlossene Einheit zu konfigurieren, führen Sie die Prozedur aus.

### Vorgehensweise

---




1. Führen Sie das Programm SMIT aus.
2. Wählen Sie Devices aus.
3. Wählen Sie IBM Spectrum Protect Devices aus.
4. Wählen Sie Fibre Channel SAN Attached devices aus.
5. Wählen Sie Discover Devices Supported by IBM Spectrum Protect aus. Der Erkennungsprozess kann einige Zeit dauern.
6. Kehren Sie zum Menü Fibre Channel zurück und wählen Sie List Attributes of a Discovered Device aus.
7. Beachten Sie die aus drei Zeichen bestehende Einheiten-ID, die verwendet wird, wenn ein Pfad zu der Einheit für IBM Spectrum Protect definiert wird. Wenn ein Bandlaufwerk beispielsweise die ID *mt2* hat, geben Sie */dev/mt2* als den Einheitennamen an.


 Linux-Betriebssysteme

## Bandeinheitentreiber auf Linux-Systemen konfigurieren

---

Lesen Sie die folgenden Abschnitte, wenn Sie Bandeinheitentreiber auf Linux-Systemen installieren und konfigurieren.

-  Linux-Betriebssysteme IBM Spectrum Protect-Durchgriffstreiber für Bandeinheiten und Speicherarchive konfigurieren  
Um den IBM Spectrum Protect-Durchgriffstreiber unter Linux verwenden zu können, müssen Sie die folgenden Schritte ausführen.
-  Linux-Betriebssysteme zSeries Linux Fibre Channel-Adapter-Einheitentreiber (zfc) installieren  
Der zSeries Linux Fibre Channel-Adapter-Einheitentreiber (zfc) ist ein spezieller Adaptortreiber auf dem IBM® zSeries-System.
-  Linux-Betriebssysteme Informationen zu SCSI-Einheiten Ihres Systems  
Informationen zu den Einheiten, die von Ihrem System erkannt werden, befinden sich in der Datei */proc/scsi/scsi*. Diese Datei enthält eine Liste aller erkannten SCSI-Einheiten.

-  Linux-Betriebssysteme Überschreiben von Bandkennsätzen verhindern  
Der IBM Spectrum Protect-Durchgriffseinheitentreiber verwendet den generischen Linux-SCSI-Einheitentreiber (sg), um Bandeinheiten, die an das System angeschlossen sind, zu steuern und zu betreiben. Wenn der generische Linux-SCSI-Bandeneinheitentreiber (st) in den Kernel geladen wird und angeschlossene Bandeinheiten konfiguriert, können in Bezug auf die Art und Weise, wie eine Einheit verwaltet wird, Konflikte auftreten, da der generische sg-Treiber und der st-Treiber beide dieselbe Einheit steuern können.

 Linux-Betriebssysteme

## IBM Spectrum Protect-Durchgriffstreiber für Bandeinheiten und Speicherarchive konfigurieren

Um den IBM Spectrum Protect-Durchgriffstreiber unter Linux verwenden zu können, müssen Sie die folgenden Schritte ausführen.

### Vorgehensweise

1. Stellen Sie sicher, dass die Einheit mit Ihrem System verbunden ist, eingeschaltet und aktiv ist.
2. Stellen Sie sicher, dass die Einheit von Ihrem System korrekt erkannt wird, indem Sie den folgenden Befehl ausgeben:
 

```
cat /proc/scsi/scsi
```
3. Stellen Sie sicher, dass sowohl das IBM Spectrum Protect-Einheitentreiberpaket (tsmscsi) als auch das Speicherserverpaket installiert ist.
4. Im IBM Spectrum Protect-Einheitentreiberpaket stehen zwei Treiberkonfigurationsmethoden zur Verfügung: autoconf und tsmscsi. Mit beiden Methoden werden die folgenden Tasks ausgeführt:
  - Laden des generischen Linux-SCSI-Treibers (sg) in den Kernel
  - Erstellen der erforderlichen Gerätedateien für den Durchgriffstreiber
  - Erstellen der Einheitendatendateien für Bandeinheiten (/dev/tsmscsi/mtinfo) und Speicherarchive (/dev/tsmscsi/lbinfo)
5. Führen Sie die bevorzugte Konfigurationsmethode (autoconf oder tsmscsi) für den IBM Spectrum Protect-Durchgriffstreiber aus.
  - Um die Konfigurationsmethode autoconf auszuführen, geben Sie den folgenden Befehl aus:

```
autoconf
```

- Um die Konfigurationsmethode tsmscsi auszuführen, führen Sie die folgenden Schritte aus:
    - a. Kopieren Sie die beiden Beispielkonfigurationsdateien, die sich im Installationsverzeichnis befinden, von *mt.conf.smp* und *lb.conf.smp* in *mt.conf* bzw. *lb.conf*.
    - b. Editieren Sie die Dateien *mt.conf* und *lb.conf*. Fügen Sie (wie in dem Beispiel gezeigt am Anfang der Datei) eine Zeilengruppe für jede Kombination aus SCSI-Ziel, ID und LUN hinzu. Jede Kombination aus Einträgen für SCSI-Ziel, ID und LUN entspricht einem Bandlaufwerk oder einem Speicherarchiv, das konfiguriert werden soll. Stellen Sie sicher, dass die Dateien diese Voraussetzungen erfüllen:
      - Entfernen Sie das Beispiel, das sich am Anfang der Dateien befindet.
      - Zwischen jeder Zeilengruppe muss sich eine neue Zeile befinden.
      - Hinter der letzten Zeilengruppe muss sich eine neue Zeile befinden.
      - Stellen Sie sicher, dass keine der Dateien ein Nummernzeichen (#) enthält.
    - c. Führen Sie im Installationsverzeichnis des Einheitentreibers das Script *tsmscsi* aus.
6. Prüfen Sie, ob die Einheit korrekt konfiguriert ist, indem Sie die Textdateien für Bandeinheiten (/dev/tsmscsi/mtinfo) und Speicherarchive (/dev/tsmscsi/lbinfo) anzeigen.
  7. Bestimmen Sie die Gerätedateinamen für die Bandlaufwerke und Speicherarchive:
    - Um die Namen für Bandeinheiten zu bestimmen, geben Sie den folgenden Befehl aus:

```
> ls /dev/tsmscsi/mt*
```

- Um die Namen für Speicherarchive zu bestimmen, geben Sie den folgenden Befehl aus:

```
> ls /dev/tsmscsi/lb*
```


Mithilfe dieser Informationen können Sie ermitteln, welche der Gerätedateinamen /dev/tsmscsi/mtx und /dev/tsmscsi/lbx dem Server zur Verfügung gestellt werden müssen, wenn Sie einen Befehl DEFINE PATH ausgeben.

### Nächste Schritte

Wenn Sie das Hostsystem erneut starten, müssen Sie das Script *autoconf* oder *tsmscsi* erneut ausführen, um IBM Spectrum Protect-Einheiten zu rekonfigurieren. Wenn Sie die IBM Spectrum Protect-Serverinstanz erneut starten, müssen Sie Einheiten nicht rekonfigurieren. Im Allgemeinen ist der generische Linux-SCSI-Treiber im Kernel vorinstalliert. Um zu prüfen, ob sich der Treiber im Kernel befindet, geben Sie den folgenden Befehl aus:

```
> lsmod | grep sg
```

Wenn sich der Treiber nicht im Kernel befindet, geben Sie den Befehl `modprobe sg` aus, um den `sg`-Treiber in den Kernel zu laden.

 Linux-Betriebssysteme

## zSeries Linux Fibre Channel-Adapter-Einheitentreiber (zfcp) installieren

Der zSeries Linux Fibre Channel-Adapter-Einheitentreiber (zfcp) ist ein spezieller Adaptortreiber auf dem IBM® zSeries-System.

### Informationen zu diesem Vorgang

IBM Spectrum Protect und IBM Bandeneinheitentreiber können auf zSeries-Plattformen mit Linux-Betriebssystemen in 64-Bit-Umgebungen ausgeführt werden. Sie unterstützen die meisten OEM-Bandeneinheiten (OEM = Original-Equipment-Manufacturer) und IBM Bandeneinheiten mit Fibre Channel-Schnittstellen.

Weitere Informationen zum Treiber `zfcp` finden Sie im IBM Redpaper, *Getting Started with zSeries Fibre Channel Protocol*, das unter IBM Redbooks verfügbar ist.

### Vorgehensweise

1. Laden Sie das Modul `qdio`.
2. Installieren Sie den Treiber `zfcp`.
3. Ordnen Sie das Fibre Channel Protocol (FCP) zu und konfigurieren Sie den Treiber `zfcp`.
4. Installieren und konfigurieren Sie den IBM Bandeneinheitentreiber.

 Linux-Betriebssysteme

## Informationen zu SCSI-Einheiten Ihres Systems

Informationen zu den Einheiten, die von Ihrem System erkannt werden, befinden sich in der Datei `/proc/scsi/scsi`. Diese Datei enthält eine Liste aller erkannten SCSI-Einheiten.

Die folgenden Einheitsdaten sind verfügbar: Hostnummer, Kanalnummer, SCSI-ID, Nummer der logischen Einheit, Anbieter, Firmwareversion, Einheitentyp und SCSI-Modus. Wenn ein System beispielsweise einige StorageTek- und IBM® Speicherarchive, ein SAN-Gateway und einige Quantum DLT-Laufwerke enthält, sieht die Datei `/proc/scsi/scsi` ähnlich nachfolgend gezeigt aus:

```
Attached devices:
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor: STK      Model: 9738      Rev: 2003
  Type:  Medium Changer      ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor: PATHLIGHT Model: SAN Gateway      Rev: 32aC
  Type:  Unknown            ANSI SCSI revision: 03
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor: QUANTUM  Model: DLT7000      Rev: 2560
  Type:  Sequential-Access  ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 04
  Vendor: IBM      Model: 7337      Rev: 1.63
  Type:  Medium Changer      ANSI SCSI revision: 02
```

 Linux-Betriebssysteme

## Überschreiben von Bandkennsätzen verhindern

Der IBM Spectrum Protect-Durchgriffseinheitentreiber verwendet den generischen Linux-SCSI-Einheitentreiber (`sg`), um Bandeneinheiten, die an das System angeschlossen sind, zu steuern und zu betreiben. Wenn der generische Linux-SCSI-Bandeneinheitentreiber (`st`) in den Kernel geladen wird und angeschlossene Bandeneinheiten konfiguriert, können in Bezug auf die Art und Weise, wie eine Einheit verwaltet wird, Konflikte auftreten, da der generische `sg`-Treiber und der `st`-Treiber beide dieselbe Einheit steuern können.

### Informationen zu diesem Vorgang

Wenn der `st`-Treiber Einheiten steuert, die von IBM Spectrum Protect verwendet werden, können interne IBM Spectrum Protect-Bandkennsätze überschrieben werden und Daten verloren gehen. Wenn eine Anwendung den `st`-Treiber zum Steuern von Einheiten verwendet und die Option, die angibt, dass Bänder nicht zurückgespult werden sollen, nicht definiert ist, werden Bänder automatisch nach Beendigung einer Operation zurückgespult. Mit der Operation zum automatischen Zurückspulen wird der Bandkennsatz wieder auf den Bandanfang positioniert. Wenn das Band im Laufwerk geladen bleibt, wird der IBM Spectrum Protect-Bandkennsatz bei der

nächsten Schreiboperation, die keine IBM Spectrum Protect-Schreiboperation ist, überschrieben, da sich der Kennsatz am Anfang des Bands befindet.

Um zu verhindern, dass IBM Spectrum Protect-Kennsätze überschrieben werden, was zu einem Datenverlust führen kann, müssen Sie sicherstellen, dass nur der IBM Spectrum Protect-Durchgriffstreiber Einheiten steuert, die von IBM Spectrum Protect verwendet werden. Entfernen Sie den st-Treiber aus dem Kernel oder löschen Sie, wenn der Treiber von einigen Anwendungen auf dem System verwendet wird, die Gerätedateien, die den IBM Spectrum Protect-Einheiten entsprechen, sodass der st-Treiber diese nicht mehr steuern kann.

Wenn Sie den IBM Bändeinheitentreiber zum Steuern von Einheiten auf Ihrem System verwenden, können dieselben Probleme in Bezug auf Konflikte bei der Steuerung durch den Einheitentreiber auftreten. Bestimmen Sie anhand der Dokumentation zum IBM Bändeinheitentreiber, wie dieses Problem behoben und ein Datenverlust verhindert werden kann.

Entfernen Sie den st-Treiber.

Wenn keine anderen Anwendungen auf dem System st-Einheiten verwenden, entfernen Sie den st-Treiber aus dem Kernel. Geben Sie den folgenden Befehl aus, um den st-Treiber zu entladen:

```
rmmod st
```

Löschen Sie Gerätedateien für Einheiten, die IBM Spectrum Protect-Einheiten entsprechen.

Wenn Anwendungen vorhanden sind, die die Verwendung des st-Treibers erfordern, löschen Sie die Gerätedateien, die IBM Spectrum Protect-Einheiten entsprechen. Diese Gerätedateien werden vom st-Treiber generiert. Wenn diese Dateien gelöscht werden, kann der st-Treiber die entsprechenden IBM Spectrum Protect-Einheiten nicht mehr steuern. Gerätedateinamen für Bandlaufwerke werden im Verzeichnis /dev/ angezeigt. Ihre Namen haben das Format /dev/[n]st[0-1024][l][m][a].

Listen Sie die Gerätedateinamen für st-Laufwerke und die Gerätedateinamen für IBM Spectrum Protect-Einheiten mit dem Befehl ls auf. Abhängig von der Ausgabe der Einheitenfolgen können Sie Einheiten in der Liste der st-Einheiten finden, die mit Einheiten in der Liste der IBM Spectrum Protect-Einheiten übereinstimmen. Mithilfe des Befehls rm können Sie dann die st-Einheiten löschen.

Geben Sie die folgenden Befehle aus, um die st-Einheiten und die IBM Spectrum Protect-Einheiten aufzulisten:

```
ls -l /dev/*st*
ls -l /dev/tmsmcsi/mt*
```

Löschen Sie die st-Einheiten mit dem Befehl rm:



```
rm /dev/*st*
```

 Windows-Betriebssysteme

## Bändeinheitentreiber auf Windows-Systemen konfigurieren

---

Lesen Sie die Anweisungen zum Installieren und Konfigurieren von Treibern für Bändeinheiten und Speicherarchive auf Windows-Systemen.

-  Windows-Betriebssysteme Verwendung des IBM Spectrum Protect-Durchgriffstreibers für Bändeinheiten und Speicherarchive vorbereiten  
Um den IBM Spectrum Protect-Durchgriffseinheitentreiber unter Windows für Bändeinheiten und Speicherarchive verwenden zu können, müssen Sie die Treiber installieren und die Einheitenamen für den zu verwendenden Server abrufen.
-  Windows-Betriebssysteme IBM Spectrum Protect-SCSI-Treiber für Bändeinheiten und Speicherarchive konfigurieren  
Wenn der Hersteller eines Bandlaufwerks oder Bandarchivs keinen SCSI-Einheitentreiber bereitstellt, müssen Sie den IBM Spectrum Protect-SCSI-Einheitentreiber installieren.

 Windows-Betriebssysteme

## Verwendung des IBM Spectrum Protect-Durchgriffstreibers für Bändeinheiten und Speicherarchive vorbereiten

---

Um den IBM Spectrum Protect-Durchgriffseinheitentreiber unter Windows für Bändeinheiten und Speicherarchive verwenden zu können, müssen Sie die Treiber installieren und die Einheitenamen für den zu verwendenden Server abrufen.

### Vorbereitende Schritte

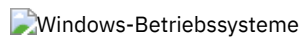
---

1. Stellen Sie fest, ob der Hersteller der Bändeinheit oder des Bandarchivs einen Einheitentreiber zur Verfügung stellt.
2. Wenn der Hersteller ein Einheitentreiberpaket bereitstellt, laden Sie das Paket herunter und installieren Sie es.
3. Konfigurieren Sie die SCSI-Einheitentreiber, indem Sie die Anweisungen des Herstellers ausführen.

## Vorgehensweise

---

1. Installieren Sie den IBM Spectrum Protect-Durchgriffseinheitentreiber.
2. Rufen Sie die Einheitenamen ab, die der Server verwenden muss, indem Sie eine der folgenden Aktionen ausführen:
  - Führen Sie auf dem Server den Befehl QUERY SAN aus. In der Ausgabe werden alle Einheitenamen und ihre zugehörigen Einheitenseriennummern angezeigt.
  - Führen Sie im Serververzeichnis das Dienstprogramm tsmdbl.exe aus. In der Ausgabe werden alle Einheitenamen, ihre zugehörigen Einheitenseriennummern und die zugehörigen Einheitenpositionen angezeigt.
  - Führen Sie in der Windows-Eingabeaufforderung den Befehl regedit aus. Rufen Sie in der Ausgabe die Einheitsdateinamen auf der Basis der Einheitenpositionen ab. Die Position besteht aus der Port-ID, der SCSI-Bus-ID, der LUN-ID und der SCSI-Ziel-ID. Der IBM Spectrum Protect-Einheitsdateiname hat das Format mtA.B.C.C für Bandlaufwerke und lbA.B.C.D für Bandarchive; dabei gilt Folgendes:
    - A ist die SCSI-Ziel-ID.
    - B ist die LUN-ID.
    - C ist die SCSI-Bus-ID.
    - D ist die Port-ID.



## IBM Spectrum Protect-SCSI-Treiber für Bandeinheiten und Speicherarchive konfigurieren

---

Wenn der Hersteller eines Bandlaufwerks oder Bandarchivs keinen SCSI-Einheitentreiber bereitstellt, müssen Sie den IBM Spectrum Protect-SCSI-Einheitentreiber installieren.

### Informationen zu diesem Vorgang

---

Der Name der Datei für den IBM Spectrum Protect-SCSI-Einheitentreiber ist tsmcsi64.sys.

## Vorgehensweise

---

1. Lokalisieren Sie die Einheit in der Konsole des Geräte-Managers (devmgmt.msc) und wählen Sie sie aus. Bandlaufwerke sind unter Bandlaufwerke, Datenträgerwechsler unter Datenträgerwechsler aufgelistet.
2. Konfigurieren Sie die Einheit für die Verwendung durch den Einheitentreiber tsmcsi64.sys:
  - a. Klicken Sie mit der rechten Maustaste auf die Einheit und klicken Sie auf Treibersoftware aktualisieren.
  - b. Klicken Sie auf Auf dem Computer nach Treibersoftware suchen.
3. Klicken Sie auf Aus einer Liste von Gerätetreibern auf dem Computer auswählen.
4. Klicken Sie auf Weiter.
5. Wählen Sie die entsprechende Option aus:
  - a. Wählen Sie für ein Bandlaufwerk IBM Spectrum Protect für Bandlaufwerke aus.
  - b. Wählen Sie für einen Datenträgerwechsler IBM Spectrum Protect für Datenträgerwechsler aus.
6. Klicken Sie auf Weiter.
7. Klicken Sie auf Schließen.
8. Prüfen Sie, ob die Einheit korrekt für den Einheitentreiber tsmcsi64 konfiguriert wurde:
  - a. Klicken Sie mit der rechten Maustaste auf die Einheit und klicken Sie auf Eigenschaften.
  - b. Klicken Sie auf die Registerkarte Treiber und dann auf Treiberdetails. Im Fenster Treiberdetails wird der Einheitentreiber angezeigt, der die Einheit steuert.

## Speicherarchive für die Verwendung durch einen Server konfigurieren

---

Um ein Speicherarchiv oder Speicherarchive für Speicher eines IBM Spectrum Protect-Servers verwenden zu können, müssen Sie zunächst die Einheiten auf dem Serversystem konfigurieren.

### Vorbereitende Schritte

---

1. Schließen Sie Einheiten an die Server-Hardware an. Führen Sie die Anweisungen in Automatisierte Speicherarchivereinheit an das System anschließen aus.
2. Wählen Sie die Bandeinheitentreiber aus. Führen Sie die Anweisungen in Bandeinheitentreiber auswählen aus.
3. Installieren und konfigurieren Sie die Bandeinheitentreiber. Führen Sie die Anweisungen in Bandeinheitentreiber installieren und konfigurieren aus.
4. Bestimmen Sie die Einheitenamen, die zum Definieren des Speicherarchivs für den Server benötigt werden. Führen Sie die Anweisungen in Gerätedateinamen für Bandeinheiten aus.

## Vorgehensweise

---

1. Definieren Sie das Speicherarchiv und den Pfad vom Server zum Speicherarchiv. Führen Sie die Anweisungen in Speicherarchive definieren aus.
2. Definieren Sie die Laufwerke im Speicherarchiv. Führen Sie die Anweisungen in Laufwerke definieren aus.

Bei SCSI-Speicherarchiven und können Sie mithilfe des Befehls `PERFORM LIBACTION` Laufwerke und Pfade für ein Speicherarchiv in einem einzigen Schritt definieren, anstatt die beiden Schritte 2 und 3 auszuführen. Um den Befehl `PERFORM LIBACTION` zum Definieren von Laufwerken und Pfaden für ein Speicherarchiv verwenden zu können, muss die Option `SANDISCOVERY` unterstützt werden und aktiviert sein.

3. Definieren Sie mithilfe des Befehls `DEFINE PATH` einen Pfad vom Server zu jedem Laufwerk.
4. Definieren Sie eine Einheitenklasse. Führen Sie die Anweisungen in Bandeinheitenklassen definieren aus.

Einheitenklassen geben die Aufzeichnungsformate für Laufwerke an und klassifizieren diese gemäß dem Typ. Verwenden Sie den Standardwert `FORMAT=DRIVE` nur dann als Aufzeichnungsformat, wenn alle Laufwerke, die der Einheitenklasse zugeordnet sind, Daten von allen Datenträgern lesen bzw. auf alle Datenträger schreiben können.

Angenommen, es ist eine Kombination aus Ultrium-Laufwerken der Generation 3 und Ultrium-Laufwerken der Generation 4 vorhanden, es sind aber nur Ultrium-Datenträger der Generation 3 vorhanden. Sie können `FORMAT=DRIVE` angeben, da sowohl die Laufwerke der Generation 4 als auch die Laufwerke der Generation 3 Daten von Datenträgern der Generation 3 lesen bzw. auf Datenträger der Generation 3 schreiben können.

5. Definieren Sie einen Speicherpool mithilfe des Befehls `DEFINE STGPOOL`.

Beachten Sie beim Definieren von Speicherpools die folgenden wichtigsten Auswahlmöglichkeiten:

- Arbeitsdatenträger sind leere Datenträger, die für die Verwendung verfügbar sind. Wenn Sie für die maximale Anzahl Arbeitsdatenträger in dem Speicherpool einen Wert angeben, kann der Server aus den in dem Speicherarchiv verfügbaren Arbeitsdatenträgern eine Auswahl treffen.

Wenn keine Arbeitsdatenträger zulässig sind, müssen Sie einen zusätzlichen Schritt ausführen, in dem Sie jeden im Speicherpool zu verwendenden Datenträger explizit definieren. Geben Sie außerdem den Parameter `MAXSCRATCH=0` an, wenn Sie den Speicherpool definieren, damit keine Arbeitsdatenträger verwendet werden.

- Die Standardeinstellung für primäre Speicherpools ist die Kollokation nach Gruppe. Für Kopierspeicherpools und Pools für aktive Daten ist die Kollokation standardmäßig inaktiviert. Mithilfe der *Kollokation* speichert der Server alle Dateien, die zu einer Gruppe von Clientknoten, einem einzelnen Clientknoten, einem Clientdateibereich oder einer Gruppe von Clientdateibereichen gehören, auf möglichst wenigen Datenträgern. Wenn die Kollokation für einen Speicherpool inaktiviert ist und Clients mit dem Speichern von Daten beginnen, können Sie die Daten in dem Pool nicht einfach so ändern, dass sie kollokiert werden.

6. Stellen Sie Datenträger in das Speicherarchiv zurück und ordnen Sie ihnen Kennsätze zu. Führen Sie die Anweisungen in Datenträger in ein automatisiertes Speicherarchiv zurückstellen und Banddatenträgern Kennsätze zuordnen aus.

Stellen Sie sicher, dass genügend Datenträger in dem Speicherarchiv für den Server verfügbar sind. Halten Sie genügend Datenträger mit Kennsätzen bereit, damit während einer Operation, wie beispielsweise einer Clientsicherung, keine Datenträger fehlen. Ordnen Sie zusätzlichen Arbeitsdatenträgern Kennsätze zu, damit später für mögliche Wiederherstellungsoperationen Arbeitsdatenträger verfügbar sind.

Die Prozeduren für das Zurückstellen von Datenträgern und das Zuordnen von Kennsätzen sind, unabhängig davon, ob das Speicherarchiv Laufwerke mit einem einzigen Einheitentyp oder Laufwerke mit mehreren Einheitentypen enthält, identisch. Mit dem Befehl `CHECKIN LIBVOLUME` können Sie Datenträger, denen bereits ein Kennsatz zugeordnet wurde, zurückstellen. Wenn Datenträger gleichzeitig mit dem Zuordnen eines Kennsatzes zurückgestellt werden sollen, geben Sie den Befehl `LABEL LIBVOLUME` aus.

Speicherarchive mit mehreren Einheitentypen: Wenn Ihr Speicherarchiv Laufwerke mit mehreren Einheitentypen enthält und Sie zwei Speicherarchive für den IBM Spectrum Protect-Server definiert hatten, stellen die beiden definierten Speicherarchive ein einziges physisches Speicherarchiv dar. Sie müssen Banddatenträger separat in jedes definierte Speicherarchiv zurückstellen. Stellen Sie sicher, dass die Datenträger in das korrekte IBM Spectrum Protect-Speicherarchiv zurückgestellt werden.

## Nächste Schritte

---

Überprüfen Sie Ihre Einheitendefinitionen, um sicherzustellen, dass die gesamte Konfiguration korrekt ist. Mit dem Befehl `QUERY` können Sie Informationen zu jedem Speicherobjekt überprüfen.

Stellen Sie bei der Überprüfung der Ergebnisse des Befehls `QUERY DRIVE` sicher, dass der Einheitentyp für das Laufwerk wie erwartet lautet. Wenn ein Pfad nicht definiert ist, wird der Laufwerkeinheitentyp als `UNKNOWN` aufgelistet; wenn der falsche Pfad verwendet wird, wird `GENERIC_TAPE` oder ein anderer Einheitentyp angezeigt. Dieser Schritt ist insbesondere dann wichtig, wenn gemischte Datenträger verwendet werden.



Konfigurieren Sie wahlweise die gemeinsame Speicherarchivnutzung. Führen Sie die Anweisungen in Gemeinsame Speicherarchivnutzung konfigurieren aus.

- Bandeinheiten definieren  
Bevor Sie Daten sichern oder auf Band umlagern können, müssen Sie eine Bandeinheit für IBM Spectrum Protect definieren.
- Gemeinsame Speicherarchivnutzung konfigurieren  
Mehrere IBM Spectrum Protect-Server können Speichereinheiten unter Verwendung eines Speicherbereichsnetzes (SAN) gemeinsam nutzen. Ein Server wird als Speicherarchivmanager konfiguriert, die anderen Server werden als Speicherarchivclients konfiguriert.

#### Zugehörige Verweise:

- 🔗 CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
- 🔗 LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)
- 🔗 PERFORM LIBACTION (Alle Laufwerke und Pfade für ein Speicherarchiv definieren oder löschen)

#### Zugehörige Informationen:

- 🔗 DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

## Bandeinheiten definieren

---

Bevor Sie Daten sichern oder auf Band umlagern können, müssen Sie eine Bandeinheit für IBM Spectrum Protect definieren.

- Speicherarchive und Laufwerke definieren  
Ein Bandarchiv kann ein oder mehrere Bandlaufwerke enthalten. Nachfolgend ist beschrieben, wie Speicherarchive, Laufwerke und Pfade für den IBM Spectrum Protect-Server definiert werden.
- Bandeinheitenklassen definieren  
Eine Einheitenklasse definiert eine Reihe von Merkmalen, die von einer Gruppe von Datenträgern verwendet wird, die in einem Speicherpool erstellt werden kann. Sie müssen eine Einheitenklasse für eine Bandeinheit definieren, um sicherzustellen, dass der Server die Einheit verwenden kann.

## Speicherarchive und Laufwerke definieren

---

Ein Bandarchiv kann ein oder mehrere Bandlaufwerke enthalten. Nachfolgend ist beschrieben, wie Speicherarchive, Laufwerke und Pfade für den IBM Spectrum Protect-Server definiert werden.

- Speicherarchive definieren  
Bevor ein Laufwerk verwendet werden kann, muss das Speicherarchiv, zu dem das Laufwerk gehört, definiert werden.
- Laufwerke definieren  
Um den Server über ein Laufwerk zu informieren, das für den Zugriff auf Speicherdatenträger verwendet werden kann, geben Sie den Befehl DEFINE DRIVE gefolgt vom Befehl DEFINE PATH aus.

## Speicherarchive definieren

---

Bevor ein Laufwerk verwendet werden kann, muss das Speicherarchiv, zu dem das Laufwerk gehört, definiert werden.

### Vorgehensweise


---

1. Definieren Sie das Speicherarchiv mit dem Befehl DEFINE LIBRARY.

Beispielsweise können Sie bei einem Bandarchiv IBM TS3500 mithilfe des folgenden Befehls ein Speicherarchiv mit dem Namen ROBOTMOUNT definieren:

```
define library robotmount libtype=scsi
```

Wenn die gemeinsame Speicherarchivnutzung oder die LAN-unabhängige Datenversetzung erforderlich ist, lesen Sie die folgenden Informationen:

- Gemeinsame Speicherarchivnutzung konfigurieren
  - LAN-unabhängige Datenversetzung konfigurieren
2. Definieren Sie mithilfe des Befehls DEFINE PATH einen Pfad vom Server zum Speicherarchiv. Wenn Sie den Parameter DEVICE angeben, geben Sie den Gerätedateinamen für die Einheit ein. Dieser Name wird vom Server für die Kommunikation mit Bandlaufwerken, Datenträgerwechslern, und Einheiten für austauschbare Datenträger benötigt. Weitere Informationen zu Gerätedateinamen für Einheiten finden Sie in Gerätedateinamen für Bandeinheiten.  AIX-Betriebssysteme

```
define path server1 robotmount srctype=server desttype=library  
device=/dev/lb0
```

## Linux-Betriebssysteme



```
define path server1 robotmount srctype=server desttype=library
device=/dev/tmscsi/lb0
```

## Windows-Betriebssysteme

```
define path server1 robotmount srctype=server desttype=library
device=lb0.0.1.0
```

- SCSI-Speicherarchive in einem SAN definieren  
Beim Speicherarchivtyp SCSI in einem SAN kann der Server die Seriennummer des Speicherarchivs verfolgen. Mit der Seriennummer kann der Server die Identität der Einheit bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet.

### Zugehörige Informationen:

-  DEFINE LIBRARY (Speicherarchiv definieren)
-  DEFINE PATH (Pfad definieren)

## Laufwerke definieren

---

Um den Server über ein Laufwerk zu informieren, das für den Zugriff auf Speicherdatenträger verwendet werden kann, geben Sie den Befehl DEFINE DRIVE gefolgt vom Befehl DEFINE PATH aus.

### Vorbereitende Schritte

---

Ein *Laufwerkobjekt* stellt einen Laufwerkmechanismus in einem Speicherarchiv dar, das austauschbare Datenträger verwendet. Bei Einheiten mit mehreren Laufwerken, einschließlich automatisierter Speicherarchive, müssen Sie jedes Laufwerk separat definieren und einem Speicherarchiv zuordnen. Laufwerkdefinitionen können Informationen wie die Elementadresse für Laufwerke in SCSI-Speicherarchiven, die Anzahl Reinigungsvorgänge für ein Bandlaufwerk und die Angabe enthalten, ob das Laufwerk online ist.

IBM Spectrum Protect unterstützt Bandlaufwerke, bei denen es sich um Standalone-Bandlaufwerke handeln kann oder die Teil eines automatisierten Speicherarchivs sein können. Die bevorzugte Methode ist die Konfiguration der Bandspeicherlösung durch die Verwendung automatisierter Speicherarchive.

### Informationen zu diesem Vorgang

---

Wenn Sie den Befehl DEFINE DRIVE ausgeben, müssen Sie einen Teil oder alle der folgenden Informationen zur Verfügung stellen:

#### Speicherarchivname

Der Name des Speicherarchivs, in dem sich das Laufwerk befindet.

#### Laufwerkname

Der Name, der dem Laufwerk zugeordnet ist.

#### Seriennummer

Die Seriennummer des Laufwerks. Der Parameter für die Seriennummer gilt nur für Laufwerke in SCSI-Speicherarchiven. Mit der Seriennummer kann der Server die Identität der Einheit bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet.

Falls gewünscht, können Sie die Seriennummer angeben. Standardmäßig kann der Server die Seriennummer vom Laufwerk selbst abrufen, wenn der Pfad definiert wird. Wenn Sie die Seriennummer angeben, bestätigt der Server, dass die Seriennummer korrekt ist, wenn Sie den Pfad zu dem Laufwerk definieren. Wenn Sie den Pfad definieren, können Sie den Parameter AUTODETECT=YES angeben, um dem Server die Korrektur der Seriennummer zu ermöglichen, wenn die von ihm erkannte Nummer nicht mit Ihrer Eingabe bei der Definition des Laufwerks übereinstimmt. Ein bewährtes Verfahren ist die Angabe des Parameters AUTODETECT=YES, damit die Seriennummer für das Laufwerk automatisch in der Datenbank aktualisiert wird, wenn der Pfad definiert wird.

Abhängig vom Leistungsspektrum des Laufwerks kann der Server die Seriennummer möglicherweise nicht automatisch erkennen. In diesem Fall zeichnet der Server keine Seriennummer für die Einheit auf und kann die Identität der Einheit nicht bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet. Siehe Auswirkungen von Einheitenänderungen im SAN.

#### Elementadresse

Die Elementadresse des Laufwerks. Der Parameter ELEMENT gilt nur für Laufwerke in SCSI-Speicherarchiven. Die Elementadresse ist eine Zahl, die die physische Position eines Laufwerks in einem automatisierten Speicherarchiv angibt. Der Server benötigt die Elementadresse, um die physische Position des Laufwerks mit der SCSI-Adresse des Laufwerks zu verbinden. Der Server kann die Elementadresse vom Laufwerk abrufen, wenn Sie den Pfad definieren, oder Sie können die Elementadresse angeben, wenn Sie das Laufwerk definieren. Ein bewährtes Verfahren ist die Angabe des Parameters ELEMENT=AUTODETECT, damit der Server die Elementnummer automatisch erkennt, wenn der Pfad zu dem Laufwerk definiert wird.

Abhängig vom Leistungsspektrum des Speicherarchivs kann der Server die Elementadresse möglicherweise nicht automatisch erkennen. In diesem Fall müssen Sie die Elementadresse angeben, wenn Sie das Laufwerk definieren, falls das Speicherarchiv über mehrere Laufwerke verfügt. Um die Elementadresse abzurufen, rufen Sie das IBM® Support Portal for IBM Spectrum Protect auf.

Tipp: IBM Bandeinheitentreiber und Bandeinheitentreiber anderer Hersteller als IBM generieren unterschiedliche Einheitendateien und Formate:

- Bei IBM Bandeinheitentriibern beginnen Einheitenamen mit rmt, gefolgt von einer ganzen Zahl, beispielsweise /dev/rmt0.
- Bei IBM Spectrum Protect-Bandeinheitentriibern beginnen Bandeinheitenamen mit mt, gefolgt von einer ganzen Zahl, beispielsweise /dev/mt0.

Sie müssen die korrekte Einheitendatei verwenden, wenn Sie einen Pfad definieren.

## Vorgehensweise

---

1. Ordnen Sie einem Speicherarchiv ein Laufwerk zu, indem Sie den Befehl DEFINE DRIVE ausgeben.
2. Damit der Server das Laufwerk verwenden kann, geben Sie den Befehl DEFINE PATH aus.

Beispiele für die Konfiguration von Speicherarchiven, Pfaden und Laufwerken finden Sie in Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit einem einzigen Laufwerkeinheitentyp konfigurieren und Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit mehreren Laufwerkeinheitentypen konfigurieren.

## Bandeinheitenklassen definieren

---

Eine Einheitenklasse definiert eine Reihe von Merkmalen, die von einer Gruppe von Datenträgern verwendet wird, die in einem Speicherpool erstellt werden kann. Sie müssen eine Einheitenklasse für eine Bandeinheit definieren, um sicherzustellen, dass der Server die Einheit verwenden kann.

## Vorbereitende Schritte

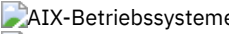
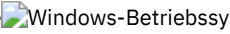
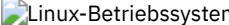
---

Sie müssen Speicherarchive und Laufwerke für den Server definieren, bevor Sie Einheitenklassen definieren.

## Informationen zu diesem Vorgang

---

Eine Liste der unterstützten Einheiten und gültigen Einheitenklassenformate finden Sie auf der Website mit den von IBM Spectrum Protect unterstützten Einheiten für Ihr Betriebssystem:

-   Supported devices for AIX and Windows
-  Supported devices for Linux

Sie können mehrere Einheitenklassen für jeden Einheitentyp definieren. Beispielsweise möchten Sie möglicherweise unterschiedliche Attribute für unterschiedliche Speicherpools angeben, die denselben Typ von Bandlaufwerk verwenden. Unter Umständen sind Variationen erforderlich, die nicht einheitenspezifisch sind, sondern davon abhängig sind, wie die Einheit verwendet werden soll (zum Beispiel Mount-Aufbewahrungszeitraum oder Mountlimit).

Richtlinien:

- Eine einzelne Einheitenklasse kann mehreren Speicherpools zugeordnet werden, jeder Speicherpool ist jedoch nur einer einzigen Einheitenklasse zugeordnet.
- SCSI-Speicherarchive können Bandlaufwerke mehrerer Einheitentypen umfassen. Wenn Sie die Einheitenklasse in dieser Umgebung definieren, müssen Sie einen Wert für den Parameter FORMAT deklarieren.

Weitere Informationen finden Sie in Gemischte Einheitentypen in Speicherarchiven.

## Vorgehensweise

---

Um eine Einheitenklasse zu definieren, verwenden Sie den Befehl DEFINE DEVCLASS mit dem Parameter DEVTYPE, mit dem der Einheitenklasse ein Einheitentyp zugeordnet wird.

## Ergebnisse

---

Wenn Sie die Option DEVCONFIG in die Datei dsmserv.opt einschließen, werden die über diese Option angegebenen Dateien automatisch mit den Ergebnissen der Befehle DEFINE DEVCLASS, UPDATE DEVCLASS und DELETE DEVCLASS aktualisiert.

- Einheitenklassen LTO definieren  
Um Probleme beim Mischen verschiedener Generationen von LTO-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv zu vermeiden, beachten Sie die Einschränkungen. Beachten Sie außerdem die Einschränkungen für die LTO-Laufwerkverschlüsselung.
- Einheitenklassen 3592 definieren  
Einheitenklassendefinitionen für 3592-, TS1130-, TS1140-, TS1150-Einheiten und Einheiten späterer Generationen umfassen Parameter für höhere Datenträgerzugriffsgeschwindigkeiten und Laufwerkverschlüsselung. Um Probleme beim Mischen verschiedener Generationen von 3592- und TS1130-Laufwerken und Laufwerken späterer Generationen in einem Speicherarchiv zu verhindern, lesen Sie die Richtlinien.

#### Zugehörige Verweise:

➔ DEFINE DEVCLASS (Einheitenklasse definieren)

#### Zugehörige Informationen:

➔ QUERY DEVCLASS (Informationen zu einer oder mehreren Einheitenklassen anzeigen)

➔ UPDATE DEVCLASS (Einheitenklasse aktualisieren)

## Einheitenklassen LTO definieren

Um Probleme beim Mischen verschiedener Generationen von LTO-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv zu vermeiden, beachten Sie die Einschränkungen. Beachten Sie außerdem die Einschränkungen für die LTO-Laufwerkverschlüsselung.

- LTO-Laufwerke und -Datenträger in einem Speicherarchiv mischen  
Beim Mischen verschiedener Generationen von LTO-Laufwerken und -Datenträgern müssen Sie die Schreib-/Lesefunktionalität jeder Generation berücksichtigen. Die bevorzugte Methode ist die Konfiguration einer anderen Einheitenklasse für jede Generation von Datenträgern.
- Mountlimits in LTO-Umgebungen mit gemischten Datenträgern  
In einem Speicherarchiv mit gemischten Datenträgern, in dem mehrere Einheitenklassen auf dasselbe Speicherarchiv verweisen, werden kompatible Laufwerke von Speicherpools gemeinsam genutzt. Stellen Sie sicher, dass Sie für den Parameter MOUNTLIMIT in jeder der Einheitenklassen einen geeigneten Wert festlegen.
- Laufwerkverschlüsselung für LTO-Bandlaufwerke der Generation 4 oder späterer Generationen aktivieren und inaktivieren  
IBM Spectrum Protect unterstützt die drei Typen von Laufwerkverschlüsselung, die für LTO-Laufwerke der Generation 4 oder späterer Generationen verfügbar sind: Anwendung, System und Speicherarchiv. Diese Verfahren werden über die Hardware definiert.

## LTO-Laufwerke und -Datenträger in einem Speicherarchiv mischen

Beim Mischen verschiedener Generationen von LTO-Laufwerken und -Datenträgern müssen Sie die Schreib-/Lesefunktionalität jeder Generation berücksichtigen. Die bevorzugte Methode ist die Konfiguration einer anderen Einheitenklasse für jede Generation von Datenträgern.

### Informationen zu diesem Vorgang

Wenn Sie das Mischen verschiedener Generationen von LTO-Datenträgern und -Laufwerken in Betracht ziehen, beachten Sie die folgenden Einschränkungen:

Tabelle 1. Schreib-/Lesefunktionalität für verschiedene Generationen von LTO-Laufwerken

| Laufwerke    | Datenträger der Generation 1 | Datenträger der Generation 2 | Datenträger der Generation 3 | Datenträger der Generation 4 | Datenträger der Generation 5 | Datenträger der Generation 6 | Datenträger der Generation 7 |
|--------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|
| Generation 1 | Schreib-/Lesezugriff         | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             |
| Generation 2 | Schreib-/Lesezugriff         | Schreib-/Lesezugriff         | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             |
| Generation 3 | Lesezugriff                  | Schreib-/Lesezugriff         | Schreib-/Lesezugriff         | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             |
| Generation 4 | nicht zutreffend             | Lesezugriff                  | Schreib-/Lesezugriff         | Schreib-/Lesezugriff         | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             |
| Generation 5 | nicht zutreffend             | nicht zutreffend             | Lesezugriff                  | Schreib-/Lesezugriff         | Schreib-/Lesezugriff         | nicht zutreffend             | nicht zutreffend             |
| Generation 6 | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | Lesezugriff                  | Schreib-/Lesezugriff         | Schreib-/Lesezugriff         | nicht zutreffend             |

| Laufwerke    | Datenträger der Generation 1 | Datenträger der Generation 2 | Datenträger der Generation 3 | Datenträger der Generation 4 | Datenträger der Generation 5 | Datenträger der Generation 6 | Datenträger der Generation 7 |
|--------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|
| Generation 7 | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | Lesezugriff                  | Schreib-/Lesezugriff         | Schreib-/Lesezugriff         |

## Beispiel

Wenn Sie verschiedene Typen von Laufwerken und Datenträgern mischen, konfigurieren Sie unterschiedliche Einheitenklassen: eine Einheitenklasse für jeden Datenträgertyp. Um den Datenträgertyp anzugeben, verwenden Sie den Parameter FORMAT in jeder der Einheitenklassendefinitionen. (Geben Sie nicht FORMAT=DRIVE an.) Wenn Sie beispielsweise Ultrium-Laufwerke der Generation 5 und Ultrium-Laufwerke der Generation 6 mischen, geben Sie FORMAT=ULTRIUM5C (oder ULTRIUM5) für die Ultrium-Einheitenklasse der Generation 5 und FORMAT=ULTRIUM6C (oder ULTRIUM6) für die Ultrium-Einheitenklasse der Generation 6 an.

In diesem Beispiel können beide Einheitenklassen auf dasselbe Speicherarchiv mit Ultrium-Laufwerken der Generation 5 und Ultrium-Laufwerken der Generation 6 verweisen. Die Laufwerke werden von den beiden Speicherpools gemeinsam genutzt. Ein Speicherpool verwendet ausschließlich die erste Einheitenklasse und Ultrium-Datenträger der Generation 5. Der andere Speicherpool verwendet ausschließlich die zweite Einheitenklasse und Ultrium-Datenträger der Generation 6. Da die beiden Speicherpools ein einzelnes Speicherarchiv gemeinsam nutzen, können Ultrium-Datenträger der Generation 5 in Ultrium-Laufwerken der Generation 6 bereitgestellt werden, sobald sie während der Mountpunktverarbeitung verfügbar werden.

Wenn Sie ältere Generationen von Datenträgern mit Lesezugriff mit neueren Generationen von Datenträgern mit Schreib-/Lesezugriff in einem einzelnen Speicherarchiv mischen, müssen Sie die Datenträger mit Lesezugriff als schreibgeschützt markieren und alle Arbeitsdatenträger mit Lesezugriff entnehmen. Wenn Sie beispielsweise Ultrium-Laufwerke und -Datenträger der Generation 4 und Ultrium-Laufwerke und -Datenträger der Generation 6 in einem einzelnen Speicherarchiv mischen, müssen Sie die Datenträger der Generation 4 als schreibgeschützt markieren. Außerdem müssen alle Arbeitsdatenträger der Generation 4 entnommen werden.

## Mountlimits in LTO-Umgebungen mit gemischten Datenträgern

In einem Speicherarchiv mit gemischten Datenträgern, in dem mehrere Einheitenklassen auf dasselbe Speicherarchiv verweisen, werden kompatible Laufwerke von Speicherpools gemeinsam genutzt. Stellen Sie sicher, dass Sie für den Parameter MOUNTLIMIT in jeder der Einheitenklassen einen geeigneten Wert festlegen.

Beispielsweise können in einem Speicherarchiv mit gemischten Datenträgern, das Ultrium-Laufwerke und -Datenträger der Generation 1 und der Generation 2 enthält, Ultrium-Datenträger der Generation 1 in Ultrium-Laufwerken der Generation 2 bereitgestellt werden.

Betrachten Sie das Beispiel für ein Speicherarchiv mit gemischten Datenträgern, das die folgenden Laufwerke und Datenträger enthält:

- Vier LTO Ultrium-Laufwerke der Generation 1 und LTO Ultrium-Datenträger der Generation 1
- Vier LTO Ultrium-Laufwerke der Generation 2 und LTO Ultrium-Datenträger der Generation 2

Sie haben die folgenden Einheitenklassen erstellt:

- Einheitenklasse LTO1CLASS für LTO Ultrium Generation 1 mit der Angabe FORMAT=ULTRIUMC
- Einheitenklasse LTO2CLASS für LTO Ultrium Generation 2 mit der Angabe FORMAT=ULTRIUM2C

Außerdem haben Sie die folgenden Speicherpools erstellt:

- LTO Ultrium-Speicherpool LTO1POOL der Generation 1, der auf Einheitenklasse LTO1CLASS basiert
- LTO Ultrium-Speicherpool LTO2POOL der Generation 2, der auf Einheitenklasse LTO2CLASS basiert

Die Anzahl Mountpunkte, die von jedem Speicherpool verwendet werden können, wird mit dem Parameter MOUNTLIMIT in der Einheitenklasse angegeben. Der Parameter MOUNTLIMIT in der Einheitenklasse LTO2CLASS muss auf 4 gesetzt werden, damit er mit der Anzahl verfügbarer Laufwerke übereinstimmt, die nur LTO2-Datenträger bereitstellen können. Der Parameter MOUNTLIMIT in der Einheitenklasse LTO1CLASS muss auf einen Wert gesetzt werden, der größer als die Anzahl verfügbarer Laufwerke (5 oder möglicherweise 6) ist, um der Tatsache Rechnung zu tragen, dass Ultrium-Datenträger der Generation 1 in Ultrium-Laufwerken der Generation 2 bereitgestellt werden können. Der optimale Wert für MOUNTLIMIT ist von der Workload und Speicherpoolzugriffsmustern abhängig.

Überwachen Sie die Einstellung für MOUNTLIMIT und passen Sie sie gemäß sich ändernden Workloads an. Wenn der Wert für MOUNTLIMIT für LTO1POOL zu hoch definiert wird, können Mountanforderungen für LTO2POOL verzögert werden oder fehlschlagen, da die Ultrium-Laufwerke der Generation 2 zur Ausführung von Mountanforderungen für Ultrium Generation 1 verwendet werden. Im Worst-Case-Szenario kann ein zu starkes Konkurrieren um Ultrium-Laufwerke der Generation 2 dazu führen, dass Mounts für Datenträger der Generation 2 mit der folgenden Nachricht fehlschlagen:

ANR8447E Gegenwärtig sind keine Laufwerke im Kassettenarchiv verfügbar.

Wenn der Wert für MOUNTLIMIT für LTO1POOL nicht hoch genug definiert wird, werden Mountanforderungen, die von LTO Ultrium-Laufwerken der Generation 2 ausgeführt werden könnten, verzögert.

Einschränkung: Aufgrund der Art und Weise, auf die Mountpunkte zugeordnet werden, gelten beim Kombinieren von Ultrium-Laufwerken der Generation 1 mit Ultrium-Laufwerken der Generation 2 oder der Generation 3 Einschränkungen. Prozesse, die mehrere Mountpunkte erfordern, die sowohl Ultrium-Datenträger der Generation 1 als auch Ultrium-Datenträger der Generation 2 einschließen, versuchen beispielsweise unter Umständen, nur Ultrium-Laufwerke der Generation 2 zu reservieren, selbst wenn ein einzelner Mount von einem verfügbaren Ultrium-Laufwerk der Generation 1 ausgeführt werden kann. Zu den Prozessen, die dieses Verhalten zeigen, gehören die Befehle MOVE DATA und BACKUP STGPOOL. Diese Prozesse warten, bis die erforderliche Anzahl Mountpunkte mit Ultrium-Laufwerken der Generation 2 erreicht werden kann.

#### Zugehörige Verweise:

- ➔ BACKUP STGPOOL (Daten in primären Speicherpools in einem Kopierspeicherpool sichern)
- ➔ DEFINE DEVCLASS (Einheitenklasse definieren)
- ➔ MOVE DATA (Dateien auf einen Speicherpoolatenträger versetzen)

## Laufwerkverschlüsselung für LTO-Bandlaufwerke der Generation 4 oder späterer Generationen aktivieren und inaktivieren

---

IBM Spectrum Protect unterstützt die drei Typen von Laufwerkverschlüsselung, die für LTO-Laufwerke der Generation 4 oder späterer Generationen verfügbar sind: Anwendung, System und Speicherarchiv. Diese Verfahren werden über die Hardware definiert.

### Informationen zu diesem Vorgang

---

Der Parameter DRIVEENCRYPTION im Befehl DEFINE DEVCLASS gibt an, ob die Laufwerkverschlüsselung für IBM und HP LTO-Formate der Generation 4 oder späterer Generationen sowie für Ultrium 4- und Ultrium 4C-Formate zulässig ist. Mit diesem Parameter wird IBM Spectrum Protect-Kompatibilität mit Hardwareverschlüsselungseinstellungen für leere Datenträger sichergestellt. Sie können diesen Parameter nicht für Speicherpoolatenträger verwenden, die voll sind oder gefüllt werden.

IBM Spectrum Protect unterstützt das Anwendungsverschlüsselungsverfahren mit IBM und HP LTO-4-Laufwerken oder Laufwerken späterer Generationen. Die System- und Speicherarchivverfahren werden nur von IBM LTO-4 oder späteren Generationen unterstützt. Das Speicherarchivverschlüsselungsverfahren kann nur verwendet werden, wenn es von Ihrer Systemhardware (beispielsweise IBM TS3500) unterstützt wird.

Einschränkung: Sie können keine Laufwerkverschlüsselung für WORM-Datenträger (WORM = Write Once Read Many) verwenden.

Das Anwendungsverfahren wird über die Hardware definiert. Um das Anwendungsverfahren zu verwenden, bei dem IBM Spectrum Protect Verschlüsselungsschlüssel generiert und verwaltet, setzen Sie den Parameter DRIVEENCRYPTION auf ON. Mit dieser Aktion wird die Datenverschlüsselung für leere Datenträger aktiviert. Wenn der Parameter auf ON gesetzt wird und die Hardware für ein anderes Verschlüsselungsverfahren konfiguriert ist, schlagen Sicherungsoperationen fehl.

### Vorgehensweise

---

Das folgende vereinfachte Beispiel zeigt die Schritte für die Aktivierung und die Inaktivierung der Datenverschlüsselung für leere Datenträger in einem Speicherpool:

1. Definieren Sie ein Speicherarchiv, indem Sie den Befehl DEFINE LIBRARY ausgeben:

```
define library 3584 libtype=SCSI
```

2. Definieren Sie eine Einheitenklasse mit dem Namen LTO\_ENCRYPT, indem Sie den Befehl DEFINE DEVCLASS unter Angabe von IBM Spectrum Protect als Schlüsselmanager ausgeben:

```
define devclass lto_encrypt library=3584 devtype=lto driveencryption=on
```

3. Definieren Sie einen Speicherpool, indem Sie den Befehl DEFINE STGPOOL ausgeben:

```
define stgpool lto_encrypt_pool lto_encrypt
```

4. Um die Verschlüsselung für neue Datenträger zu inaktivieren, setzen Sie den Parameter DRIVEENCRYPTION auf OFF. Der Standardwert ist ALLOW. Die Laufwerkverschlüsselung für leere Datenträger ist zulässig, wenn ein anderes Verschlüsselungsverfahren aktiviert ist.

#### Zugehörige Konzepte:

Verschlüsselungsverfahren für Bänder

## Einheitenklassen 3592 definieren

---

Einheitenklassendefinitionen für 3592-, TS1130-, TS1140-, TS1150-Einheiten und Einheiten späterer Generationen umfassen Parameter für höhere Datenträgerzugriffsgeschwindigkeiten und Laufwerkverschlüsselung. Um Probleme beim Mischen verschiedener Generationen von 3592- und TS1130-Laufwerken und Laufwerken späterer Generationen in einem Speicherarchiv zu verhindern, lesen Sie die Richtlinien.

- Generationen von 3592-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv mischen  
Um eine optimale Leistung zu erzielen, dürfen Sie keine Generationen von 3592-Datenträgern in einem einzelnen Speicherarchiv mischen. Es können Datenträgerprobleme auftreten, wenn verschiedene Laufwerkgenerationen gemischt werden. Beispielsweise kann IBM Spectrum Protect möglicherweise den Kennsatz eines Datenträgers nicht lesen.
- Datenzugriffsgeschwindigkeiten für 3592-Datenträger steuern  
Sie können die Speicherkapazität optimieren und Datenzugriffsgeschwindigkeiten verbessern, wenn Sie Datenträger erstellen. Indem Daten in Speicherpools mit Datenträgern partitioniert werden, können Sie die Skalierungskapazität in Prozent angeben, um maximale Speicherkapazität oder schnellen Zugriff auf den Datenträger bereitzustellen zu können.
- Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen aktivieren und inaktivieren  
Bei IBM Spectrum Protect können Sie die folgenden Typen von Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen verwenden: Anwendung, System und Speicherarchiv. Diese Verfahren werden über die Hardware definiert.

## Generationen von 3592-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv mischen

Um eine optimale Leistung zu erzielen, dürfen Sie keine Generationen von 3592-Datenträgern in einem einzelnen Speicherarchiv mischen. Es können Datenträgerprobleme auftreten, wenn verschiedene Laufwerkgenerationen gemischt werden. Beispielsweise kann IBM Spectrum Protect möglicherweise den Kennsatz eines Datenträgers nicht lesen.

### Informationen zu diesem Vorgang

Die folgende Tabelle zeigt Schreib-/Leseinteroperabilität für Laufwerkgenerationen.

| Laufwerke    | Format der Generation 1 | Format der Generation 2 | Format der Generation 3 | Format der Generation 4 | Format der Generation 5 |
|--------------|-------------------------|-------------------------|-------------------------|-------------------------|-------------------------|
| Generation 1 | Schreib-/Lesezugriff    | nicht zutreffend        | nicht zutreffend        | nicht zutreffend        | nicht zutreffend        |
| Generation 2 | Schreib-/Lesezugriff    | Schreib-/Lesezugriff    | nicht zutreffend        | nicht zutreffend        | nicht zutreffend        |
| Generation 3 | Lesezugriff             | Schreib-/Lesezugriff    | Schreib-/Lesezugriff    | nicht zutreffend        | nicht zutreffend        |
| Generation 4 | nicht zutreffend        | Lesezugriff             | Schreib-/Lesezugriff    | Schreib-/Lesezugriff    | nicht zutreffend        |
| Generation 5 | nicht zutreffend        | nicht zutreffend        | Lesezugriff             | Schreib-/Lesezugriff    | Schreib-/Lesezugriff    |

Wenn Generationen von Laufwerken in einem Speicherarchiv gemischt werden müssen, schauen Sie sich das Beispiel und die Einschränkungen an, um Probleme zu vermeiden.

Tabelle 1. Generationen von Laufwerken mischen

| Speicherarchivtyp | Beispiel und Einschränkungen |
|-------------------|------------------------------|
|-------------------|------------------------------|

| Speicherarchivtyp | Beispiel und Einschränkungen   |
|-------------------|--|
| SCSI              | <p>Definieren Sie einen neuen Speicherpool und eine neue Einheitenklasse für die neueste Laufwerkgeneration. Angenommen, Sie verfügen über einen Speicherpool und eine Einheitenklasse für 3592-2. Der Speicherpool enthält alle Datenträger, die im Format der Generation 2 geschrieben wurden. Angenommen, der Wert des Parameters FORMAT in der Einheitenklassendefinition ist auf 3952-2 (nicht DRIVE) gesetzt. Sie fügen dem Speicherarchiv Laufwerke der Generation 3 hinzu. Führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Setzen Sie in der neuen Einheitenklassendefinition für die Laufwerke der Generation 3 den Wert für den Parameter FORMAT auf 3592-3 oder 3592-3C. Geben Sie nicht DRIVE an.</li> <li>2. Aktualisieren Sie in der Definition des Speicherpools, der Laufwerken der Generation 2 zugeordnet ist, den Parameter MAXSCRATCH mit 0, beispielsweise:</li> </ol> <pre>update stgpool genpool2 maxscratch=0</pre> <p>Diese Methode ermöglicht beiden Generationen die Verwendung ihres optimalen Formats und minimiert mögliche Datenträgerprobleme, die aus dem Mischen von Generationen resultieren können. Es werden jedoch nicht alle Datenträgerprobleme behoben. Beispielsweise könnten Konkurrenzsituationen bei Mountpunkten und Mountfehler die Folge sein. (Weitere Informationen zu Konkurrenzsituationen bei Mountpunkten im Kontext von 3592-Laufwerken und -Datenträgern finden Sie in Einheitenklassen 3592 definieren.)</p> <p>Einschränkung: In der folgenden Liste sind Einschränkungen beschrieben, die für Datenträger gelten:</p> <ul style="list-style-type: none"> <li>• CHECKIN LIBVOL: Das Problem liegt in der Verwendung der Option CHECKLABEL=YES. Wenn der Kennsatz in einem Format der Generation 3 oder einem späteren Format geschrieben ist und Sie die Option CHECKLABEL=YES angeben, schlägt die Verwendung dieses Befehls für Laufwerke früherer Generationen fehl. Um dieses Problem zu verhindern, geben Sie CHECKLABEL=BARCODE an.</li> <li>• LABEL LIBVOL: Wenn der Server versucht, Laufwerke einer früheren Generation zum Lesen des Kennsatzes zu verwenden, der in einem Format der Generation 3 oder einem späteren Format geschrieben ist, schlägt der Befehl LABEL LIBVOL fehl, es sei denn, OVERWRITE=YES wird angegeben. Stellen Sie sicher, dass Datenträger, denen unter Angabe von OVERWRITE=YES ein Kennsatz zugeordnet wird, keine aktiven Daten enthalten.</li> <li>• CHECKOUT LIBVOL: Wenn IBM Spectrum Protect feststellt, dass der Kennsatz (CHECKLABEL=YES) in einem Format der Generation 3 oder einem Format einer späteren Generation geschrieben ist, und Leseoperationen durch Laufwerke früherer Generationen erfolgen, schlägt der Befehl fehl. Um dieses Problem zu verhindern, geben Sie CHECKLABEL=NO an.</li> </ul> |

**Zugehörige Verweise:**

- 🔗 [CHECKIN LIBVOLUME](#) (Speicherdatenträger in ein Speicherarchiv zurückstellen)
- 🔗 [CHECKOUT LIBVOLUME](#) (Speicherdatenträger aus einem Speicherarchiv entnehmen)
- 🔗 [LABEL LIBVOLUME](#) (Datenträger im Speicherarchiv einen Kennsatz zuordnen)
- 🔗 [UPDATE STGPOOL](#) (Speicherpool aktualisieren)

## Datenzugriffsgeschwindigkeiten für 3592-Datenträger steuern

Sie können die Speicherkapazität optimieren und Datenzugriffsgeschwindigkeiten verbessern, wenn Sie Datenträger erstellen. Indem Daten in Speicherpools mit Datenträgern partitioniert werden, können Sie die Skalierungskapazität in Prozent angeben, um maximale Speicherkapazität oder schnellen Zugriff auf den Datenträger bereitstellen zu können.

### Informationen zu diesem Vorgang

Um die Datenträgerkapazität zu reduzieren, geben Sie den Parameter SCALECAPACITY an, wenn Sie die Einheitenklasse mit dem Befehl DEFINE DEVCLASS definieren oder wenn Sie die Einheitenklasse mit dem Befehl UPDATE DEVCLASS aktualisieren.

Geben Sie einen Prozentwert von 20, 90 oder 100 an. Mit einem Wert von 20 Prozent wird die schnellste Zugriffszeit und mit einem Wert von 100 Prozent die größte Speicherkapazität zur Verfügung gestellt. Wird beispielsweise eine Skalierungskapazität von 20 für eine Einheitenklasse 3592 ohne Komprimierung angegeben, würde ein 3592-Datenträger in dieser Einheitenklasse 20 Prozent seiner vollen Kapazität von 300 GB, d. h. ungefähr 60 GB, speichern.

Die Skalierungskapazität hat nur Auswirkungen, wenn Daten zum ersten Mal auf einen Datenträger geschrieben werden. Aktualisierungen an der Einheitenklasse für die Skalierungskapazität haben erst Auswirkungen auf einen Datenträger, auf den bereits Daten geschrieben wurden, wenn der Datenträger in den Arbeitsstatus zurückversetzt wird.



#### Zugehörige Verweise:

➔ DEFINE DEVCLASS (Einheitenklasse definieren)

#### Zugehörige Informationen:

➔ UPDATE DEVCLASS (Einheitenklasse aktualisieren)

## Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen aktivieren und inaktivieren

---

Bei IBM Spectrum Protect können Sie die folgenden Typen von Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen verwenden: Anwendung, System und Speicherarchiv. Diese Verfahren werden über die Hardware definiert.

### Informationen zu diesem Vorgang

---

Der Parameter DRIVEENCRYPTION im Befehl DEFINE DEVCLASS gibt an, ob die Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen zulässig ist. Verwenden Sie diesen Parameter, um IBM Spectrum Protect-Kompatibilität mit Hardwareverschlüsselungseinstellungen für leere Datenträger sicherzustellen. Sie können diesen Parameter nicht für Speicherpooldatenträger verwenden, die voll sind oder gefüllt werden.

- Um das Anwendungsverfahren zu verwenden, bei dem IBM Spectrum Protect Verschlüsselungsschlüssel generiert und verwaltet, setzen Sie den Parameter DRIVEENCRYPTION auf ON. Damit wird die Verschlüsselung von Daten für leere Datenträger aktiviert. Wenn der Parameter auf ON gesetzt wird und die Hardware für ein anderes Verschlüsselungsverfahren konfiguriert ist, schlagen Sicherungsoperationen fehl.
- Um das Speicherarchiv- oder Systemverschlüsselungsverfahren zu verwenden, setzen Sie den Parameter auf ALLOW. Damit wird angegeben, dass IBM Spectrum Protect nicht der Schlüsselmanager für die Laufwerkverschlüsselung ist, der Hardware wird jedoch die Verschlüsselung der Daten des Datenträgers über eines der anderen Verfahren ermöglicht. Bei Angabe dieses Parameters werden Datenträger nicht automatisch verschlüsselt. Daten können nur verschlüsselt werden, wenn der Parameter ALLOW angegeben wird und die Hardware für die Verwendung eines dieser Verfahren konfiguriert wird.

Der Parameter DRIVEENCRYPTION ist optional. Gemäß dem Standardwert ist das Speicherarchiv- oder Systemverschlüsselungsverfahren zulässig.

### Vorgehensweise

---

Das folgende vereinfachte Beispiel zeigt, wie Daten für leere Datenträger in einem Speicherpool unter Verwendung von IBM Spectrum Protect als Schlüsselmanager verschlüsselt werden können:

1. Definieren Sie ein Speicherarchiv, indem Sie den Befehl DEFINE LIBRARY ausgeben. Geben Sie beispielsweise den folgenden Befehl aus:

```
define library 3584 libtype=SCSI
```

2. Definieren Sie eine Einheitenklasse mit dem Namen 3592\_ENCRYPT, indem Sie den Befehl DEFINE DEVCLASS unter Angabe des Werts ON für den DRIVEENCRYPTION Parameter ausgeben. Geben Sie beispielsweise den folgenden Befehl aus:

```
define devclass 3592_encrypt library=3584 devtype=3592 driveencryption=on
```

3. Definieren Sie einen Speicherpool. Geben Sie beispielsweise den folgenden Befehl aus:

```
define stgpool 3592_encrypt_pool 3592_encrypt
```

### Nächste Schritte

---

Um eines des Verschlüsselungsverfahrens für neue Datenträger zu inaktivieren, setzen Sie den Parameter DRIVEENCRYPTION auf OFF. Wenn die Hardware für die Verschlüsselung von Daten durch das Speicherarchiv- oder Systemverfahren konfiguriert ist und DRIVEENCRYPTION auf OFF gesetzt ist, schlagen Sicherungsoperationen fehl.

## Gemeinsame Speicherarchivnutzung konfigurieren

---

Mehrere IBM Spectrum Protect-Server können Speichereinheiten unter Verwendung eines Speicherbereichsnetzes (SAN) gemeinsam nutzen. Ein Server wird als Speicherarchivmanager konfiguriert, die anderen Server werden als Speicherarchivclients konfiguriert.

### Vorbereitende Schritte

---

Stellen Sie sicher, dass Ihre Systeme die Lizenzierungsanforderungen für die gemeinsame Speicherarchivnutzung erfüllen. Ein Nutzungsrecht für IBM Spectrum Protect for SAN ist für jeden IBM Spectrum Protect-Server erforderlich, der als Speicherarchivclient oder Speicherarchivmanager in einer SAN-Umgebung konfiguriert wird.

## Informationen zu diesem Vorgang

---

Bei der LAN-unabhängigen Datenversetzung können IBM Spectrum Protect-Clientsysteme direkt auf Speichereinheiten zugreifen, die für einen IBM Spectrum Protect-Server definiert sind. Speicheragenten werden auf den Clientsystemen zur Ausführung der Datenversetzung installiert und konfiguriert.

Um die gemeinsame Speicherarchivnutzung zu konfigurieren, müssen Sie einen einzelnen IBM Spectrum Protect-Server als den Speicherarchivmanager für die Konfiguration der gemeinsamen Speicherarchivnutzung definieren. Anschließend definieren Sie weitere IBM Spectrum Protect-Server als Speicherarchivclients, die mit dem Speicherarchivmanager kommunizieren und Speicherressourcen vom Speicherarchivmanager anfordern. Der Speicherarchivmanager-Server muss dieselbe Version oder eine höhere Version wie der Server oder die Server haben, die als Speicherarchivclients definiert sind.

## Vorgehensweise

---

Um Speicherarchivressourcen in einem SAN zwischen mehreren IBM Spectrum Protect-Servern gemeinsam nutzen zu können, führen Sie die folgenden Schritte aus:

1. Konfigurieren Sie die Kommunikation zwischen Servern.

Um eine Speichereinheit in einem SAN gemeinsam nutzen zu können, definieren Sie Server mithilfe der Überkreuzdefinitionsfunktion füreinander. Jeder Server muss einen eindeutigen Namen haben.

2. Definieren Sie ein gemeinsam genutztes Speicherarchiv und konfigurieren Sie Bandeinheiten auf den Serversystemen.

Verwenden Sie die in Speicherarchive für die Verwendung durch einen Server konfigurieren beschriebene Prozedur zum Definieren eines Speicherarchivs für die Verwendung in einer Umgebung mit gemeinsamer Nutzung. Ändern Sie die Prozedur, um das Speicherarchiv als gemeinsam genutzt zu definieren, indem Sie den Parameter SHARED=YES für den Befehl DEFINE LIBRARY angeben.

3. Definieren Sie den Speicherarchivmanager-Server.
4. Definieren Sie das gemeinsam genutzte Speicherarchiv auf dem Server, der der Speicherarchivclient ist.
5. Definieren Sie auf dem Speicherarchivmanager-Server Pfade vom Speicherarchivclient zu jedem Laufwerk, auf das der Speicherarchivclient zugreifen kann. Der Einheitenname muss die Art und Weise widerspiegeln, auf die das Speicherarchivclientsystem die Bandeinheit erkennt. Vom Speicherarchivmanager muss ein Pfad zu jedem Laufwerk definiert werden, damit der Speicherarchivclient das Laufwerk verwenden kann.



Um Probleme zu verhindern, stellen Sie sicher, dass alle Laufwerkpfaddefinitionen, die für den Speicherarchivmanager definiert werden, auch für jeden Speicherarchivclient definiert werden.

Wenn beispielsweise der Speicherarchivmanager drei Bandlaufwerke definiert, muss auch der Speicherarchivclient drei Bandlaufwerke definieren. Um die Anzahl Bandlaufwerke, die ein Speicherarchivclient gleichzeitig nutzen kann, zu begrenzen, verwenden Sie den Parameter MOUNTLIMIT der Einheitenklasse auf dem Speicherarchivclient.

6. Definieren Sie Einheitenklassen für das gemeinsam genutzte Speicherarchiv.

Die bevorzugte Methode ist, auf beiden Servern identische Einheitenklassennamen zu verwenden, um Unklarheiten zu vermeiden, wenn mehrere Einheitenklassen mit demselben Einheitentyp und denselben Speicherarchivparametern definiert werden. Bei einigen Operationen, wie beispielsweise der Datenbanksicherung, wird der Einheitenklassenname zur Identifikation der Daten für die Sicherung verwendet.

Die Einheitenklassenparameter, die auf dem Speicherarchivmanager angegeben sind, überschreiben die für den Speicherarchivclient angegebenen Parameter. Wenn die Einheitenklassennamen unterschiedlich sind, verwendet der Speicherarchivmanager die Parameter, die in einer Einheitenklasse angegeben sind, die mit dem für den Speicherarchivclient angegebenen Einheitentyp übereinstimmt.


7. Definieren Sie einen Speicherpool für das gemeinsam genutzte Speicherarchiv.
  8. Wiederholen Sie die Schritte, um einen anderen Server als Speicherarchivclient zu konfigurieren.
-   Beispiel: Gemeinsame Speicherarchivnutzung für AIX- und Linux-Server  
Die Beispielprozedur zeigt, wie eine Umgebung mit gemeinsamer Speicherarchivnutzung für SCSI-Speicherarchive für Server, die auf AIX- oder Linux-Systemen ausgeführt werden, konfiguriert werden kann.
  - Beispiel: Gemeinsame Speicherarchivnutzung für Windows-Server  
Die Beispielprozedur zeigt, wie eine Umgebung mit gemeinsamer Speicherarchivnutzung für Server, die auf Windows-Systemen ausgeführt werden, konfiguriert werden kann.

### Zugehörige Verweise:

 DEFINE DEVCLASS (Einheitenklasse definieren)

### Zugehörige Informationen:

 DEFINE LIBRARY (Speicherarchiv definieren)

 DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

 AIX-Betriebssysteme  Linux-Betriebssysteme

## Beispiel: Gemeinsame Speicherarchivnutzung für AIX- und Linux-Server

Die Beispielprozedur zeigt, wie eine Umgebung mit gemeinsamer Speicherarchivnutzung für SCSI-Speicherarchive für Server, die auf AIX- oder Linux-Systemen ausgeführt werden, konfiguriert werden kann.

### Informationen zu diesem Vorgang

In diesem Beispiel werden ein Speicherarchivmanager-Server mit dem Namen ASTRO und ein Speicherarchivclient mit dem Namen JUDY konfiguriert. Um zu verdeutlichen, auf welchem Server der Schritt jeweils ausgeführt wird, steht vor dem jeweiligen Befehl der Name des Servers, auf dem der Befehl ausgegeben wird. Der größte Teil der Befehle wird auf dem Speicherarchivclient ausgegeben.

Definieren Sie für SCSI-Speicherarchive das Speicherarchiv unter Angabe des Parameters `libtype=scsi`.

### Vorgehensweise

1. Um ASTRO als den Speicherarchivmanager-Server zu konfigurieren, definieren Sie ein gemeinsam genutztes SCSI-Speicherarchiv mit dem Namen SANGROUP. Beispiel:

```
astro> define library sangroup libtype=scsi shared=yes
```

Führen Sie dann die übrigen Schritte zum Konfigurieren des Speicherarchivs wie in Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit einem einzigen Laufwerkeinheitentyp konfigurieren beschrieben aus.

Tipp: Mithilfe des Befehls `PERFORM LIBACTION` können Sie Laufwerke und Pfade für ein Speicherarchiv in einem einzigen Schritt definieren.

2. Definieren Sie ASTRO als den Speicherarchivmanager-Server, indem Sie den Befehl `DEFINE SERVER` ausgeben.


```
judy> define server astro serverpassword=secret hladdress=192.0.2.24  
lladdress=1777 crossdefine=yes
```

3. Definieren Sie das gemeinsam genutzte Speicherarchiv SANGROUP, indem Sie den Befehl `DEFINE LIBRARY` ausgeben. Sie müssen den im Parameter `PRIMARYLIBMANAGER` angegebenen Namen des Speicherarchivmanager-Servers und `LIBTYPE=SHARED` verwenden.

```
judy> define library sangroup libtype=shared primarylibmanager=astro
```

Stellen Sie sicher, dass der Speicherarchivname mit dem Speicherarchivnamen auf dem Speicherarchivmanager übereinstimmt.


4. Definieren Sie Pfade vom Speicherarchivmanager ASTRO zu zwei Laufwerken in dem gemeinsam genutzten Speicherarchiv, indem Sie den Befehl `DEFINE PATH` ausgeben.

 AIX-Betriebssysteme

```
astro> define path judy drivea srctype=server desttype=drive  
library=sangroup device=/dev/rmt6  
astro> define path judy driveb srctype=server desttype=drive  
library=sangroup device=/dev/rmt7
```

 Linux-Betriebssysteme

```
astro> define path judy drivea srctype=server desttype=drive  
library=sangroup device=/dev/IBMtape6  
astro> define path judy driveb srctype=server desttype=drive  
library=sangroup device=/dev/IBMtape7
```

5. Definieren Sie alle Einheitenklassen, die dem gemeinsam genutzten Speicherarchiv zugeordnet sind.  AIX-Betriebssysteme

```
judy> define devclass tape library=sangroup devtype=lto
```

 Linux-Betriebssysteme

```
judy> define devclass tape library=sangroup devtype=lto
```

Die folgenden Parameter für die Einheitenklassendefinition müssen auf dem Speicherarchivclient und dem Speicherarchivmanager übereinstimmen:

- o LIBRARY


- o DRIVEENCRYPTION
  - o WORM
  - o FORMAT
6. Definieren Sie einen Speicherpool mit dem Namen BACKTAPE für die Verwendung durch das gemeinsam genutzte Speicherarchiv. Geben Sie den Befehl DEFINE STGPOOL aus.

```
judy> define stgpool backtape tape maxscratch=50
```


## Nächste Schritte

Wiederholen Sie die Prozedur, um weitere Speicherarchivclients für Ihren Speicherarchivmanager zu definieren.


### Zugehörige Verweise:


 DEFINE DEVCLASS (Einheitenklasse definieren)

### Zugehörige Informationen:

 DEFINE DRIVE (Laufwerk für ein Speicherarchiv definieren)

 DEFINE LIBRARY (Speicherarchiv definieren)

 DEFINE PATH (Pfad definieren)

 DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

 Windows-Betriebssysteme



## Beispiel: Gemeinsame Speicherarchivnutzung für Windows-Server

Die Beispielprozedur zeigt, wie eine Umgebung mit gemeinsamer Speicherarchivnutzung für Server, die auf Windows-Systemen ausgeführt werden, konfiguriert werden kann.

### Informationen zu diesem Vorgang

In diesem Beispiel werden ein Speicherarchivmanager-Server mit dem Namen ASTRO und ein Speicherarchivclient mit dem Namen JUDY konfiguriert.

Definieren Sie für SCSI-Speicherarchive das Speicherarchiv unter Angabe des Parameters libtype=scsi.

-  Windows-Betriebssysteme Speicherarchivmanager-Server konfigurieren  
Sie müssen den Speicherarchivmanager-Server konfigurieren, um die IBM Spectrum Protect-Server für die gemeinsame Nutzung von Einheiten, die über ein SAN verbunden sind, konfigurieren zu können.
-  Windows-Betriebssysteme Speicherarchivclient-Server konfigurieren  
Sie müssen einen oder mehrere Speicherarchivclient-Server konfigurieren, um die IBM Spectrum Protect-Server für die gemeinsame Nutzung von Einheiten, die über ein SAN verbunden sind, konfigurieren zu können.

 Windows-Betriebssysteme

## Speicherarchivmanager-Server konfigurieren

Sie müssen den Speicherarchivmanager-Server konfigurieren, um die IBM Spectrum Protect-Server für die gemeinsame Nutzung von Einheiten, die über ein SAN verbunden sind, konfigurieren zu können.

### Vorgehensweise

Die folgende Beispielprozedur zeigt, wie ein IBM Spectrum Protect-Server mit dem Namen ASTRO als Speicherarchivmanager konfiguriert wird:

1. Stellen Sie sicher, dass der Speicherarchivmanager-Server aktiv ist:
  - a. Starten Sie die Windows-Dienstverwaltungskonsole (services.msc).
  - b. Wählen Sie den Dienst aus, beispielsweise TSM Server1.
  - c. Wenn der Dienst nicht aktiv ist, klicken Sie mit der rechten Maustaste auf den Namen des Dienstes und wählen Sie Starten aus.
2. Rufen Sie die Speicherarchiv- und Laufwerkdaten für die gemeinsam genutzte Speicherarchivseinheit ab:
  - a. Führen Sie das Dienstprogramm `tsmdlst.exe` aus. Das Dienstprogramm befindet sich im Verzeichnis `\Programme\Tivoli\TSM\server`.
3. Definieren Sie ein Speicherarchiv mit dem Speicherarchivtyp SCSI. Beispiel:

```
define library sangroup libtype=scsi shared=yes
```

In diesem Beispiel wird die Standardeinstellung für die Seriennummer des Speicherarchivs verwendet, gemäß der der Server die Seriennummer vom Speicherarchiv selbst abrufen, wenn der Pfad definiert wird. Abhängig vom Leistungsspektrum des Speicherarchivs kann der Server die Seriennummer möglicherweise nicht automatisch erkennen. In diesem Fall zeichnet der Server keine Seriennummer für die Einheit auf und kann die Identität der Einheit nicht bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet.

4. Definieren Sie den Pfad vom Server zum Speicherarchiv.

```
define path astro sangroup srctype=server desttype=library
device=lb0.0.0.2
```

Wenn die Seriennummer beim Definieren des Speicherarchivs nicht eingeschlossen wurde, fragt der Server das Speicherarchiv jetzt ab, um diese Informationen abzurufen. Wenn die Seriennummer beim Definieren des Speicherarchivs eingeschlossen wurde, überprüft der Server die Definition und gibt eine Nachricht aus, wenn eine Übereinstimmung vorliegt.

5. Definieren Sie die Laufwerke im Speicherarchiv.

```
define drive sangroup drivea
define drive sangroup driveb
```

In diesem Beispiel wird die Standardeinstellung für die Seriennummer des Laufwerks verwendet, gemäß der der Server die Seriennummer vom Laufwerk selbst abrufen, wenn der Pfad definiert wird. Abhängig vom Leistungsspektrum des Laufwerks kann der Server die Seriennummer möglicherweise nicht automatisch erkennen. In diesem Fall zeichnet der Server keine Seriennummer für die Einheit auf und kann die Identität der Einheit nicht bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet.

In diesem Beispiel wird auch die Standardeinstellung für die Elementadresse des Laufwerks verwendet, gemäß der der Server die Elementnummer vom Laufwerk selbst abrufen, wenn der Pfad definiert wird.

Die Elementadresse ist eine Zahl, die die physische Position eines Laufwerks in einem automatisierten Speicherarchiv angibt. Der Server benötigt die Elementadresse, um die physische Position des Laufwerks mit der SCSI-Adresse des Laufwerks zu verbinden. Der Server kann die Elementnummer vom Laufwerk selbst abrufen, wenn der Pfad definiert wird, oder Sie können die Elementnummer angeben, wenn Sie das Laufwerk definieren.

Abhängig vom Leistungsspektrum des Speicherarchivs kann der Server die Elementadresse möglicherweise nicht automatisch erkennen. In diesem Fall müssen Sie die Elementadresse angeben, wenn Sie das Laufwerk definieren. Elementnummern für viele Speicherarchive sind unter IBM® Support Portal for IBM Spectrum Protect verfügbar.

6. Definieren Sie den Pfad vom Server zu jedem der Laufwerke.

```
define path astro drivea srctype=server desttype=drive library=sangroup
device=mt0.1.0.2
define path astro driveb srctype=server desttype=drive library=sangroup
device=mt0.2.0.2
```

Wenn die Seriennummer oder Elementadresse beim Definieren des Laufwerks nicht eingeschlossen wurde, fragt der Server das Laufwerk oder Speicherarchiv jetzt ab, um diese Informationen abzurufen.

7. Definieren Sie mindestens eine Einheitenklasse.

```
define devclass tape devtype=dlt library=sangroup
```

8. Stellen Sie den Speicherarchivbestand zurück. Bei dem folgenden Beispiel werden alle Datenträger als Arbeitsdatenträger in den Speicherarchivbestand zurückgestellt. Der Server verwendet den Namen auf dem Barcodeetikett als den Datenträgernamen.

```
checkin libvolume sangroup search=yes status=scratch
checklabel=barcode
```

9. Konfigurieren Sie einen Speicherpool mit maximal 50 Arbeitsdatenträgern für das gemeinsam genutzte Speicherarchiv.

```
define stgpool backtape tape
description='Speicherpool für gemeinsam genutztes Speicherarchiv sangroup' maxscratch=50
```

#### Zugehörige Verweise:

- [CHECKIN LIBVOLUME](#) (Speicherdatenträger in ein Speicherarchiv zurückstellen)
- [DEFINE DEVCLASS](#) (Einheitenklasse definieren)

#### Zugehörige Informationen:

- [DEFINE DRIVE](#) (Laufwerk für ein Speicherarchiv definieren)
- [DEFINE LIBRARY](#) (Speicherarchiv definieren)
- [DEFINE PATH](#) (Pfad definieren)
- [DEFINE STGPOOL](#) (Datenträger in einem Speicherpool definieren)

## Speicherarchivclient-Server konfigurieren

---

Sie müssen einen oder mehrere Speicherarchivclient-Server konfigurieren, um die IBM Spectrum Protect-Server für die gemeinsame Nutzung von Einheiten, die über ein SAN verbunden sind, konfigurieren zu können.

### Vorbereitende Schritte

---

Stellen Sie sicher, dass ein Speicherarchivmanager-Server definiert ist.

### Informationen zu diesem Vorgang

---

Sie müssen den Speicherarchivmanager-Server definieren. Die folgende Beispielprozedur zeigt, wie ein IBM Spectrum Protect-Server mit dem Namen JUDY als Speicherarchivclient konfiguriert wird.

### Vorgehensweise

---

1. Stellen Sie sicher, dass der Speicherarchivmanager-Server aktiv ist:
  - a. Starten Sie die Windows-Dienstverwaltungskonsolle (services.msc).
  - b. Wählen Sie den Dienst aus, beispielsweise TSM Server1.
  - c. Wenn der Dienst nicht aktiv ist, klicken Sie mit der rechten Maustaste und wählen Sie Starten aus.
2. Rufen Sie die Speicherarchiv- und Laufwerkdaten für die gemeinsam genutzte Speicherarchivseinheit ab:
  - a. Führen Sie das Dienstprogramm `tsmdlst.exe` aus. Das Dienstprogramm befindet sich im Verzeichnis `\Programme\Tivoli\TSM\server`.
3. Definieren Sie das gemeinsam genutzte Speicherarchiv SANGROUP und geben Sie den Speicherarchivmanager an. Stellen Sie sicher, dass der Speicherarchivname mit dem Speicherarchivnamen auf dem Speicherarchivmanager übereinstimmt.

```
define library sangroup libtype=shared primarylibmanager=astro
```

4. Definieren Sie die Pfade vom Speicherarchivclient-Server zu jedem der Laufwerke, indem Sie Befehle auf dem Verwaltungsclient ausgeben:

```
define path judy drivea srctype=server desttype=drive library=sangroup  
device=mt0.1.0.3  
define path judy driveb srctype=server desttype=drive library=sangroup  
device=mt0.2.0.3
```

5. Definieren Sie mindestens eine Einheitenklasse, indem Sie Befehle auf dem Speicherarchivclient ausgeben:

```
define devclass tape devtype=dlt mountretention=1 mountwait=10  
library=sangroup
```

Definieren Sie die Parameter für die Einheitenklasse auf dem Speicherarchivclient mit denselben Werten wie auf dem Speicherarchivmanager. Es ist zwar sinnvoll, auf beiden Servern identische Einheitenklassennamen zu verwenden, dies ist jedoch nicht erforderlich.

Die Einheitenklassenparameter, die auf dem Speicherarchivmanager-Server angegeben sind, überschreiben die für den Speicherarchivclient angegebenen Parameter. Dies gilt unabhängig davon, ob die Einheitenklassennamen auf beiden Servern identisch sind. Wenn die Einheitenklassennamen unterschiedlich sind, verwendet der Speicherarchivmanager die Parameter, die in einer Einheitenklasse angegeben sind, die mit dem für den Speicherarchivclient angegebenen Einheitentyp übereinstimmt.

Wenn ein Speicherarchivclient eine andere Einstellung als die in der Einheitenklasse des Speicherarchivmanagers angegebene Einstellung (beispielsweise ein anderes Mountlimit) erfordert, führen Sie die folgenden Schritte aus:

- a. Erstellen Sie auf dem Speicherarchivmanager-Server eine zusätzliche Einheitenklasse. Geben Sie die Parametereinstellungen an, die der Speicherarchivclient verwenden soll.
  - b. Erstellen Sie auf dem Speicherarchivclient eine Einheitenklasse mit demselben Namen und Einheitentyp wie die neue Einheitenklasse, die Sie auf dem Speicherarchivserver erstellt haben.
6. Definieren Sie den Speicherpool BACKTAPE, der das gemeinsam genutzte Speicherarchiv verwenden wird:

```
define stgpool backtape tape  
description='Speicherpool für gemeinsam genutztes Speicherarchiv sangroup' maxscratch=50
```

7. Wiederholen Sie diese Prozedur, um weitere Server als Speicherarchivclients zu definieren.

#### Zugehörige Verweise:

[DEFINE DEVCLASS \(Einheitenklasse definieren\)](#)

#### Zugehörige Informationen:

- ➔ DEFINE LIBRARY (Speicherarchiv definieren)
- ➔ DEFINE PATH (Pfad definieren)
- ➔ DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

## Speicherpoolhierarchie konfigurieren

---

Im Rahmen des Implementierungsprozesses müssen Sie eine Speicherpoolhierarchie konfigurieren. Konfigurieren Sie mindestens einen primären Speicherpool auf Platte und einen primären Speicherpool auf Band. Stellen Sie sicher, dass Daten täglich von Platte auf Band umgelagert werden.

### Vorbereitende Schritte

---

1. Stellen Sie sicher, dass Sie die Informationen in Planung der Speicherpoolhierarchie gelesen haben.
2. Stellen Sie sicher, dass die entsprechenden Regeln, die auch als *Maßnahmen* bezeichnet werden, zum Sichern von Clientdaten angegeben sind. Führen Sie die Anweisungen in Regeln zum Sichern und Archivieren von Clientdaten angeben aus.
3. Stellen Sie sicher, dass jedem Knoten eine Maßnahme zugeordnet ist. Anweisungen zum Zuordnen einer Maßnahme beim Registrieren eines Knotens finden Sie in Clients registrieren.

### Vorgehensweise

---

Um eine Speicherpoolhierarchie zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Definieren Sie einen primären Speicherpool für die Bandeinheit, indem Sie den Befehl DEFINE STGPOOL ausgeben.

Definieren Sie beispielsweise einen primären Speicherpool mit dem Namen TAPE1 mit der Einheitenklasse LTO und aktivieren Sie die Gruppenkollokation. Legen Sie die maximale Anzahl Arbeitsdatenträger, die der Server für diesen Speicherpool anfordern kann, mit 999 fest. Geben Sie den folgenden Befehl aus:

```
define stgpool tape1 lto pooltype=primary collocate=group  
maxscratch=999
```

2. Definieren Sie die Laufwerke, Pfade, und Speicherarchive für den primären Speicherpool auf Band. Führen Sie die Anweisungen in Bandeinheiten definieren aus.
3. Definieren Sie einen primären Speicherpool für die Platteneinheit, indem Sie den Befehl DEFINE STGPOOL ausgeben.

Definieren Sie beispielsweise einen Speicherpool mit dem Namen DISK1 mit der Einheitenklasse FILE. Stellen Sie sicher, dass Daten in den Bandspeicherpool TAPE1 umgelagert werden können, verhindern Sie jedoch die automatische Umlagerung, indem Sie 100 für den Parameter HIGHMIG und 0 für den Parameter LOWMIG angeben. Verhindern Sie die Konsolidierung, indem Sie 100 für den Parameter RECLAIM angeben. Aktivieren Sie die Knotenkollokation. Legen Sie die maximale Anzahl Arbeitsdatenträger, die der Server für diesen Speicherpool anfordern kann, mit 9999 fest. Geben Sie mithilfe des Parameters MIGPROCESS die Anzahl Umlagerungsprozesse an. Der Wert des Parameters MIGPROCESS sollte der Anzahl Laufwerke in dem Speicherarchiv minus der Anzahl Laufwerke, die für Zurückschreibungsoperationen reserviert sind, entsprechen. Geben Sie den folgenden Befehl aus:

```
define stgpool disk1 file pooltype=primary nextstgpool=tape1  
highmig=100 lowmig=0 reclaim=100 collocate=node maxscratch=9999 migprocess=5
```

Weitere Informationen zum Konfigurieren der Umlagerung von Platte auf Band finden Sie in Plattenspeicherpools umlagern.

### Nächste Schritte

---

Eine Speicherpoolhierarchie umfasst nur primäre Speicherpools. Nachdem Sie die Speicherpoolhierarchie konfiguriert haben, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen Kopierspeicherpool auf einer Bandeinheit. Anweisungen finden Sie in DEFINE STGPOOL (Kopierspeicherpool definieren, der Einheiten mit sequenziellem Zugriff zugeordnet ist).
2. Sichern Sie den bandbasierten primären Speicherpool im Kopierspeicherpool mithilfe des Befehls BACKUP STGPOOL. Anweisungen finden Sie in BACKUP STGPOOL (Daten in primären Speicherpools in einem Kopierspeicherpool sichern).
3. Um sicherzustellen, dass Daten in einem Katastrophenfall wiederhergestellt werden können, definieren Sie eine Prozedur zum Versetzen von Banddatenträgern aus dem Kopierspeicherpool an einen anderen Standort. Anweisungen finden Sie in Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM.

#### Zugehörige Verweise:

- ➔ CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

#### Zugehörige Informationen:

## Anwendungen und Systeme schützen

---

Der Server schützt Daten für Clients, die Anwendungen, virtuelle Maschinen und Systeme umfassen können.

- Clients hinzufügen  
Installieren und konfigurieren Sie im Anschluss an die erfolgreiche Konfiguration Ihres IBM Spectrum Protect-Servers die Client-Software, um mit dem Sichern von Daten beginnen zu können.

## LAN-unabhängige Datenversetzung konfigurieren

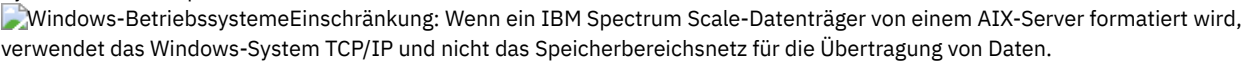
---

Sie können den IBM Spectrum Protect-Client und -Server so konfigurieren, dass der Client seine Daten über einen Speicheragenten direkt in Speicher in einem SAN versetzen kann. Diese Funktion, die als LAN-unabhängige Datenversetzung bezeichnet wird, wird vom Produkt IBM Spectrum Protect for SAN bereitgestellt.

### Vorgehensweise

---

Um die LAN-unabhängige Datenversetzung zu konfigurieren, führen Sie die folgenden Schritte aus. Ausführliche Informationen finden Sie in der Dokumentation für IBM Spectrum Protect for SAN.

1. Überprüfen Sie die Netzverbindung.
2. Richten Sie die Kommunikation zwischen dem Client, dem Speicheragenten und dem Server ein.
3. Installieren und konfigurieren Sie die Software auf Clientsystemen.
4. Konfigurieren Sie Einheiten auf dem Server für den Zugriff durch den Speicheragenten.
5. Konfigurieren Sie IBM Spectrum Protect-Maßnahmen für die LAN-unabhängige Datenversetzung für den Client.
6. Wenn Sie gemeinsam genutzten Speicher des Typs FILE verwenden, installieren und konfigurieren Sie IBM® TotalStorage SAN File System oder IBM Spectrum Scale.  

7. Definieren Sie Pfade vom Speicheragenten zu Laufwerken.
8. Starten Sie den Speicheragenten und überprüfen Sie die LAN-unabhängige Konfiguration.

### Nächste Schritte

---

Zur Optimierung Ihrer LAN- und SAN-Ressourcennutzung können Sie den Pfad steuern, über den Datenübertragungen für Clients mit der Fähigkeit zur LAN-unabhängigen Datenversetzung erfolgen. Steuern Sie den Pfad mithilfe des Befehls UPDATE NODE. Für jeden Client können Sie für Lese- und Schreiboperationen für Daten eine der folgenden Einstellungen auswählen. Geben Sie Operationen zum Lesen von Daten mit dem Parameter DATAREADPATH und Operationen zum Schreiben von Daten mit dem Parameter DATAWRITEPATH an. Der Parameter ist optional. Der Standardwert ist ANY.

LAN (nur LAN-Pfad)

Geben Sie den Wert LAN an, wenn eine der folgenden Bedingungen erfüllt ist:

- Es soll ein kleines Datenvolumen gesichert oder zurückgeschrieben werden.
- Der Client verfügt nicht über SAN-Konnektivität.

LANFREE (nur LAN-unabhängiger Pfad)

Geben Sie den Wert LANFREE an, wenn sich der Client und der Server in demselben SAN befinden und eine der folgenden Bedingungen erfüllt ist

- Es soll ein großes Datenvolumen gesichert oder zurückgeschrieben werden.
- Die Serververarbeitungslast soll auf den Client verlagert werden.
- Das LAN soll entlastet werden.

ANY (jeder beliebige verfügbare Pfad)

Ein LAN-unabhängiger Pfad wird verwendet, sofern ein derartiger Pfad verfügbar ist. Wenn kein LAN-unabhängiger Pfad verfügbar ist, werden die Daten über das LAN übertragen.

- LAN-unabhängige Konfiguration prüfen  
Nach der Konfiguration eines IBM Spectrum Protect-Clients für die LAN-unabhängige Datenversetzung können Sie die Konfiguration und die Serverdefinitionen mithilfe des Befehls VALIDATE LANFREE prüfen.

## Verschlüsselungsverfahren für Bänder

---



Die Entscheidung über das zu verwendende Verschlüsselungsverfahren ist davon abhängig, wie Ihre Daten verwaltet werden sollen.

Es ist wichtig, Clientdaten zu schützen, insbesondere dann, wenn diese Daten sensibel sind. Mithilfe von IBM Bandverschlüsselungstechnologie kann sichergestellt werden, dass Daten auf Datenträgern vor Ort und an einem anderen Standort geschützt sind.

IBM Bandtechnologie unterstützt verschiedene Verfahren der Laufwerkverschlüsselung für die folgenden Einheiten:

- IBM 3592 Generation 2 und Generation 3
- IBM Linear Tape-Open (LTO) Generation 4 und Generation 5

Die Verfahren der Laufwerkverschlüsselung, die Sie mit IBM Spectrum Protect verwenden können, werden auf der Hardwareebene konfiguriert. IBM Spectrum Protect kann nicht steuern oder ändern, welches Verschlüsselungsverfahren in der Hardwarekonfiguration verwendet wird. Wenn die Hardware für das Anwendungsverfahren konfiguriert ist, kann IBM Spectrum Protect die Verschlüsselung abhängig vom Wert für DRIVEENCRYPTION für die Einheitenklasse aktivieren oder inaktivieren.

Um alle Daten in einem bestimmten logischen Speicherarchiv zu verschlüsseln oder Daten auf mehr als nur Speicherpooldatenträgern zu verschlüsseln, verwenden Sie die das Speicherarchiv- oder Systemverfahren. Wenn der Verschlüsselungsschlüsselmanager für die gemeinsame Nutzung von Schlüsseln konfiguriert ist, können die Speicherarchiv- und Systemverfahren den Verschlüsselungsschlüssel gemeinsam nutzen, was den gegenseitigen Austausch der beiden Verfahren ermöglicht. IBM Spectrum Protect kann Verschlüsselungsschlüssel zwischen dem Anwendungsverfahren und dem Speicherarchiv- oder dem Systemverschlüsselungsverfahren nicht gemeinsam nutzen oder verwenden.

Tabelle 1. Verschlüsselungsverfahren

| Verschlüsselungsverfahren | Beschreibung  |
|---------------------------|---|
| Anwendungsverschlüsselung | <p>Bei der anwendungsverwalteten Verschlüsselung, können Sie dedizierte Speicherpools erstellen, die nur verschlüsselte Datenträger enthalten. Auf diese Weise können Sie Speicherpoolhierarchien und Maßnahmen verwenden, um zu steuern, wie die Daten verschlüsselt werden.</p> <p>Verschlüsselungsschlüssel werden von der Anwendung verwaltet, in diesem Fall von IBM Spectrum Protect. IBM Spectrum Protect generiert und speichert die Schlüssel in der Serverdatenbank. Daten werden während der Ausführung von Schreiboperationen verschlüsselt, wenn der Verschlüsselungsschlüssel vom Server an das Laufwerk übergeben wird. Daten werden für Leseoperation entschlüsselt.</p> <p>Um Speicherpooldatenträger zu verschlüsseln und einen Teil der Verschlüsselungsverarbeitung auf Ihrem System zu eliminieren, aktivieren Sie das Anwendungsverfahren. Verwenden Sie die anwendungsverwaltete Verschlüsselung nur für Speicherpooldatenträger. Andere Datenträger, wie beispielsweise Bänder mit Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger, werden nicht mithilfe des Anwendungsverfahrens verschlüsselt.</p> <p>Voraussetzung: Wenn die Anwendungsverschlüsselung aktiviert ist, müssen Sie beim Schützen von Datenbanksicherungen besonders vorsichtig vorgehen, da die Verschlüsselungsschlüssel zum Verschlüsseln und Entschlüsseln von Daten in der Serverdatenbank gespeichert sind. Um Ihre Daten zurückschreiben zu können, müssen Sie über die korrekte Datenbanksicherung und die zugehörigen Verschlüsselungsschlüssel verfügen, um auf Ihre Informationen zugreifen zu können. Stellen Sie sicher, dass die Datenbank häufig gesichert wird, und schützen Sie die Sicherungen, um Datenverlust oder Diebstahl zu verhindern. Jeder, der sowohl Zugriff auf die Datenbanksicherung als auch auf die Verschlüsselungsschlüssel hat, hat Zugriff auf Ihre Daten.</p> |

| Verschlüsselungsverfahren     | Beschreibung   |
|-------------------------------|--|
| Speicherarchivverschlüsselung | <p>Bei der speicherarchivverwalteten Verschlüsselung können Sie steuern, welche Datenträger unter Verwendung ihrer Seriennummern verschlüsselt werden. Sie können einen Bereich oder eine Gruppe von Datenträgern angeben, die verschlüsselt werden sollen.</p> <p>Verschlüsselungsschlüssel werden vom Speicherarchiv verwaltet. Schlüssel sind in einem Verschlüsselungsschlüsselmanager gespeichert und werden dem Laufwerk zur Verfügung gestellt. Wenn Sie die Hardware für die Verwendung der speicherarchivverwalteten Verschlüsselung konfigurieren, können Sie dieses Verfahren verwenden, indem Sie den Befehl DEFINE DEVCLASS unter Angabe des Parameters DRIVEENCRYPTION=ALLOW ausgeben.</p> <p>Einschränkung: Die Verschlüsselung mit IBM LTO-4 und späteren Generationen wird nur von bestimmten IBM Speicherarchiven unterstützt. Ausführliche Informationen finden Sie in Bandlaufwerkverschlüsselung konfigurieren.</p> |
| Systemverschlüsselung         | <p>Die systemverwaltete Verschlüsselung ist nur unter dem Betriebssystem AIX® verfügbar. Verschlüsselungsschlüssel, die dem Laufwerk zur Verfügung gestellt werden, werden vom Einheitsreiber oder Betriebssystem verwaltet und in einem Verschlüsselungsschlüsselmanager gespeichert. Wenn die Hardware für die Verwendung der Systemverschlüsselung konfiguriert ist, können Sie dieses Verfahren verwenden, indem Sie den Befehl DEFINE DEVCLASS unter Angabe des Parameters DRIVEENCRYPTION=ALLOW ausgeben.</p>  |



Um festzustellen, ob ein Datenträger verschlüsselt ist und welches Verfahren verwendet wurde, geben Sie den Befehl QUERY VOLUME unter Angabe des Parameters FORMAT=DETAILED aus.

- Bandlaufwerkverschlüsselung konfigurieren  
Mithilfe der Laufwerkverschlüsselung können Sie Bänder schützen, die kritische oder sensible Daten enthalten, wie beispielsweise Bänder mit vertraulichen Finanzdaten. Die Laufwerkverschlüsselung kann hilfreich sein, wenn Sie Bänder aus der IBM Spectrum Protect-Serverumgebung an einen Standort vor Ort oder an einen anderen Standort versetzen.

## Bandspeicheroperationen steuern

Einheitenklassendefinitionen für Bänder umfassen Parameter, die Ihnen die Steuerung von Speicheroperationen ermöglichen.

- Wie Datenträger von IBM Spectrum Protect gefüllt werden  
Der Befehl DEFINE DEVCLASS hat einen optionalen Parameter ESTCAPACITY, der die geschätzte Kapazität sequenzieller Datenträger angibt, die der Einheitenklasse zugeordnet sind. IBM Spectrum Protect bestimmt mithilfe der geschätzten Kapazität von Datenträgern die geschätzte Kapazität eines Speicherpools sowie die geschätzte Auslastung in Prozent.
- Geschätzte Kapazität von Banddatenträgern angeben  
IBM Spectrum Protect bestimmt anhand der geschätzten Kapazität außerdem, wann die Konsolidierung von Speicherpooldatenträgern beginnen soll.
- Aufzeichnungsformate für Banddatenträger angeben  
Sie können das Aufzeichnungsformat angeben, das von IBM Spectrum Protect zum Schreiben von Daten auf Banddatenträger verwendet wird. Wenn Sie planen, Generationen von Laufwerken oder unterschiedliche Laufwerktypen in einem Speicherarchiv zu mischen, müssen Sie für jede Laufwerkgeneration und jeden Laufwerktyp ein Aufzeichnungsformat angeben. Auf diese Weise kann der Server zwischen den einzelnen Laufwerkgenerationen und Laufwerktypen unterscheiden.
- Speicherarchivobjekte Einheitenklassen zuordnen  
Ein Speicherarchiv enthält die Laufwerke, die zum Bereitstellen des Datenträgers verwendet werden können. Einer Einheitenklasse kann nur ein einziges Speicherarchiv zugeordnet werden. Mehrere Einheitenklassen können jedoch dasselbe Speicherarchiv referenzieren.
- Datenträgermountoperationen für Bänder steuern  
Mithilfe von Einheitenklassendefinitionen können Sie die Anzahl bereitgestellter Datenträger, die Zeit, die ein Datenträger bereitgestellt bleibt, und die Zeit, die der IBM Spectrum Protect-Server auf ein verfügbares Laufwerk wartet, steuern.

- Operationen zurückstellen  
Der Server kann Server- oder Clientoperationen für eine Operation mit höherer Priorität zurückstellen, wenn ein Mountpunkt im Gebrauch ist und keine anderen Mountpunkte verfügbar sind oder der Zugriff auf einen bestimmten Datenträger erforderlich ist. Wenn eine Operation zurückgestellt wird, wird sie abgebrochen.
- Auswirkungen von Einheitenänderungen im SAN  
Die SAN-Umgebung kann sich aufgrund von Änderungen an den Einheiten oder an der Verkabelung dramatisch ändern. Aufgrund der dynamischen Natur des SAN können statische Definitionen fehlschlagen oder unvorhersehbar werden.
-  Windows-Betriebssysteme Einheitsdaten anzeigen  
Mithilfe des Dienstprogramms für Einheitsdaten (tsmdlst) können Sie Informationen zu Einheiten anzeigen, die mit dem Server verbunden sind.
- WORM-Banddatenträger  
WORM-Datenträger können als Schutz vor dem versehentlichen oder absichtlichen Löschen kritischer Daten verwendet werden. In IBM Spectrum Protect gibt es jedoch bestimmte Einschränkungen und Richtlinien, die bei der Verwendung von WORM-Datenträgern zu beachten sind.
-  Windows-Betriebssysteme Einheitenfehler beheben  
Sie können Fehler beheben, die bei der Konfiguration oder Verwendung von Einheiten mit IBM Spectrum Protect auftreten.

## Wie Datenträger von IBM Spectrum Protect gefüllt werden

---

Der Befehl DEFINE DEVCLASS hat einen optionalen Parameter ESTCAPACITY, der die geschätzte Kapazität sequenzieller Datenträger angibt, die der Einheitenklasse zugeordnet sind. IBM Spectrum Protect bestimmt mithilfe der geschätzten Kapazität von Datenträgern die geschätzte Kapazität eines Speicherpools sowie die geschätzte Auslastung in Prozent.

Wenn der Parameter ESTCAPACITY nicht angegeben wird, verwendet IBM Spectrum Protect einen Standardwert, der auf dem Aufzeichnungsformat basiert, das für die Einheitenklasse unter Verwendung des Parameters FORMAT angegeben wird.

Wenn Sie eine geschätzte Kapazität angeben, die die tatsächliche Kapazität des Datenträgers in der Einheitenklasse überschreitet, aktualisiert IBM Spectrum Protect die geschätzte Kapazität des Datenträgers, wenn der Datenträger voll wird. Wenn IBM Spectrum Protect das Ende des Datenträgers erreicht, wird die Kapazität in Übereinstimmung mit dem Datenvolumen, das auf den Datenträger geschrieben wurde, aktualisiert.

Sie können den Standardwert für die geschätzte Kapazität für die Einheitenklasse akzeptieren oder explizit eine geschätzte Kapazität angeben. Ein genauer Wert für die geschätzte Kapazität ist nicht erforderlich, aber nützlich. IBM Spectrum Protect bestimmt mithilfe der geschätzten Kapazität von Datenträgern die geschätzte Kapazität eines Speicherpools sowie die geschätzte Auslastung in Prozent. Unter Umständen möchten Sie die geschätzte Kapazität ändern, wenn eine oder beide der folgenden Bedingungen erfüllt sind:

- Der Standardwert für die geschätzte Kapazität ist aufgrund der Datenkomprimierung ungenau.
- Es sind Datenträger vorhanden, deren Größe vom Standard abweicht.

### Zugehörige Verweise:

 DEFINE DEVCLASS (Einheitenklasse definieren)

### Zugehörige Informationen:

 UPDATE DEVCLASS (Einheitenklasse aktualisieren)

## Geschätzte Kapazität von Banddatenträgern angeben

---

IBM Spectrum Protect bestimmt anhand der geschätzten Kapazität außerdem, wann die Konsolidierung von Speicherpooldatenträgern beginnen soll.

### Informationen zu diesem Vorgang

---


Bei Bandeinheitenklassen sind die vom Server ausgewählten Standardwerte von dem Aufzeichnungsformat abhängig, mit dem Daten auf den Datenträger geschrieben werden. Sie können entweder den Standardwert für einen Einheitentyp akzeptieren oder einen Wert angeben.

Um die geschätzte Kapazität für Banddatenträger anzugeben, verwenden Sie den Parameter ESTCAPACITY, wenn Sie die Einheitenklasse definieren oder ihre Definition aktualisieren.

### Zugehörige Verweise:

 DEFINE DEVCLASS (Einheitenklasse definieren)

### Zugehörige Informationen:

 UPDATE DEVCLASS (Einheitenklasse aktualisieren)

## Aufzeichnungsformate für Banddatenträger angeben

---

Sie können das Aufzeichnungsformat angeben, das von IBM Spectrum Protect zum Schreiben von Daten auf Banddatenträger verwendet wird. Wenn Sie planen, Generationen von Laufwerken oder unterschiedliche Laufwerktypen in einem Speicherarchiv zu mischen, müssen Sie für jede Laufwerkgeneration und jeden Laufwerktyp ein Aufzeichnungsformat angeben. Auf diese Weise kann der Server zwischen den einzelnen Laufwerkgenerationen und Laufwerktypen unterscheiden.

## Informationen zu diesem Vorgang

---

Um ein Aufzeichnungsformat anzugeben, verwenden Sie den Parameter `FORMAT`, wenn Sie die Einheitenklasse definieren oder ihre Definition aktualisieren.

Wenn alle Laufwerke, die dieser Einheitenklasse zugeordnet sind, identisch sind, geben Sie `FORMAT=DRIVE` an. Der Server wählt das höchste Format aus, das von dem Laufwerk unterstützt wird, in dem ein Datenträger bereitgestellt wird.

Wenn einige der Laufwerke, die der Einheitenklasse zugeordnet sind, ein Format mit höherer Speicherdichte als andere unterstützen, geben Sie ein Format an, das mit allen Laufwerken kompatibel ist.

Wenn Laufwerke in einem einzelnen SCSI-Speicherarchiv verschiedene Bandtechnologien (beispielsweise DLT und LTO Ultrium) verwenden, geben Sie einen eindeutigen Wert für den Parameter `FORMAT` in jeder Einheitenklassendefinition an.

Ein Konfigurationsbeispiel befindet sich in Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit mehreren Laufwerkeinheitentypen konfigurieren.

Das Aufzeichnungsformat, das der Server für einen Datenträger verwendet, wird ausgewählt, wenn zum ersten Mal Daten auf den Datenträger geschrieben werden. Eine Aktualisierung des Parameters `FORMAT` wirkt sich auf Datenträger, die bereits Daten enthalten, erst dann aus, wenn diese Datenträger ab dem Anfang neu beschrieben werden. Dies kann nach dem Konsolidieren oder Löschen eines Datenträgers oder nach dem Verfall aller Daten auf dem Datenträger der Fall sein.

### Zugehörige Verweise:

➔ `DEFINE DEVCLASS` (Einheitenklasse definieren)

### Zugehörige Informationen:

➔ `UPDATE DEVCLASS` (Einheitenklasse aktualisieren)

## Speicherarchivobjekte Einheitenklassen zuordnen

---

Ein Speicherarchiv enthält die Laufwerke, die zum Bereitstellen des Datenträgers verwendet werden können. Einer Einheitenklasse kann nur ein einziges Speicherarchiv zugeordnet werden. Mehrere Einheitenklassen können jedoch dasselbe Speicherarchiv referenzieren.

## Informationen zu diesem Vorgang

---

Um eine Einheitenklasse einem Speicherarchiv zuzuordnen, verwenden Sie den Parameter `LIBRARY` wenn Sie eine Einheitenklasse definieren oder ihre Definition aktualisieren.

### Zugehörige Verweise:

➔ `DEFINE DEVCLASS` (Einheitenklasse definieren)

### Zugehörige Informationen:

➔ `UPDATE DEVCLASS` (Einheitenklasse aktualisieren)

## Datenträgermountoperationen für Bandeinheiten steuern

---

Mithilfe von Einheitenklassendefinitionen können Sie die Anzahl bereitgestellter Datenträger, die Zeit, die ein Datenträger bereitgestellt bleibt, und die Zeit, die der IBM Spectrum Protect-Server auf ein verfügbares Laufwerk wartet, steuern.

- Anzahl gleichzeitig bereitgestellter Datenträger steuern  
Wenn Sie ein Mountlimit für eine Einheitenklasse festlegen, müssen Sie die Anzahl Speichereinheiten berücksichtigen, die mit Ihrem System verbunden sind. Außerdem müssen Sie berücksichtigen, ob die Funktion für gleichzeitiges Schreiben verwendet wird und ob mehrere Einheitenklassen einem einzelnen Speicherarchiv zugeordnet werden; darüber hinaus müssen Sie die Anzahl Prozesse berücksichtigen, die gleichzeitig ausgeführt werden.
- Steuern, wie lange ein Datenträger bereitgestellt bleibt  
Sie können steuern, wie lange ein bereitgestellter Datenträger nach seiner letzten E/A-Aktivität bereitgestellt bleiben soll. Wenn ein Datenträger häufig verwendet wird, können Sie die Leistung verbessern, indem Sie einen längeren Mount-Aufbewahrungszeitraum definieren, um unnötige Operationen zum Bereitstellen und Aufheben der Bereitstellung zu vermeiden.
- Zeit steuern, die der Server auf ein Laufwerk wartet  
Sie können die Höchstdauer in Minuten angeben, die der IBM Spectrum Protect-Server für die aktuelle Mountanforderung auf ein verfügbares Laufwerk wartet.

## Anzahl gleichzeitig bereitgestellter Datenträger steuern

---

Wenn Sie ein Mountlimit für eine Einheitenklasse festlegen, müssen Sie die Anzahl Speichereinheiten berücksichtigen, die mit Ihrem System verbunden sind. Außerdem müssen Sie berücksichtigen, ob die Funktion für gleichzeitiges Schreiben verwendet wird und ob mehrere Einheitenklassen einem einzelnen Speicherarchiv zugeordnet werden; darüber hinaus müssen Sie die Anzahl Prozesse berücksichtigen, die gleichzeitig ausgeführt werden.

### Informationen zu diesem Vorgang

---

Wenn Sie ein Mountlimit für eine Einheitenklasse auswählen, müssen Sie Folgendes berücksichtigen:

- Wie viele Speichereinheiten sind an Ihr System angeschlossen?

Geben Sie keinen Wert für das Mountlimit an, der größer als die Anzahl zugeordneter, verfügbarer Laufwerke in Ihrer Installation ist. Wenn der Server versucht, die durch das Mountlimit angegebene Anzahl Datenträger bereitzustellen und keine Laufwerke für den erforderlichen Datenträger verfügbar sind, tritt ein Fehler auf und Clientsitzungen werden möglicherweise beendet. (Diese Einschränkung gilt nicht, wenn der Parameter DRIVES angegeben wird.)

Wenn Speicherarchivressourcen in einem SAN von IBM Spectrum Protect-Servern gemeinsam genutzt werden, müssen Sie die Anzahl Bandlaufwerke, die ein Speicherarchivclient gleichzeitig nutzen kann, begrenzen. Um mehreren Speicherarchivclient-Servern die gleichzeitige Verwendung eines Speicherarchivs zu ermöglichen, geben Sie den Parameter MOUNTLIMIT an, wenn Sie die Einheitenklasse auf dem Speicherarchivclient definieren oder aktualisieren. Weitere Informationen zum Konfigurieren der gemeinsamen Speicherarchivnutzung finden Sie in Gemeinsame Speicherarchivnutzung konfigurieren.

- Verwenden Sie die Funktion für gleichzeitiges Schreiben für primäre Speicherpools, Kopierspeicherpools und Pools für aktive Daten?

Geben Sie einen Wert für das Mountlimit an, mit dem genügend Mountpunkte bereitgestellt werden, um das gleichzeitige Schreiben von Daten in den primären Speicherpool und in alle zugehörigen Kopierspeicherpools und Pools für aktive Daten zu unterstützen.

- Ordnen Sie mehrere Einheitenklassen einem einzigen Speicherarchiv zu?

Eine Einheitenklasse, die einem Speicherarchiv zugeordnet ist, kann jedes Laufwerk in dem Speicherarchiv verwenden, das mit dem Einheitentyp der Einheitenklasse kompatibel ist. Da Sie einem Speicherarchiv mehrere Einheitenklassen zuordnen können, kann ein einzelnes Laufwerk im Speicherarchiv von mehreren Einheitenklassen verwendet werden. IBM Spectrum Protect stellt sicher, dass zwei Operationen nicht gleichzeitig dasselbe Laufwerk mit zwei unterschiedliche Einheitenklassen verwenden können.

- Wie viele IBM Spectrum Protect-Prozesse sollen unter Verwendung der Einheiten in dieser Einheitenklasse gleichzeitig ausgeführt werden?

IBM Spectrum Protect bricht einige Prozesse automatisch ab, um andere Prozesse mit höherer Priorität auszuführen. Wenn der Server alle verfügbaren Laufwerke in einer Einheitenklasse zur Ausführung von Prozessen mit höherer Priorität verwendet, müssen Prozesse mit niedriger Priorität warten, bis ein Laufwerk verfügbar wird. IBM Spectrum Protect bricht beispielsweise den Prozess für einen Client ab, der Daten direkt auf Band sichert, wenn das Laufwerk für einen Servermigrations- oder Bandkonsolidierungsprozess benötigt wird. IBM Spectrum Protect bricht einen Bandkonsolidierungsprozess ab, wenn das Laufwerk für eine Clientzurückschreibungsoperation benötigt wird. Weitere Informationen finden Sie in Operationen zurückstellen.

Wenn Prozesse häufig durch andere Prozesse abgebrochen werden, überlegen Sie, ob IBM Spectrum Protect mehr Laufwerke zur Verfügung gestellt werden können. Überprüfen Sie andernfalls die Planung von Operationen, um Laufwerkkonflikte zu reduzieren.

Diese Überlegungen gelten auch für die Funktion für gleichzeitiges Schreiben. Es müssen genügend Laufwerke verfügbar sein, um eine Operation für gleichzeitiges Schreiben erfolgreich ausführen zu können.

Um die maximale Anzahl Datenträger anzugeben, die gleichzeitig bereitgestellt werden können, verwenden Sie den Parameter MOUNTLIMIT wenn Sie die Einheitenklasse definieren oder ihre Definition aktualisieren.

#### Zugehörige Verweise:

[DEFINE DEVCLASS](#) (Einheitenklasse definieren)

#### Zugehörige Informationen:

[UPDATE DEVCLASS](#) (Einheitenklasse aktualisieren)

## Steuern, wie lange ein Datenträger bereitgestellt bleibt

---

Sie können steuern, wie lange ein bereitgestellter Datenträger nach seiner letzten E/A-Aktivität bereitgestellt bleiben soll. Wenn ein Datenträger häufig verwendet wird, können Sie die Leistung verbessern, indem Sie einen längeren Mount-Aufbewahrungszeitraum definieren, um unnötige Operationen zum Bereitstellen und Aufheben der Bereitstellung zu vermeiden.

## Informationen zu diesem Vorgang

---

Wenn Mountoperationen durch manuelle Bedieneraktivitäten ausgeführt werden, möchten Sie möglicherweise einen langen Mount-Aufbewahrungszeitraum angeben. Wenn beispielsweise der gesamte Betrieb an einem Wochenende durch nur einen einzigen Bediener unterstützt wird, definieren Sie einen langen Mount-Aufbewahrungszeitraum, damit der Bediener nicht ständig zur Bereitstellung von Datenträgern aufgefordert wird.

Um zu steuern, wie lange ein bereitgestellter Datenträger bereitgestellt bleiben soll, verwenden Sie den Parameter MOUNTRETENTION, wenn Sie die Einheitenklasse definieren oder ihre Definition aktualisieren. Wenn der Wert für den Mount-Aufbewahrungszeitraum beispielsweise 60 ist und ein bereitgestellter Datenträger 60 Minuten lang inaktiv ist, wird seine Bereitstellung vom Server aufgehoben.

Solange ein Datenträger für IBM Spectrum Protect bereitgestellt ist, ist das Laufwerk IBM Spectrum Protect zugeordnet und kann nicht anderweitig verwendet werden. Wenn das Laufwerk für andere Verwendungszwecke freigegeben werden muss, können Sie IBM Spectrum Protect-Operationen, die das Laufwerk verwenden, abbrechen und dann die Bereitstellung des Datenträgers aufheben. Sie können beispielsweise Servermigrations- oder -sicherungsoperationen abbrechen. Informationen zum Abbrechen von Prozessen und zum Aufheben der Bereitstellung von Datenträgern finden Sie in Serveranforderungen für Datenträger verwalten.

### Zugehörige Verweise:

➔ DEFINE DEVCLASS (Einheitenklasse definieren)

### Zugehörige Informationen:

➔ UPDATE DEVCLASS (Einheitenklasse aktualisieren)

## Zeit steuern, die der Server auf ein Laufwerk wartet

---

Sie können die Höchstdauer in Minuten angeben, die der IBM Spectrum Protect-Server für die aktuelle Mountanforderung auf ein verfügbares Laufwerk wartet.

## Informationen zu diesem Vorgang

---

Um zu steuern, wie lange gewartet werden soll, bis ein Laufwerk für eine Mountanforderung verfügbar wird, verwenden Sie den Parameter MOUNTWAIT, wenn Sie eine Einheitenklasse definieren oder aktualisieren.

### Zugehörige Verweise:

➔ DEFINE DEVCLASS (Einheitenklasse definieren)

### Zugehörige Informationen:

➔ UPDATE DEVCLASS (Einheitenklasse aktualisieren)

## Operationen zurückstellen

---

Der Server kann Server- oder Clientoperationen für eine Operation mit höherer Priorität zurückstellen, wenn ein Mountpunkt im Gebrauch ist und keine anderen Mountpunkte verfügbar sind oder der Zugriff auf einen bestimmten Datenträger erforderlich ist. Wenn eine Operation zurückgestellt wird, wird sie abgebrochen.

Mit dem Befehl QUERY MOUNT können Sie den Status des Datenträgers für den Mountpunkt anzeigen.

Standardmäßig ist die Zurückstellung auf dem Server aktiviert. Um die Zurückstellung zu inaktivieren, geben Sie NOPREEMPT in der Serveroptionsdatei an. Wenn Sie diese Option angeben, sind der Befehl BACKUP DB und die Export- und Importbefehle die einzigen Operationen, durch die andere Operationen zurückgestellt werden können.

- Zurückstellung von Operationen für einen Mountpunkt  
Wenn eine Operation mit hoher Priorität einen Mountpunkt in einer bestimmten Einheitenklasse erfordert und alle Mountpunkte in der Einheitenklasse im Gebrauch sind, kann ein Mountpunkt einer Operation mit niedrigerer Priorität durch die Operation mit hoher Priorität zurückgestellt werden.
- Zurückstellung des Datenträgerzugriffs  
Wenn eine Operation mit hoher Priorität Zugriff auf einen bestimmten Datenträger erfordert und dieser Datenträger im Gebrauch ist, kann die Operation mit niedrigerer Priorität für diesen Datenträger durch die Operation mit hoher Priorität zurückgestellt werden.

### Zugehörige Verweise:

➔ BACKUP DB (Datenbank sichern)

## Zurückstellung von Operationen für einen Mountpunkt

---

Wenn eine Operation mit hoher Priorität einen Mountpunkt in einer bestimmten Einheitenklasse erfordert und alle Mountpunkte in der Einheitenklasse im Gebrauch sind, kann ein Mountpunkt einer Operation mit niedrigerer Priorität durch die Operation mit hoher Priorität zurückgestellt werden.

Mountpunkte können nur zurückgestellt werden, wenn die Einheitenklasse der Operation, die die Zurückstellung ausführt, mit der Einheitenklasse der Operation, die zurückgestellt wird, übereinstimmt.

Die folgenden Operationen mit hoher Priorität können eine Zurückstellung anderer Operationen für einen Mountpunkt bewirken.

- Datenbanksicherungsoperationen
- Abruf-, Zurückschreibungs- oder HSM-Rückrufoperationen, die von Clients eingeleitet werden
- Zurückschreibungsoperationen mithilfe einer fernen Einheit zum Versetzen von Daten
- Exportoperationen
- Importoperationen
- Operationen zum Generieren von Sicherungsgruppen

Die folgenden Serveroperationen können keine Zurückstellung anderer Operationen bewirken bzw. nicht durch andere Operationen zurückgestellt werden:

- Prüfen eines Datenträgers
- Zurückschreiben von Daten aus einem Kopierspeicherpool oder einem Pool für aktive Daten
- Vorbereiten einer Wiederherstellungsplandatei
- Speichern von Daten mithilfe einer fernen Einheit zum Versetzen von Daten

Die folgenden Operationen können zurückgestellt werden und sind in der Reihenfolge von der höchsten zur niedrigsten Priorität aufgelistet. Der Server wählt die Operation mit der niedrigsten Priorität, beispielsweise die Identifikation doppelter Daten, für die Zurückstellung aus.

- Replizieren von Knoten
- Sichern von Daten in einem Kopierspeicherpool
- Kopieren aktiver Daten in einen Pool für aktive Daten
- Versetzen von Daten auf einen Speicherpoolatenträger
- Umlagern von Daten von Platte auf sequenzielle Datenträger
- Umlagern von Daten von sequenziellen Datenträgern auf sequenzielle Datenträger
- Sicherungs-, Archivierungs- oder HSM-Umlagerungsoperationen, die von Clients eingeleitet werden
- Konsolidieren von Datenträgern in einem Speicherpool mit sequenziellem Zugriff
- Identifizieren doppelter Daten

## Zurückstellung des Datenträgerzugriffs

---

Wenn eine Operation mit hoher Priorität Zugriff auf einen bestimmten Datenträger erfordert und dieser Datenträger im Gebrauch ist, kann die Operation mit niedrigerer Priorität für diesen Datenträger durch die Operation mit hoher Priorität zurückgestellt werden.

Wenn beispielsweise eine Zurückschreibungsanforderung Zugriff auf einen Datenträger erfordert, der von einer Konsolidierungsoperation verwendet wird, und ein Laufwerk verfügbar ist, wird die Konsolidierungsoperation abgebrochen.

Die folgenden Operationen mit hoher Priorität können eine Zurückstellung von Operationen für den Zugriff auf einen bestimmten Datenträger bewirken:

- Datenbanksicherungsoperationen
- Abruf-, Zurückschreibungs- oder HSM-Rückrufoperationen, die von Clients eingeleitet werden
- Zurückschreibungsoperationen mithilfe einer fernen Einheit zum Versetzen von Daten
- Exportoperationen
- Importoperationen
- Operationen zum Generieren von Sicherungsgruppen

Die folgenden Operationen können keine Zurückstellung anderer Operationen bewirken bzw. nicht durch andere Operationen zurückgestellt werden:

- Prüfen eines Datenträgers
- Zurückschreiben von Daten aus einem Kopierspeicherpool oder einem Pool für aktive Daten
- Vorbereiten eines Wiederherstellungsplans

- Speichern von Daten mithilfe einer fernen Einheit zum Versetzen von Daten

Die folgenden Operationen können zurückgestellt werden und sind in der Reihenfolge von der höchsten zur niedrigsten Priorität aufgelistet. Der Server wählt die Operation mit der niedrigsten Priorität, beispielsweise die Identifikation doppelter Daten, für die Zurückstellung aus.

- Replizieren von Knoten
- Sichern von Daten in einem Kopierspeicherpool
- Kopieren aktiver Daten in einen Pool für aktive Daten
- Versetzen von Daten auf einen Speicherpoolatenträger
- Umlagern von Daten von Platte auf sequenzielle Datenträger
- Umlagern von Daten von sequenziellen Datenträgern auf sequenzielle Datenträger
- Sicherungs-, Archivierungs- oder HSM-Umlagerungsoperationen, die vom Client eingeleitet werden
- Konsolidieren von Datenträgern in einem Speicherpool mit sequenziellem Zugriff
- Identifizieren doppelter Daten

## Auswirkungen von Einheitenänderungen im SAN

---

Die SAN-Umgebung kann sich aufgrund von Änderungen an den Einheiten oder an der Verkabelung dramatisch ändern. Aufgrund der dynamischen Natur des SAN können statische Definitionen fehlschlagen oder unvorhersehbar werden.

Einheiten-IDs, die vom SAN zugeordnet werden und dem Server oder Speicheragenten bekannt sind, können sich aufgrund von Buszurücksetzungen oder aufgrund anderer Umgebungsänderungen ändern. Beispielsweise kann dem Server eine Einheit X auf der Basis der ursprünglichen Pfadspezifikation für den Server und der ursprünglichen Konfiguration des LAN als *rmt0* (unter AIX) bekannt sein. Ein Ereignis im SAN, beispielsweise das Hinzufügen der neuen Einheit Y, führt jedoch dazu, dass der Einheit X die ID *rmt1* zugeordnet wird. Wenn der Server versucht, auf Einheit X unter Verwendung von *rmt0* zuzugreifen, schlägt der Zugriff fehl oder der Zugriff erfolgt auf die falsche Zieleinheit. Der Server versucht, die Wiederherstellung nach Änderungen an Einheiten im SAN durch Verwendung von Seriennummern auszuführen, um die Identität der Einheiten, auf die er zugreift, zu bestätigen.

Wenn Sie ein Laufwerk oder Speicherarchiv definieren, können Sie wahlweise die Seriennummer für diese Einheit angeben. Wenn Sie die Seriennummer bei der Definition der Einheiten nicht angeben, ruft der Server die Seriennummer ab, wenn Sie den Pfad für die Einheit definieren. In beiden Fällen wird die Einheitenseriennummer in der Datenbank des Servers gespeichert und kann zum Bestätigen der Identität einer Einheit für Operationen verwendet werden.


Wenn der Server Laufwerke und Speicherarchive in einem SAN verwendet, versucht der Server zu überprüfen, ob die korrekte Einheit verwendet wird. Der Server kontaktiert die Einheit unter Verwendung des Einheitennamens in dem von Ihnen für die Einheit definierten Pfad. Anschließend fordert der Server die Seriennummer von der Einheit an und vergleicht diese Seriennummer mit der Seriennummer, die für diese Einheit in der Serverdatenbank gespeichert ist.

Wenn die Seriennummern nicht übereinstimmen, startet der Server den Erkennungsprozess im SAN und versucht, die Einheit mit der übereinstimmenden Seriennummer zu finden. Wenn der Server die Einheit mit der übereinstimmenden Seriennummer findet, korrigiert er die Definition des Pfads in der Serverdatenbank, indem er den Einheitennamen in diesem Pfad aktualisiert. Der Server gibt eine Nachricht mit Informationen zu der an der Einheit durchgeführten Änderung aus. Anschließend wird die Einheit vom Server verwendet.

Um festzustellen, wann sich Einheitenänderungen im SAN auf den IBM Spectrum Protect-Server auswirken, können Sie das Aktivitätenprotokoll auf Nachrichten überwachen. Die folgenden Nachrichten betreffen Seriennummern:

- ANR8952 bis ANR8958
- ANR8961 bis ANR8968
- ANR8974 bis ANR8975

Einschränkung: Einige Einheiten können ihre Seriennummern nicht an Anwendungen wie den IBM Spectrum Protect-Server melden. Wenn der Server die Seriennummer einer Einheit nicht abrufen kann, kann der Server das System nicht bei der Wiederherstellung nach der Änderung einer Einheitenposition im SAN unterstützen.

 Windows-Betriebssysteme

## Einheitendaten anzeigen

---

Mithilfe des Dienstprogramms für Einheitendaten (tsmdlst) können Sie Informationen zu Einheiten anzeigen, die mit dem Server verbunden sind.

### Vorbereitende Schritte

---

- Stellen Sie sicher, dass die HBA-API installiert ist. Die HBA-API ist erforderlich, um das Dienstprogramm für Einheitendaten auszuführen.



- Stellen Sie sicher, dass der Bandeinheitentreiber installiert und konfiguriert ist.

## Vorgehensweise

---

1. Wechseln Sie über eine Eingabeaufforderung in das Unterverzeichnis `server` im Serverinstallationsverzeichnis, beispielsweise `C:\Programme\Tivoli\TSM\server`.
2. Führen Sie die ausführbare Datei `tsmdlst.exe` aus.

### Zugehörige Verweise:

- 📄 [QUERY SAN](#) (Einheiten im SAN abfragen)
- 📄 [tsmdlst](#) (Informationen zu Einheiten anzeigen)

## WORM-Banddatenträger

---

WORM-Datenträger können als Schutz vor dem versehentlichen oder absichtlichen Löschen kritischer Daten verwendet werden. In IBM Spectrum Protect gibt es jedoch bestimmte Einschränkungen und Richtlinien, die bei der Verwendung von WORM-Datenträgern zu beachten sind.

Die folgenden Typen von WORM-Datenträgern können mit IBM Spectrum Protect verwendet werden:

- IBM® 3592, alle unterstützten Generationen
- IBM LTO-3 und alle unterstützten Generationen
- HP LTO-3 und alle unterstützten Generationen
- Quantum LTO-3 und alle unterstützten Generationen
- Quantum SDLT 600, Quantum DLT V4 und Quantum DLT S4
- StorageTek VolSafe
- Sony AIT50 und AIT100

### Tipps:

- Ein Speicherpool kann entweder aus WORM-Datenträgern oder aus RW-Datenträgern bestehen, aber nicht aus Datenträgern beider Typen.
- Um die Verschwendung von Bändern nach einer Zurückschreibungs- oder Importoperation zu verhindern, verwenden Sie keine WORM-Bänder für Datenbanksicherungs- oder Exportoperationen.
- WORM-fähige Laufwerke  
Um WORM-Datenträger in einem Speicherarchiv verwenden zu können, müssen alle Laufwerke in dem Speicherarchiv WORM-fähig sein. Ein Mount schlägt fehl, wenn eine WORM-Kassette in einem Laufwerk mit Schreib-/Lesezugriff (RW-Laufwerk) bereitgestellt wird.
- WORM-Datenträger zurückstellen  
Der Typ des WORM-Datenträgers legt fest, ob der Datenträgerkennsatz beim Zurückstellen gelesen werden muss.
- Einschränkungen für WORM-Datenträger  
Sie können keine WORM-Datenträger, denen vorab Kennsätze zugeordnet wurden, mit der Einheitenklasse LTO oder ECARTRIDGE verwenden.
- Mountfehler bei WORM-Datenträgern  
Wenn WORM-Banddatenträger für einen Mount mit einer Einheitenklasse mit Schreib-/Lesezugriff (RW) in ein Laufwerk geladen werden, hat dies einen Mountfehler zur Folge. Dementsprechend hat, wenn RW-Banddatenträger für einen Mount mit einer Einheitenklasse WORM in ein Laufwerk geladen werden, dies ebenfalls das Fehlschlagen des Mounts zur Folge.
- WORM-Datenträgern neue Kennsätze zuordnen  
Einer WORM-Kassette kann kein neuer Kennsatz zugeordnet werden, wenn sie Daten enthält. Dies gilt für Sony AIT WORM-, LTO WORM-, SDLT WORM-, DLT WORM- und IBM 3592-Kassetten. Der Kennsatz auf einem VolSafe-Datenträger sollte nur einmal überschrieben werden und sollte nur überschrieben werden, wenn der Datenträger keine verwendbaren, gelöschten oder verfallenen Daten enthält.
- Private WORM-Datenträger aus einem Speicherarchiv entfernen  
Wenn Sie eine Aktion für einen WORM-Datenträger ausführen (wenn Sie beispielsweise Dateibereiche löschen) und der Server den Datenträger nicht als voll markiert, wird der Datenträger in den Arbeitsstatus zurückversetzt. Wenn ein WORM-Datenträger nicht als voll markiert wird und aus einem Speicherpool gelöscht wird, bleibt der Datenträger ein privater Datenträger. Um einen privaten WORM-Datenträger aus einem Speicherarchiv zu entfernen, müssen Sie den Befehl `CHECKOUT LIBVOLUME` ausgeben.
- Erstellung von DLT WORM-Datenträgern  
DLT WORM-Datenträger können aus Datenträgern mit Schreib-/Lesezugriff (RW-Datenträgern) erstellt werden, indem sie konvertiert werden.
- Unterstützung für kurze und normale 3592 WORM-Bänder  
IBM Spectrum Protect unterstützt sowohl kurze als auch normale 3592 WORM-Bänder. Die besten Ergebnisse werden erzielt, wenn Sie die Bänder in separaten Speicherpools definieren.

- Einheitenklasse nach der Einstellung des Parameters WORM abfragen  
Sie können die Einstellung des Parameters WORM für eine Einheitenklasse mithilfe des Befehls QUERY DEVCLASS bestimmen. Die Ausgabe enthält ein Feld mit der Bezeichnung WORM und einen Wert (YES oder NO).

## WORM-fähige Laufwerke

---

Um WORM-Datenträger in einem Speicherarchiv verwenden zu können, müssen alle Laufwerke in dem Speicherarchiv WORM-fähig sein. Ein Mount schlägt fehl, wenn eine WORM-Kassette in einem Laufwerk mit Schreib-/Lesezugriff (RW-Laufwerk) bereitgestellt wird.

Ein WORM-fähiges Laufwerk kann jedoch als RW-Laufwerk verwendet werden, wenn der Parameter WORM in der Einheitenklasse auf NO gesetzt wird. Jeder Typ von Speicherarchiv kann sowohl über WORM- als auch über RW-Datenträger verfügen, wenn *alle* Laufwerke für WORM aktiviert sind. Die einzige Ausnahme von dieser Regel sind NAS-Speicherarchive, in denen WORM-Banddatenträger nicht verwendet werden können.

### Zugehörige Verweise:

[DEFINE DEVCLASS](#) (Einheitenklasse definieren)

### Zugehörige Informationen:

[UPDATE DEVCLASS](#) (Einheitenklasse aktualisieren)

## WORM-Datenträger zurückstellen

---

Der Typ des WORM-Datenträgers legt fest, ob der Datenträgerkennsatz beim Zurückstellen gelesen werden muss.

Speicherarchivwechsler können nicht zwischen standardmäßigen Banddatenträgern mit Schreib-/Lesezugriff (RW-Banddatenträgern) und den folgenden Typen von WORM-Banddatenträgern unterscheiden:

- VolSafe
- Sony AIT
- LTO
- SDLT
- DLT

Um den Typ des WORM-Datenträgers zu bestimmen, der verwendet wird, muss ein Datenträger in ein Laufwerk geladen werden. Daher müssen Sie beim Zurückstellen einer dieser Typen von WORM-Datenträgern die Option CHECKLABEL=YES im Befehl CHECKIN LIBVOLUME verwenden.

Wenn Speicherarchivwechsler IBM® 3592 Unterstützung für WORM-Datenträger zur Verfügung stellen, können diese Speicherarchivwechsler feststellen, ob ein Datenträger ein WORM-Datenträger ist, ohne den Datenträger in ein Laufwerk laden zu müssen. Die Angabe von CHECKLABEL=YES ist nicht erforderlich. Prüfen Sie mit Ihren Hardwareanbietern, ob Ihre 3592-Laufwerke und -Speicherarchive die erforderliche Unterstützung zur Verfügung stellen.

### Zugehörige Verweise:

[CHECKIN LIBVOLUME](#) (Speicherdatenträger in ein Speicherarchiv zurückstellen)

## Einschränkungen für WORM-Datenträger

---

Sie können keine WORM-Datenträger, denen vorab Kennsätze zugeordnet wurden, mit der Einheitenklasse LTO oder ECARTRIDGE verwenden.

Wenn IBM Spectrum Protect als Schlüsselmanager für die Laufwerkverschlüsselung angegeben ist, können Sie für die folgenden Laufwerke keine WORM-Datenträger verwenden:

- IBM® LTO-5, LTO-6 und später
- HP LTO-5, LTO-6 und später
- Oracle StorageTek T10000B
- Oracle StorageTek T10000C
- Oracle StorageTek T10000D

## Mountfehler bei WORM-Datenträgern

---

Wenn WORM-Banddatenträger für einen Mount mit einer Einheitenklasse mit Schreib-/Lesezugriff (RW) in ein Laufwerk geladen werden, hat dies einen Mountfehler zur Folge. Dementsprechend hat, wenn RW-Banddatenträger für einen Mount mit einer Einheitenklasse WORM in ein Laufwerk geladen werden, dies ebenfalls das Fehlschlagen des Mounts zur Folge.

## WORM-Datenträgern neue Kennsätze zuordnen

Einer WORM-Kassette kann kein neuer Kennsatz zugeordnet werden, wenn sie Daten enthält. Dies gilt für Sony AIT WORM-, LTO WORM-, SDLT WORM-, DLT WORM- und IBM® 3592-Kassetten. Der Kennsatz auf einem VolSafe-Datenträger sollte nur einmal überschrieben werden und sollte nur überschrieben werden, wenn der Datenträger keine verwendbaren, gelöschten oder verfallenen Daten enthält.

Geben Sie den Befehl LABEL LIBVOLUME nur einmal für VolSafe-Datenträger aus. Um zu verhindern, dass der Kennsatz überschrieben wird, können Sie die Option OVERWRITE=NO im Befehl LABEL LIBVOLUME verwenden.

### Zugehörige Verweise:

 LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

## Private WORM-Datenträger aus einem Speicherarchiv entfernen

Wenn Sie eine Aktion für einen WORM-Datenträger ausführen (wenn Sie beispielsweise Dateibereiche löschen) und der Server den Datenträger nicht als voll markiert, wird der Datenträger in den Arbeitsstatus zurückversetzt. Wenn ein WORM-Datenträger nicht als voll markiert wird und aus einem Speicherpool gelöscht wird, bleibt der Datenträger ein privater Datenträger. Um einen privaten WORM-Datenträger aus einem Speicherarchiv zu entfernen, müssen Sie den Befehl CHECKOUT LIBVOLUME ausgeben.

### Zugehörige Verweise:

 CHECKOUT LIBVOLUME (Speicherdatenträger aus einem Speicherarchiv entnehmen)

## Erstellung von DLT WORM-Datenträgern

DLT WORM-Datenträger können aus Datenträgern mit Schreib-/Lesezugriff (RW-Datenträgern) erstellt werden, indem sie konvertiert werden.

Wenn SDLT-600-, DLT-V4- oder DLT-S4-Laufwerke vorhanden sind und diese für WORM-Datenträger aktiviert werden sollen, führen Sie für die Laufwerke unter Verwendung von V30 oder einer späteren Firmware, die von Quantum verfügbar ist, ein Upgrade durch. Sie können auch DLTIce-Software verwenden, um unformatierte RW-Datenträger oder leere Datenträger in WORM-Datenträger zu konvertieren.

In SCSI-Speicherarchiven erstellt der IBM Spectrum Protect-Server automatisch DLT WORM-Arbeitsdatenträger, wenn der Server keine WORM-Arbeitsdatenträger im Bestand eines Speicherarchivs finden kann. Der Server konvertiert verfügbare unformatierte oder leere RW-Arbeitsdatenträger oder leere private RW-Datenträger in WORM-Arbeitsdatenträger. Der Server schreibt auch die Kennsätze auf neu erstellten WORM-Datenträgern neu, indem die Kennsatzinformationen auf den vorhandenen RW-Datenträgern verwendet werden.


## Unterstützung für kurze und normale 3592 WORM-Bänder

IBM Spectrum Protect unterstützt sowohl kurze als auch normale 3592 WORM-Bänder. Die besten Ergebnisse werden erzielt, wenn Sie die Bänder in separaten Speicherpools definieren.

## Einheitenklasse nach der Einstellung des Parameters WORM abfragen

Sie können die Einstellung des Parameters WORM für eine Einheitenklasse mithilfe des Befehls QUERY DEVCLASS bestimmen. Die Ausgabe enthält ein Feld mit der Bezeichnung WORM und einen Wert (YES oder NO).

### Zugehörige Informationen:

 QUERY DEVCLASS (Informationen zu einer oder mehreren Einheitenklassen anzeigen)

 Windows-Betriebssysteme

## Einheitenfehler beheben



Sie können Fehler beheben, die bei der Konfiguration oder Verwendung von Einheiten mit IBM Spectrum Protect auftreten.

## Informationen zu diesem Vorgang

Verwenden Sie Tabelle 1, um eine Lösung für den einheitenbezogenen Fehler zu finden.

Tabelle 1. Behebung von Einheitenfehlern

| Symptom | Problem | Lösung |
|---------|---------|--------|
|---------|---------|--------|

| Symptom                                   | Problem  | Lösung  |
|---|--|---|
| Konflikte mit anderen Anwendungen         | IBM Spectrum Protect erfordert für die gemeinsame Nutzung von Einheiten ein Speicherbereichsnetz.  | Konfigurieren Sie ein Speicherbereichsnetz.<br>Achtung: Wenn mehrere IBM Spectrum Protect-Server dieselbe Einheit verwenden, kann dies zu einem Datenverlust führen. Definieren oder verwenden Sie eine Einheit nur für einen einzigen IBM Spectrum Protect-Server.<br> AIX-Betriebssysteme<br> Linux-Betriebssysteme<br>Andere Anwendungen können auf IBM Spectrum Protect-Einheiten unter Verwendung eines SCSI-Bandtreibers zugreifen. |
| Fehlschlagen der Zuordnung von Kennsätzen | Eine Einheit kann nicht zum Zuordnen von Kennsätzen zu Datenträgern verwendet werden, wenn der Server die Einheit gleichzeitig für andere Prozesse verwendet.  | Sie können vorhandene Datenträger in einem Speicherpool nicht überschreiben.<br><br>Sie müssen alle Hardwareprobleme lösen, bevor Sie einem Datenträger einen Kennsatz zuordnen können.   |
|   | Falsche oder unvollständige Lizenzregistrierung  | Registrieren Sie die Lizenz für die gekaufte Einheitenunterstützung.  |
| Konflikte zwischen Einheitentreibern      | IBM Spectrum Protect gibt Nachrichten zu E/A-Fehlern aus, wenn Sie eine Einheit mit sequenziellem Zugriff definieren oder verwenden.   | Bei Windows-Einheitentreibern und von anderen Anwendungen bereitgestellten Treibern können Konflikte mit dem IBM Spectrum Protect-Einheitentreiber auftreten, wenn der IBM Spectrum Protect-Treiber nicht zuerst gestartet wird. Um die Reihenfolge zu überprüfen, in der die Einheitentreiber vom System gestartet werden, führen Sie die folgenden Schritte aus:<br><br><ol style="list-style-type: none"> <li>1. Klicken Sie auf Systemsteuerung.</li> <li>2. Klicken Sie auf Geräte.<br/>Einheitentreiber und ihre Starttypen werden aufgelistet.</li> </ol>  |
| E/A-Fehler                                | Wenn Sie versuchen, eine Bandeinheit zu definieren oder zu verwenden, können Konflikte mit Einheitentreibern auftreten. Bei Windows-Einheitentreibern und von anderen Anwendungen bereitgestellten Treibern können Konflikte mit dem IBM Spectrum Protect-Einheitentreiber auftreten, wenn dieser nicht zuerst gestartet wird. |   |

## Implementierung abschließen

Nachdem die IBM Spectrum Protect- Lösung konfiguriert wurde und aktiv ist, testen Sie Sicherungsoperationen und konfigurieren Sie die Überwachung, um sicherzustellen, dass alles ordnungsgemäß funktioniert.

### Vorgehensweise

1. Testen Sie Sicherungsoperationen, um sicherzustellen, dass Ihre Daten wie erwartet geschützt werden.
  - a. Wählen Sie auf der Seite Clients im Operations Center die Clients aus, die gesichert werden sollen, und klicken Sie auf Sichern.
  - b. Wählen Sie auf der Seite Server im Operations Center den Server aus, dessen Datenbank gesichert werden soll. Klicken Sie auf Sichern und führen Sie die Anweisungen im Fenster Datenbank sichern aus.
  - c. Überprüfen Sie, ob die Sicherungsoperationen erfolgreich ohne Warnungen oder Fehlermeldungen ausgeführt wurden.

- Tipp: Sie können auch stattdessen die GUI des Clients für Sichern/Archivieren zum Sichern von Clientdaten verwenden und die Serverdatenbank sichern, indem Sie den Befehl BACKUP DB in einer Verwaltungsbefehlszeile ausgeben.
2. Konfigurieren Sie die Überwachung für Ihre Lösung, indem Sie die Anweisungen in Bandspeicherlösung überwachen ausführen.

## Bandspeicherlösung überwachen

Überwachen Sie nach der Implementierung einer bandbasierten Lösung in IBM Spectrum Protect die Lösung, um ihre korrekte Funktionsweise sicherzustellen. Indem die Lösung täglich und regelmäßig überwacht wird, können Sie bestehende und potenzielle Probleme erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden.

### Informationen zu diesem Vorgang

Die Überwachung einer Lösung erfolgt bevorzugt über die Verwendung des Operations Center, das den Gesamtsystemstatus und den detaillierten Systemstatus in einer grafischen Benutzerschnittstelle bereitstellt. Darüber hinaus können Sie das Operations Center zum Generieren von E-Mail-Berichten zur Zusammenfassung des Systemstatus konfigurieren.

### Vorgehensweise

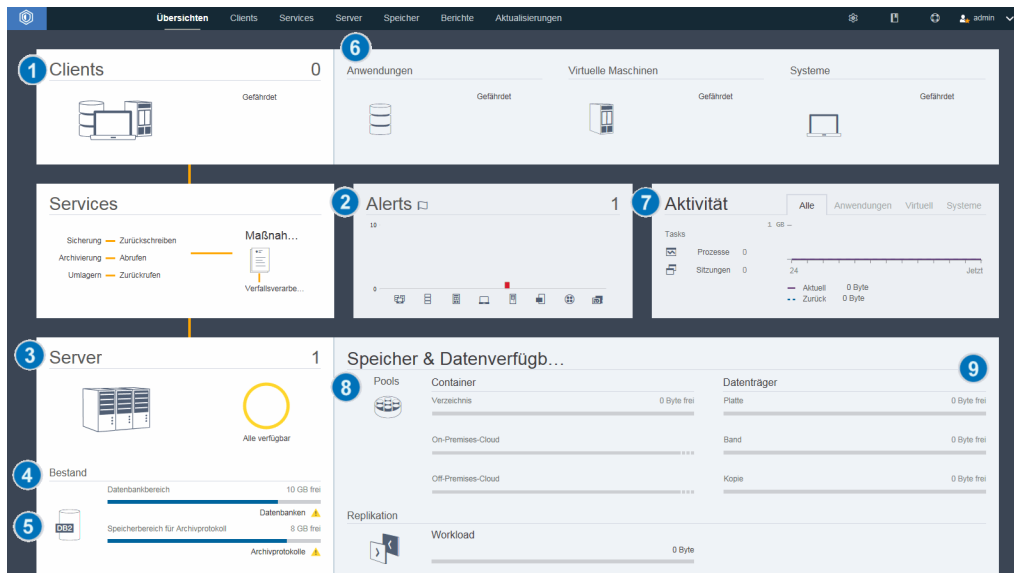
1. Führen Sie tägliche Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für tägliche Überwachungstasks.
2. Führen Sie regelmäßige Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für regelmäßige Überwachungstasks.
3. Überprüfen Sie, ob Ihr System die Lizenzierungsanforderungen erfüllt. Anweisungen finden Sie in Lizenzierung überprüfen.
4. Optional: Konfigurieren Sie E-Mail-Berichte des Systemstatus. Anweisungen finden Sie in Systemstatus mithilfe von E-Mail-Berichten verfolgen.


## Prüfliste für tägliche Überwachungstasks

Um sicherzustellen, dass die täglichen Überwachungstasks für Ihre IBM Spectrum Protect-Lösung ausgeführt werden, überprüfen Sie die Prüfliste für tägliche Überwachungstasks.

Führen Sie die täglichen Überwachungstasks über die Seite Übersicht im Operations Center aus. Sie können auf die Seite Übersicht zugreifen, indem Sie das Operations Center öffnen und auf Übersichten klicken.

Die folgende Abbildung zeigt die Position zur Ausführung der jeweiligen Task.









Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen  und klicken Sie auf Command Builder.

In der folgenden Tabelle sind die täglichen Überwachungstasks sowie Anweisungen zur Ausführung jeder Task aufgeführt.

Tabelle 1. Tägliche Überwachungstasks



| Task   | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen  |
|--|--|---|
| <p><b>1</b> Bestimmen Sie, ob Clients vorhanden sind, bei denen die Gefahr besteht, dass sie aufgrund fehlgeschlagener oder versäumter Sicherungsoperationen ungeschützt sind.</p> | <p>Um zu überprüfen, ob Clients gefährdet sind, suchen Sie nach einem Hinweis Gefährdet. Um Details anzuzeigen, klicken Sie auf den Bereich 'Clients'.</p> <p>Achtung: Wenn der Prozentsatz für Gefährdet sehr viel höher als üblicherweise ist, kann dies eine Ransomware-Attacke anzeigen. Eine Ransomware-Attacke kann das Fehlschlagen von Sicherungsoperationen zur Folge haben und somit Clients in den Status 'Gefährdet' versetzen. Wenn beispielsweise der Prozentsatz gefährdeter Clients normalerweise zwischen 5 % und 10 % liegt, sich aber auf 40 % oder 50 % erhöht, ermitteln Sie die Ursache.</p> <p>Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie die Clientfehler- und -planungsprotokolle anzeigen, indem Sie die folgenden Schritte ausführen:</p> <ol style="list-style-type: none"> <li>1. Wählen Sie in der Tabelle 'Clients' den Client aus und klicken Sie auf Details.</li> <li>2. Um ein Problem zu diagnostizieren, klicken Sie auf Diagnose.</li> </ol> | <p>Greifen Sie bei Clients, für die der Clientverwaltungsservice nicht installiert ist, auf das Clientsystem zu, um die Clientfehlerprotokolle zu überprüfen.</p>   |
| <p><b>2</b> Bestimmen Sie, ob clientbezogene oder serverbezogene Fehler einen Bedieneringriff erfordern.</p>   | <p>Um die Bewertung jedes zurückgemeldeten Alerts zu bestimmen, bewegen Sie den Mauszeiger im Bereich 'Alerts' über die Spalten.</p>   | <p>Um zusätzliche Informationen zu Alerts anzuzeigen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf den Bereich 'Alerts'.</li> <li>2. Wählen Sie in der Tabelle 'Alerts' einen Alert aus.</li> <li>3. Überprüfen Sie die Nachrichten im Fenster 'Aktivitätenprotokoll'. In dem Fenster werden zugehörige Nachrichten angezeigt, die vor und nach dem Auftreten des ausgewählten Alerts ausgegeben wurden.</li> </ol> |
| <p><b>3</b> Bestimmen Sie, ob die vom Operations Center verwalteten Server verfügbar sind, um Datenschutzservices für Clients bereitzustellen.</p>                                 | <ol style="list-style-type: none"> <li>1. Um zu überprüfen, ob Server gefährdet sind, suchen Sie im Bereich 'Server' nach einem Hinweis Nicht verfügbar.</li> <li>2. Um zusätzliche Informationen anzuzeigen, klicken Sie auf den Bereich 'Server'.</li> <li>3. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details.</li> </ol>  | <p> Tipp: Wenn Sie ein Problem erkennen, das sich auf die Servermerkmale bezieht, aktualisieren Sie die Servermerkmale:</p> <ol style="list-style-type: none"> <li>1. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details.</li> <li>2. Um die Servermerkmale zu aktualisieren, klicken Sie auf Merkmale.</li> </ol>   |



| Task   | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|--|--|--|
| <p>4 Bestimmen Sie, ob für den Serverbestand, der aus der Serverdatenbank, der aktiven Protokolldatei und dem Archivprotokoll besteht, genügend Speicherbereich verfügbar ist.</p> | <ol style="list-style-type: none"> <li>1. Klicken Sie auf den Bereich 'Server'.</li> <li>2. Zeigen Sie in der Spalte 'Status' der Tabelle den Status des Servers an und beheben Sie alle Probleme: <ul style="list-style-type: none"> <li>o Normal  Für die Serverdatenbank, die aktive Protokolldatei und das Archivprotokoll ist genügend Speicherbereich verfügbar.</li> <li>o Kritisch  Für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll ist nicht genügend Speicherbereich verfügbar. Sie müssen unverzüglich Speicherbereich hinzufügen; andernfalls werden die vom Server bereitgestellten Datenschutzservices unterbrochen.</li> <li>o Warnung  Der Speicherbereich für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll wird knapp. Wenn diese Bedingung bestehen bleibt, müssen Sie Speicherbereich hinzufügen.</li> <li>o Nicht verfügbar  Der Status kann nicht abgerufen werden. Stellen Sie sicher, dass der Server aktiv ist und keine Netzprobleme vorliegen. Dieser Status wird auch angezeigt, wenn die Überwachungsadministrator-ID gesperrt ist oder aus anderen Gründen auf dem Server nicht verfügbar ist. Diese ID hat den Namen IBM-OC-Name_des_Hub-Servers.</li> <li>o Nicht überwacht  Nicht überwachte Server sind für den Hub-Server definiert, aber nicht für die Verwaltung durch das Operations Center konfiguriert. Um einen nicht überwachten Server zu konfigurieren, wählen Sie den Server aus und klicken Sie auf Peripherieserver überwachen.</li> </ul> </li> </ol> | <p>Sie können auch auf der Seite Alerts nach zugehörigen Alerts suchen. Weitere Anweisungen zur Fehlerbehebung finden Sie in Serverprobleme beheben.</p> |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|---|--|--|
| <p><b>5</b> Überprüfen Sie Operationen zur Sicherung der Serverdatenbank.</p>   | <p>Um zu bestimmen, ob ein Server kürzlich gesichert wurde, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf den Bereich 'Server'.</li> <li>2. Überprüfen Sie in der Tabelle 'Server' die Spalte 'Letzte Datenbanksicherung'.</li> </ol>   | <p>Um detaillierte Informationen zu Sicherungsoperationen abzurufen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Wählen Sie in der Tabelle 'Server' eine Zeile aus und klicken Sie auf Details.</li> <li>2. Bewegen Sie im Bereich 'Datenbanksicherung' den Mauszeiger über die Häkchen, um Informationen zu Sicherungsoperation zu überprüfen.</li> </ol> <p>Wenn eine Datenbank nicht kürzlich (beispielsweise innerhalb der letzten 24 Stunden) gesichert wurde, können Sie eine Sicherungsoperation starten:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Server'.</li> <li>2. Wählen Sie in der Tabelle einen Server aus und klicken Sie auf Sichern.</li> </ol> <p>Um zu bestimmen, ob die Serverdatenbank für automatische Sicherungsoperationen konfiguriert ist, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>2. Geben Sie den Befehl QUERY DB aus: <pre>query db f=d</pre> </li> <li>3. Überprüfen Sie in der Ausgabe das Feld Einheitenklassenname für Gesamtsicherungen. Wenn eine Einheitenklasse angegeben ist, ist der Server für automatische Datenbanksicherungen konfiguriert.</li> </ol> |
| <p><b>6</b> Überwachen Sie andere Serververwaltungstasks. Serververwaltungstasks können die Ausführung von Zeitplänen für Verwaltungsbefehle, Verwaltungsscripts und zugehörigen Befehlen umfassen.</p> | <p>Um nach Informationen zu Prozessen zu suchen, die aufgrund von Serverproblemen fehlgeschlagen sind, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf Server &gt; Verwaltung.</li> <li>2. Um das zwei Wochen umfassende Verlaufsprotokoll eines Prozesses abzurufen, zeigen Sie Spalte 'History' an.</li> <li>3. Um weitere Informationen zu einem geplanten Prozess abzurufen, bewegen Sie den Mauszeiger über das Kontrollkästchen, das dem Prozess zugeordnet ist.</li> </ol> | <p>Weitere Informationen zum Überwachen von Prozessen und Beheben von Problemen, finden Sie in der Onlinehilfe des Operations Center.</p>  |



| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|---|--|--|
| <p><b>7</b> Überprüfen Sie, ob das Datenvolumen, das kürzlich an Server bzw. von Servern gesendet wurde, innerhalb des erwarteten Bereichs liegt.</p> | <ul style="list-style-type: none"> <li>• Um eine Übersicht über die Aktivität der letzten 24 Stunden abzurufen, zeigen Sie den Bereich 'Aktivität' an.</li> <li>• Um die Aktivität der letzten 24 Stunden mit der Aktivität der vorherigen 24 Stunden zu vergleichen, studieren Sie die Zahlen in den Bereichen 'Aktuell' und 'Vorherig'.</li> </ul> | <ul style="list-style-type: none"> <li>• Wenn mehr Daten als erwartet an den Server gesendet wurden, bestimmen Sie die Clients, die mehr Daten sichern und ermitteln Sie die Ursache. Möglicherweise funktioniert die clientseitige Datendeduplizierung nicht ordnungsgemäß.<br/>Achtung: Wenn das Volumen gesicherter Daten deutlich umfangreicher als üblicherweise ist, kann dies eine Ransomware-Attacke anzeigen. Wenn Daten durch Ransomware verschlüsselt werden, werden die Daten vom System als geändert wahrgenommen und die geänderten Daten werden gesichert. Demzufolge wird das Volumen gesicherter Daten umfangreicher. Um die betroffenen Clients zu bestimmen, klicken Sie auf die Registerkarten Anwendungen, Virtuell oder Systeme.</li> <li>• Wenn weniger Daten als erwartet an den Server gesendet wurden, überprüfen Sie, ob Clientsicherungsoperationen gemäß Zeitplan ausgeführt werden.</li> </ul> |

| Task   | Basisprozeduren   | Erweiterte Prozeduren und Fehlerbehebungsinformationen  |
|--|---|---|
| <p><b>8</b> Stellen Sie sicher, dass Speicherpools zum Sichern von Clientdaten verfügbar sind.</p> | <ol style="list-style-type: none"> <li>1. Wenn im Bereich 'Speicher &amp; Datenverfügbarkeit' Probleme angezeigt werden, klicken Sie auf Pools, um die Details anzuzeigen: <ul style="list-style-type: none"> <li>◦ Wenn der Status Kritisch  angezeigt wird, ist in dem Speicherpool nicht genügend Speicherbereich verfügbar oder der Speicherpool hat den Zugriffsstatus UNAVAILABLE (Nicht verfügbar).<br/>Achtung: Wenn der Status kritisch ist, ermitteln Sie die Ursache: <ul style="list-style-type: none"> <li>■ Wenn die Dateneduplizierungsrate für einen Speicherpool deutlich fällt, kann dies eine Ransomware-Attacke anzeigen. Während einer Ransomware-Attacke werden Daten verschlüsselt und können nicht dedupliziert werden. Um die Dateneduplizierungsrate zu verifizieren, überprüfen Sie in der Tabelle 'Speicherpools' den Wert in der Spalte 'Einsparungen in %'.</li> <li>■ Wenn ein Speicherpool wider Erwarten zu 100 % ausgelastet ist, kann dies eine Ransomware-Attacke anzeigen. Um die Auslastung zu verifizieren, überprüfen Sie den Wert in der Spalte 'Verwendete Kapazität'.<br/>Bewegen Sie den Mauszeiger über die Werte, um den Prozentsatz für den verwendeten Speicherbereich und den Prozentsatz für den freien Speicherbereich anzuzeigen.</li> </ul> </li> <li>◦ Wenn der Status Warnung  angezeigt wird, wird der Speicherbereich für den Speicherpool knapp oder der Speicherpool hat den Zugriffsstatus READONLY (Lesezugriff).</li> </ul> </li> <li>2. Um den verwendeten Speicherbereich, den freien Speicherbereich und den Gesamtspeicherbereich für Ihren ausgewählten Speicherpool anzuzeigen, bewegen Sie den Mauszeiger über die Einträge in der Spalte 'Verwendete Kapazität'.</li> </ol> | <p>Um die Speicherpoolkapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie eine Zeile in der Tabelle 'Speicherpools' aus und klicken Sie auf Details.</p> |

| Task   | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|--|--|--|
| <p><b>9</b> Stellen Sie sicher, dass Speichereinheiten für Sicherungsoperationen verfügbar sind.</p> | <p>Überprüfen Sie im Bereich 'Speicher &amp; Datenverfügbarkeit' im Abschnitt 'Datenträger' unterhalb der Balken für die Kapazität den Status, der neben Einheiten angegeben ist. Wenn der Status Kritisch  oder Warnung  für eine Einheit angezeigt wird, müssen Sie das Problem untersuchen. Um Details anzuzeigen, klicken Sie auf Einheiten.</p> | <p>Bandeinheiten können den Status 'Warnung' oder 'Kritisch' haben, wenn Laufwerke nicht verfügbar sind. Ein Laufwerk ist nicht verfügbar, wenn es offline ist, während der Antwort an den Server gestoppt wurde oder sein Pfad offline ist. Eine Bandeinheit kann auch den Status 'Kritisch' haben, wenn das Speicherarchiv offline ist. In anderen Spalten der Tabelle 'Bandeinheiten' wird der Status der automatischen Einheiten im Speicherarchiv, der Laufwerke und der Pfade angezeigt.</p> <p>Um Probleme mit Bandlaufwerken zu beheben, die einen kritischen Status haben, können Sie das Laufwerk offline schalten, wenn es für eine andere Aktivität, wie beispielsweise Wartung, verwendet werden muss. Um ein Laufwerk offline zu schalten, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Wählen Sie auf der Seite Speicher im Operations Center Bandeinheiten aus.</li> <li>2. Um weitere Informationen zu einem Bandarchiv anzuzeigen, wählen Sie eine Zeile aus und klicken Sie auf Details.</li> <li>3. Um ein Laufwerk offline zu schalten, wählen Sie das Bandlaufwerk aus und klicken Sie auf Offline.</li> </ol> <p>Stellen Sie bei Bandsicherungsoperationen sicher, dass genügend Arbeitsbänder verfügbar sind. Wenn Sie sich nicht sicher sind, ob die Anzahl verfügbarer Arbeitsbänder ausreichend ist, öffnen Sie das Notizbuch 'Details', um die Bandnutzung sowie eine Schätzung der Verfügbarkeit von Arbeitsbändern anzuzeigen. Um das Notizbuch 'Details' zu öffnen, wählen Sie in der Tabelle ein Speicherarchiv aus und klicken Sie auf 'Details'.</p> |

## Prüfliste für regelmäßige Überwachungstasks

Um sicherzustellen, dass Operationen korrekt ausgeführt werden, führen Sie die Tasks in der Prüfliste für regelmäßige Überwachungstasks aus. Planen Sie regelmäßige Tasks häufig genug, sodass Sie potenzielle Probleme erkennen können, bevor diese wirklich problematisch werden.








Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen  und klicken Sie auf Command Builder.

Tabelle 1. Regelmäßige Überwachungstasks

| Task | Basisprozeduren | Erweiterte Prozeduren und Fehlerbehebung |
|------|-----------------|--|
|------|-----------------|--|

| Task                               | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung   |
|------------------------------------|--|--|
| Überwachen Sie die Systemleistung. | <p>Bestimmen Sie den für Clientsicherungsoperationen erforderlichen Zeitraum:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients. Suchen Sie den Server, der dem Client zugeordnet ist.</li> <li>2. Klicken Sie auf Server. Wählen Sie den Server aus und klicken Sie auf Details.</li> <li>3. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die in den letzten 24 Stunden abgeschlossen wurden, klicken Sie auf Abgeschlossene Tasks.</li> <li>4. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die vor mehr als 24 Stunden abgeschlossen wurden, verwenden Sie den Befehl QUERY ACTLOG. Informationen zu diesem Befehl finden Sie in QUERY ACTLOG (Aktivitätenprotokoll abfragen).</li> <li>5. Wenn die Dauer von Clientsicherungsoperationen zunimmt, ohne dass ein offensichtlicher Grund erkennbar ist, überprüfen Sie Ursache.</li> </ol> <p>Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie Leistungsprobleme für den Client für Sichern/Archivieren diagnostizieren, indem Sie die folgenden Schritte ausführen:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients.</li> <li>2. Wählen Sie einen Client für Sichern/Archivieren aus und klicken Sie auf Details.</li> <li>3. Um Clientprotokolle abzurufen, klicken Sie auf Diagnose.</li> </ol> | <p>Begrenzen Sie die Zeit für Clientsicherungsoperationen auf 8 bis 12 Stunden. Stellen Sie sicher, dass sich Clientzeitpläne nicht mit Serververwaltungstasks überschneiden.</p> <p>Anweisungen zur Reduzierung der Zeit, die der Client zum Sichern von Daten auf dem Server benötigt, finden Sie in Häufig auftretende Clientleistungsprobleme lösen.</p> <p>Suchen Sie nach Leistungsgpässen. Anweisungen finden Sie in Leistungsgpässe identifizieren.</p> <p>Informationen zur Identifikation und Behebung anderer Leistungsprobleme finden Sie in Leistung.</p> |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung |
|---|--|--|
| <p>Stellen Sie sicher, dass aktuelle Sicherungsdateien für Einheitenkonfigurations- und Datenträgerprotokolldaten gesichert werden.</p> | <p>Greifen Sie auf Ihre Speicherpositionen zu, um sicherzustellen, dass die Dateien verfügbar sind. Die bevorzugte Methode ist die Sicherung der Dateien an zwei Positionen.</p> <p>Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder.</li> <li>2. Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, geben Sie die folgenden Befehle aus: <ul style="list-style-type: none"> <li><code>query option volhistory</code></li> <li><code>query option devconfig</code></li> </ul> </li> <li>3. Überprüfen Sie in der Ausgabe die Spalte 'Optionseinstellung', um die Dateipositionen zu finden.</li> </ol> <p>Wenn ein Katastrophenfall eintritt, sind sowohl die Protokolldatei für Datenträger als auch die Einheitenkonfigurationsdatei für die Zurückschreibung der Serverdatenbank erforderlich.</p> |  |

| Task  | Basisprozeduren   | Erweiterte Prozeduren und Fehlerbehebung |
|---|---|--|
| <p>Bestimmen Sie, ob im Verzeichnis für die Serverinstanz genügend Speicherbereich verfügbar ist.</p> | <p>Stellen Sie sicher, dass im Verzeichnis für die Serverinstanz mindestens 50 GB freier Speicherbereich verfügbar ist. Führen Sie die für Ihr Betriebssystem zutreffende Aktion aus:</p> <ul style="list-style-type: none"> <li>•  <b>AIX-Betriebssysteme</b> Um den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus: <pre>df -g Instanzverzeichnis</pre> <p>Dabei gibt <i>Instanzverzeichnis</i> das Instanzverzeichnis an.</p> </li> <li>•  <b>Linux-Betriebssysteme</b> Um den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus: <pre>df -h Instanzverzeichnis</pre> <p>Dabei gibt <i>Instanzverzeichnis</i> das Instanzverzeichnis an.</p> </li> <li>•  <b>Windows-Betriebssysteme</b> Klicken Sie in Windows Explorer mit der rechten Maustaste auf das Dateisystem und klicken Sie auf Eigenschaften. Zeigen Sie die Kapazitätsdaten an.</li> </ul> <p>Die bevorzugte Position des Instanzverzeichnisses ist von dem Betriebssystem abhängig, unter dem der Server installiert ist:</p> <ul style="list-style-type: none"> <li>•  <b>AIX-Betriebssysteme</b></li> <li>•  <b>Linux-Betriebssysteme</b><br/>/home/tsminst1/tsminst1</li> <li>•  <b>Windows-Betriebssysteme</b><br/>C:\tsminst1</li> </ul> <p>Tipp: Wenn Sie ein Arbeitsblatt zur Planung ausgefüllt haben, ist die Position des Instanzverzeichnisses im Arbeitsblatt vermerkt.</p> |  |

| Task   | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung  |
|--|--|---|
| Ermitteln Sie nicht erwartete Clientaktivität. | <p>Um im Rahmen der Überwachung der Clientaktivität zu bestimmen, ob das Datenvolumen das erwartete Volumen überschreitet, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Clients'.</li> <li>2. Um die Aktivität der vergangen zwei Wochen anzuzeigen, doppelklicken Sie auf einen beliebigen Client.</li> <li>3. Um die Anzahl Byte anzuzeigen, die an den Client gesendet wurden, klicken Sie auf die Registerkarte Merkmale.</li> <li>4. Zeigen Sie im Bereich 'Letzte Sitzung' die Zeile 'An Client gesendet' an.</li> </ol> | <p>Wenn Sie auf einen Client in der Tabelle 'Clients' doppelklicken, wird im Bereich Aktivität im Lauf von 2 Wochen das Datenvolumen angezeigt, das vom Client jeden Tag an den Server gesendet wurde.</p> <p>Überprüfen Sie in regelmäßigen Abständen die SQL-Aktivitätsübersichtstabelle, die statistische Daten zu Clientsitzungen enthält. Um die aktuelle Aktivität mit der vorherigen Aktivität zu vergleichen, verwenden Sie eine Anweisung SQL SELECT. Wenn der Grad an Aktivität sich deutlich von dem für die vorherige Aktivität unterscheidet, kann dies eine Ransomware-Attacke anzeigen.</p> <p>Überprüfen Sie das Aktivitätenprotokoll in regelmäßigen Abständen. Suchen Sie nach ANE-Nachrichten, die angeben, wie viele Dateien gesichert und überprüft wurden. Vergleichen Sie die aktuellen Dateneduplizierungsraten mit den vorherigen Raten. Wenn eine ungewöhnlich hohe Anzahl Dateien gesichert wurde oder die Dateneduplizierungsrate wider Erwarten auf 0 fällt, kann dies eine Ransomware-Attacke anzeigen.</p> |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung   |
|---|--|--|
| <p>Überwachen Sie das Speicherpoolwachstum im Laufe der Zeit.</p> | <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Pools'.</li> <li>2. Um die Kapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie einen Pool aus und klicken Sie auf Details.</li> </ol> | <p>Tipps:</p> <ul style="list-style-type: none"> <li>• Um die Zeit anzugeben, die verstreichen muss, bevor alle deduplizierten Speicherbereiche aus einem Verzeichniscontainerspeicherpool oder einem Cloud-Containerspeicherpool entfernt werden, nachdem sie nicht mehr vom Bestand referenziert werden, führen Sie die folgenden Schritte aus: <ol style="list-style-type: none"> <li>1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus.</li> <li>2. Klicken Sie auf Details &gt; Merkmale.</li> <li>3. Geben Sie im Feld<br/>Verzögerungszeitraum für Containerwiederverwendung den Zeitraum an.</li> </ol> </li> <li>• Bestimmen Sie die Dateneduplizierungsleistung für Verzeichniscontainer- und Cloud-Containerspeicherpools mithilfe des Befehls GENERATE DEDUPSTATS.</li> <li>• Um Deduplizierungsstatistikdaten für einen Speicherpool anzuzeigen, führen Sie die folgenden Schritte aus: <ol style="list-style-type: none"> <li>1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus.</li> <li>2. Klicken Sie auf Details &gt; Merkmale.</li> </ol> </li> </ul> <p>Verwenden Sie dementsprechend den Befehl QUERY EXTENTUPDATES, um Informationen zu Aktualisierungen an Datenbereichen in Verzeichniscontainer- oder Cloud-Containerspeicherpools anzuzeigen. Anhand der Befehlsausgabe können Sie die Datenbereiche bestimmen, die nicht mehr referenziert werden, sowie die Datenbereiche, die zum Löschen vom System auswählbar sind. Überwachen Sie in der Ausgabe die Anzahl Datenbereiche, die zum Löschen vom System auswählbar sind. Diese Messgröße steht in direkten Zusammenhang mit dem Umfang des freien Speicherbereichs, der im Containerspeicherpool verfügbar ist.</p> <ul style="list-style-type: none"> <li>• Um den Umfang des physischen Speicherbereichs anzuzeigen, der von einem Dateibereich nach dem Entfernen der Dateneduplizierungseinsparungen belegt wird, verwenden Sie den Befehl select * from occupancy. Die Befehlsausgabe umfasst den Wert für LOGICAL_MB. LOGICAL_MB gibt an, wie viel Speicherbereich von diesem Dateibereich belegt wird.</li> </ul> |



| Task   | Basisprozeduren   | Erweiterte Prozeduren und Fehlerbehebung   |
|--|---|--|
| Überwachen und verwalten Sie Bandeinheiten.  | <p>Überwachen Sie Ihre Umgebung auf Hardwarefehler auf Bandlaufwerken und in Bandarchiven. Anweisungen finden Sie in Bandalernachrichten auf Hardwarefehler überwachen.</p> <p>Überwachen Sie die Datenträgerkompatibilität, um Fehler auf Bandlaufwerken zu verhindern. Anweisungen finden Sie in Durch Datenträgerinkompatibilität verursachte Fehler verhindern.</p> <p>Überwachen Sie Reinigungsnachrichten für Bandlaufwerke. Anweisungen finden Sie in Operationen mit Reinigungskassetten.</p> |  |
| Werten Sie das Timing von Clientzeitplänen aus. Stellen Sie sicher, dass sich die Start- und Endzeiten von Clientzeitplänen nicht mit denen von Serververwaltungstasks überschneiden. Begrenzen Sie die Zeit für Clientsicherungsoperationen auf 8 bis 12 Stunden. | <p>Klicken Sie auf der Seite Übersicht im Operations Center auf Clients &gt; Zeitpläne.</p> <p>In der Tabelle 'Zeitpläne' wird in der Spalte 'Start' die konfigurierte Startzeit für die geplante Operation angezeigt. Um anzuzeigen, wann die letzte Operation gestartet wurde, bewegen Sie den Mauszeiger über das Uhrsymbol.</p>   | <p>Tipp: Wenn die Ausführung einer Clientoperation länger als erwartet dauert, empfangen Sie unter Umständen eine Warnung. Führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite 'Übersicht' im Operations Center den Mauszeiger über Clients und klicken Sie auf Zeitpläne.</li> <li>2. Wählen Sie einen Zeitplan aus und klicken Sie auf Details.</li> <li>3. Zeigen Sie die Details eines Zeitplans an, indem Sie auf den blauen Pfeil neben der Zeile klicken.</li> <li>4. Geben Sie im Feld Ausführungszeitalter die Uhrzeit an, zu der eine Warnung ausgegeben wird, wenn die geplante Operation nicht ausgeführt wird.</li> <li>5. Klicken Sie auf Sichern.</li> </ol>   |
| Werten Sie das Timing von Verwaltungstasks aus. Stellen Sie sicher, dass sich die Start- und Endzeiten von Verwaltungstasks nicht mit denen von Clientzeitplänen überschneiden.  | <p>Klicken Sie auf der Seite Übersicht im Operations Center auf Server &gt; Verwaltung.</p> <p>Überprüfen Sie in der Tabelle 'Verwaltung' die Informationen in der Spalte 'Letzte Ausführungsdauer'. Um anzuzeigen, wann die letzte Verwaltungstask gestartet wurde, bewegen Sie den Mauszeiger über das Uhrsymbol.</p>   | <p>Bei der bevorzugten Methode wird sichergestellt, dass jede Verwaltungstask bis zum Abschluss ausgeführt wird, bevor die nächste Verwaltungstask gestartet wird. Beispiele für Verwaltungstasks umfassen Bestandsverfall, Kopieren von Speicherpools, Speicherbereichskonsolidierung und Datenbanksicherung.</p> <p>Tipp: Wenn die Ausführung einer Verwaltungstask zu lange dauert, ändern Sie die Startzeit oder die maximale Ausführungszeit. Führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder.</li> <li>2. Um die Startzeit oder die maximale Ausführungszeit für eine Task zu ändern, geben Sie den Befehl UPDATE SCHEDULE aus. Informationen zu diesem Befehl finden Sie in UPDATE SCHEDULE (Clientzeitplan aktualisieren).</li> </ol> |

- Bandalernachrichten auf Hardwarefehler überwachen  
Bandalernachrichten werden von Band- und Speicherarchiveinheiten generiert, um Hardwarefehler zurückzumelden. Diese Nachrichten unterstützen Sie bei der Bestimmung von Fehlern, die sich nicht auf den IBM Spectrum Protect-Server beziehen.
- Durch Datenträgerinkompatibilität verursachte Fehler verhindern  
Indem Datenträgerkompatibilitätsprobleme überwacht und behoben werden, können Sie Fehler in einer bandbasierten Lösung in

IBM Spectrum Protect verhindern. Ein neues Laufwerk hat möglicherweise nur eingeschränkt die Fähigkeit zur Verwendung der von einer vorherigen Version des Laufwerks unterstützten Datenträgerformate. Häufig kann ein neues Laufwerk Daten mit dem vorherigen Datenträgerformat lesen, aber nicht schreiben.

- Operationen mit Reinigungskassetten  
Um sicherzustellen, dass Bandlaufwerke wie erforderlich gereinigt werden, und um Probleme mit Bandspeicher zu verhindern, müssen Sie die Richtlinien beachten.

## Bandalernachrichten auf Hardwarefehler überwachen

---

Bandalernachrichten werden von Band- und Speicherarchiveinheiten generiert, um Hardwarefehler zurückzumelden. Diese Nachrichten unterstützen Sie bei der Bestimmung von Fehlern, die sich nicht auf den IBM Spectrum Protect-Server beziehen.

### Informationen zu diesem Vorgang

---

Es wird eine Protokollseite erstellt, die jederzeit oder zu einem bestimmten Zeitpunkt, beispielsweise wenn ein Laufwerk abgehängt wird, abgerufen werden kann.

Eine Bandalernachricht kann eine der folgenden Bewertungsstufen haben:

- Information (beispielsweise wird versucht, einen nicht unterstützten Kassettentyp einzulegen)
- Warnung (beispielsweise wird ein Hardwarefehler vorhergesagt)
- Kritisch (beispielsweise liegt ein Bandfehler vor und Ihre Daten sind gefährdet)

Bandalernachrichten sind standardmäßig inaktiviert.

### Vorgehensweise

---

- Um Bandalernachrichten zu aktivieren, geben Sie den Befehl SET TAPEALERTMSG unter Angabe des Werts ON aus: `set tapealertmsg on`
- Um zu überprüfen, ob Bandalernachrichten aktiviert sind, geben Sie den Befehl QUERY TAPEALERTMSG aus: `query tapealertmsg`

## Durch Datenträgerinkompatibilität verursachte Fehler verhindern

---

Indem Datenträgerkompatibilitätsprobleme überwacht und behoben werden, können Sie Fehler in einer bandbasierten Lösung in IBM Spectrum Protect verhindern. Ein neues Laufwerk hat möglicherweise nur eingeschränkt die Fähigkeit zur Verwendung der von einer vorherigen Version des Laufwerks unterstützten Datenträgerformate. Häufig kann ein neues Laufwerk Daten mit dem vorherigen Datenträgerformat lesen, aber nicht schreiben.

### Informationen zu diesem Vorgang

---

Standardmäßig verbleiben vorhandene Datenträger mit dem Status `FILLING` nach einem Laufwerkupgrade in diesem Status. In einigen Fällen möchten Sie vielleicht ein älteres Laufwerk weiterhin nutzen, um diese Datenträger mit Daten zu füllen. Dadurch bleibt die Schreib-/Leseunktionalität für die vorhandenen Datenträger erhalten, bis sie konsolidiert werden. Wenn für alle Laufwerke in einem Speicherarchiv ein Upgrade durchgeführt werden soll, stellen Sie sicher, dass die Datenträgerformate von der neuen Hardware unterstützt werden. Wenn nicht ausschließlich die neuesten Datenträger mit dem neuen Laufwerk verwendet werden sollen, müssen Sie sich aller Kompatibilitätsprobleme bewusst sein. Anweisungen zum Umlagern von Daten finden Sie in Daten in Laufwerke umlagern, für die ein Upgrade durchgeführt wurde.

Um ein neues Laufwerk mit Datenträgern zu verwenden, von denen Daten gelesen, auf die aber keine Daten geschrieben werden können, geben Sie den Befehl `UPDATE VOLUME` aus, um Lesezugriff für diese Datenträger festzulegen. Damit wird verhindert, dass durch Schreib-/Leseinkompatibilität Fehler auftreten. Beispielsweise kann ein neues Laufwerk unter Umständen Datenträger, auf die Daten in einem von dem Laufwerk nicht unterstützten Format geschrieben wurden, ausgeben, sobald die Datenträger in das Laufwerk geladen werden. Es kann auch vorkommen, dass ein neues Laufwerk den ersten Schreibbefehl nicht für einen Datenträger ausführt, der teilweise in einem Format beschrieben ist, das von dem Laufwerk nicht unterstützt wird.

Wenn Daten auf dem Datenträger mit Lesezugriff verfallen und der Datenträger konsolidiert wird, ersetzen Sie ihn durch einen Datenträger, der mit dem neuen Laufwerk vollständig kompatibel ist. Fehler können generiert werden, wenn ein neues Laufwerk einen in einem älteren Format beschriebenen Datenträger nicht korrekt kalibrieren kann. Um dieses Problem zu verhindern, stellen Sie sicher, dass das ursprüngliche Laufwerk voll funktionsfähig ist und über aktuelle Mikrocodeversionen verfügt.

## Operationen mit Reinigungskassetten

---

Um sicherzustellen, dass Bandlaufwerke wie erforderlich gereinigt werden, und um Probleme mit Bandspeicher zu verhindern, müssen Sie die Richtlinien beachten.

#### Reinigungsprozess überwachen

Wenn eine Reinigungskassette in ein Speicherarchiv zurückgestellt wird und ein Laufwerk gereinigt werden muss, hebt der Server die Bereitstellung des Datenträgers auf und führt die Reinigungsoperation aus. Wenn die Reinigungsoperation fehlschlägt oder wenn sie abgebrochen wird oder wenn keine Reinigungskassette verfügbar ist, sind Sie sich der Tatsache, dass das Laufwerk gereinigt werden muss, möglicherweise nicht bewusst. Überwachen Sie Reinigungsnachrichten auf diese Probleme, um sicherzustellen, dass Laufwerke wie erforderlich gereinigt werden. Geben Sie, falls erforderlich, den Befehl CLEAN DRIVE aus, damit der Server den Reinigungsversuch wiederholt, oder laden Sie manuell eine Reinigungskassette in das Laufwerk.

#### Mehrere Reinigungskassetten verwenden

Der Server verwendet eine Reinigungskassette für die Anzahl Reinigungen, die Sie beim Zurückstellen der Reinigungskassette angeben. Wenn Sie zwei oder mehr Reinigungskassetten zurückstellen, verwendet der Server nur eine der Kassetten, bis die angegebene Anzahl Reinigungen für diese Kassette erreicht ist. Dann verwendet der Server die nächste Reinigungskassette. Wenn Sie zwei oder mehr Reinigungskassetten zurückstellen und zwei oder mehr Befehle CLEAN DRIVE gleichzeitig ausgegeben, verwendet der Server mehrere Kassetten gleichzeitig und verringert die verbleibenden Reinigungen auf jeder Kassette.

#### Zugehörige Verweise:

- 🔗 AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Speicherarchiv prüfen)
- 🔗 CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
- 🔗 CLEAN DRIVE (Laufwerk reinigen)
- 🔗 LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

#### Zugehörige Informationen:

- 🔗 QUERY LIBVOLUME (Datenträger im Speicherarchiv abfragen)

## Lizenz Einhaltung überprüfen

---

Stellen Sie sicher, dass die Bedingungen Ihrer Lizenzvereinbarung von Ihrer IBM Spectrum Protect-Lösung eingehalten werden. Indem die Einhaltung regelmäßig überprüft wird, können Sie Trends beim Datenwachstum oder der PVU-Nutzung verfolgen. Planen Sie anhand dieser Informationen den weiteren Kauf von Lizenzen.

## Informationen zu diesem Vorgang

---

Die Methode zur Überprüfung der Einhaltung der Lizenzbedingungen durch Ihre Lösung variiert abhängig von den Bedingungen Ihrer IBM Spectrum Protect-Lizenzvereinbarung.

#### Front-End-Kapazitätslizenzierung

Das Front-End-Modell bestimmt die Lizenzvoraussetzungen auf der Basis des zurückgemeldeten Volumens an primären Daten, das von Clients gesichert wird. Clients umfassen Anwendungen, virtuelle Maschinen und Systeme.

#### Back-End-Kapazitätslizenzierung

Das Back-End-Modell bestimmt Lizenzvoraussetzungen auf der Basis der Terabyte Daten, die in primären Speicherpools und Repositories gespeichert werden.

Tipps:

- Um die Genauigkeit von Schätzungen der Front-End- und Back-End-Kapazität zu gewährleisten, installieren Sie die neueste Version der Client-Software auf jedem Clientknoten.
- Die Informationen zur Front-End- und Back-End-Kapazität im Operations Center dienen zum Zweck der Planung und Schätzung.

#### PVU-Lizenzierung

Das PVU-Modell basiert auf der Nutzung von PVUs durch Servereinheiten.

Wichtig: Die von IBM Spectrum Protect bereitgestellten PVU-Berechnungen werden als Schätzungen betrachtet und sind nicht rechtsverbindlich. Die von IBM Spectrum Protect zurückgemeldeten PVU-Lizenzinformationen werden nicht als zulässiger Ersatz für das IBM® License Metric Tool angesehen.



Die neuesten Informationen zu Lizenzierungsmodellen finden Sie in den Informationen zu Produktdetails und Lizenzen auf der Website der IBM Spectrum Protect-Produktfamilie. Wenden Sie sich bei Fragen oder Problemstellungen zu Lizenzierungsanforderungen an Ihren IBM Spectrum Protect-Software-Provider.

## Vorgehensweise

---

Führen Sie zur Überwachung der Lizenz Einhaltung die Schritte aus, die den Bedingungen Ihrer Lizenzvereinbarung entsprechen.

Tipp: Das Operations Center stellt einen E-Mail-Bericht bereit, in dem die Front-End- und Back-End-Kapazitätsnutzung zusammengefasst sind. Berichte können automatisch regelmäßig an einen oder mehrere Empfänger gesendet werden. Klicken Sie für die Konfiguration und Verwaltung von E-Mail-Berichten in der Menüleiste des Operations Center auf Berichte.

| Option                  | Bezeichnung   |
|-------------------------|---|
| <b>Front-End-Modell</b> | <p>a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen  und klicken Sie auf Lizenzierung.</p> <p>Die Schätzung der Front-End-Kapazität wird auf der Seite 'Front-End-Nutzung' angezeigt.</p> <p>b. Wenn in der Spalte 'Keine Zurückmeldung' ein Wert angezeigt wird, klicken Sie auf die Zahl, um Clients zu identifizieren, von denen keine Kapazitätsnutzung zurückgemeldet wurde.</p> <p>c. Um die Kapazität für Clients zu schätzen, für die keine Kapazitätsnutzung zurückgemeldet wurde, rufen Sie die folgende FTP-Site auf, auf der Tools und Anweisungen zum Messen der Kapazität bereitgestellt werden:</p> <p><code>ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools</code></p> <p>Um die Front-End-Kapazität mithilfe eines Scripts zu messen, führen Sie die Anweisungen im aktuellen Lizenzierungshandbuch aus.</p> <p>d. Addieren Sie den Operations Center-Schätzwert und alle Schätzwerte, die Sie mithilfe eines Scripts ermittelt haben.</p> <p>e. Überprüfen Sie, ob die geschätzte Kapazität die Bedingungen Ihrer Lizenzvereinbarung einhält.</p> |
| <b>Back-End-Modell</b>  | <p>Einschränkung: Wenn der Quellen- und der Zielreplikationsserver nicht dieselben Maßnahmeneinstellungen verwenden, können Sie das Operations Center nicht zur Überwachung der Back-End-Kapazitätsnutzung für replizierte Clients verwenden. Informationen zur Schätzung der Kapazitätsnutzung für diese Clients finden Sie in Technote 1656476.</p> <p>a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen  und klicken Sie auf Lizenzierung.</p> <p>b. Klicken Sie auf die Registerkarte Back-End.</p> <p>c. Überprüfen Sie, ob das geschätzte Datenvolumen die Bedingungen Ihrer Lizenzvereinbarung einhält.</p>   |
| <b>PVU-Modell</b>       | <p>Informationen zur Vorgehensweise beim Prüfen der Einhaltung der PVU-Lizenzbedingungen finden Sie in Einhaltung des PVU-Lizenzierungsmodells prüfen.</p>  |

## Systemstatus mithilfe von E-Mail-Berichten verfolgen

Konfigurieren Sie das Operations Center für die Generierung von E-Mail-Berichten zur Zusammenfassung des Systemstatus. Sie können eine Mail-Server-Verbindung konfigurieren, Berichtseinstellungen ändern und wahlweise angepasste SQL-Berichte erstellen.

### Vorbereitende Schritte

Bevor Sie E-Mail-Berichte konfigurieren, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- Es ist ein SMTP-Host-Server (SMTP = Simple Mail Transfer Protocol) verfügbar, um Berichte als E-Mail senden und empfangen zu können. Der SMTP-Server muss als offenes Mail-Relay konfiguriert sein. Außerdem müssen Sie sicherstellen, dass der IBM Spectrum Protect-Server, der E-Mail-Nachrichten sendet, Zugriff auf den SMTP-Server hat. Wenn das Operations Center auf einem anderen Computer installiert ist, ist für diesen Computer kein Zugriff auf den SMTP-Server erforderlich.
- Um E-Mail-Berichte konfigurieren zu können, müssen Sie über Systemberechtigung für den Server verfügen.
- Um die Empfänger anzugeben, können Sie eine oder mehrere E-Mail-Adressen oder Administrator-IDs eingeben. Wenn eine Administrator-ID eingegeben werden soll, muss die ID auf dem Hub-Server registriert sein und der ID muss eine E-Mail-Adresse zugeordnet sein. Eine E-Mail-Adresse für einen Administrator können Sie mithilfe des Parameters EMAILADDRESS im Befehl UPDATE ADMIN angeben.

### Informationen zu diesem Vorgang

Sie können das Operations Center zum Senden eines Berichts über allgemeine Operationen, eines Lizenzeinhaltungsberichts und eines oder mehrerer angepasster Berichte, die SQL-Anweisungen SELECT zum Abfragen verwalteter Server verwenden, konfigurieren.

## Vorgehensweise

---

Um E-Mail-Berichte zu konfigurieren und zu verwalten, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Menüleiste des Operations Center auf Berichte.
2. Wenn noch keine E-Mail-Server-Verbindung konfiguriert ist, klicken Sie auf Mail-Server konfigurieren und füllen Sie die Felder aus. Nach der Konfiguration des Mail-Servers sind der Bericht über allgemeine Operationen und der Lizenzinhaltsbericht aktiviert.
3. Um Berichtseinstellungen zu ändern, wählen Sie einen Bericht aus, klicken Sie auf Details und aktualisieren Sie das Formular.
4. Optional: Um einen angepassten SQL-Bericht hinzuzufügen, klicken Sie auf + Bericht und füllen Sie die Felder aus.  
Tipp: Um einen Bericht sofort auszuführen und zu senden, wählen Sie den Bericht aus und klicken Sie auf Senden.

## Ergebnisse

---

Aktivierte Berichte werden gemäß den angegebenen Einstellungen gesendet.

## Nächste Schritte

---

Der Bericht über allgemeine Operationen umfasst eine Anlage. Um detaillierte Informationen anzuzeigen, erweitern Sie die Abschnitte in der Anlage.

Wenn Sie das Image in einem Bericht nicht anzeigen können, verwenden Sie möglicherweise einen E-Mail-Client, der HTML in ein anderes Format konvertiert. Informationen zu Einschränkungen finden Sie in der Onlinehilfe des Operations Center.

## Operationen für eine Bandspeicherlösung verwalten

---

Verwenden Sie diese Informationen, um Operationen für eine Bandspeicherimplementierung für einen IBM Spectrum Protect-Server zu verwalten.

- **Operations Center verwalten**  
Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit.
- **Clientoperationen verwalten**  
Sie können Clientfehler beheben, Client-Upgrades verwalten und Clientknoten, die nicht mehr erforderlich sind, stilllegen. Um Speicherbereich auf dem Server freizugeben, können Sie veraltete Daten, die von Anwendungsclients gespeichert werden, inaktivieren.
- **Datenspeicher verwalten**  
Verwalten Sie Ihre Daten effizient und fügen Sie dem Server unterstützte Einheiten und Datenträger zum Speichern von Clientdaten hinzu.
- **Bandeinheiten verwalten**  
Routinemäßige Bandoperationen umfassen die Vorbereitung von Banddatenträgern für die Verwendung, die Steuerung, wie und wann Datenträger wiederverwendet werden, und die Sicherstellung, dass genügend Datenträger verfügbar sind. Außerdem müssen Sie auf Bedieneranforderungen antworten und Speicherarchive, Laufwerke, Pfade und Einheiten zum Versetzen von Daten verwalten.
- **Bandlaufwerke verwalten**  
Sie können Bandlaufwerke abfragen, aktualisieren und löschen. Außerdem können Sie Bandlaufwerke reinigen und Bandlaufwerkverschlüsselung und Datenprüfung konfigurieren.
- **IBM Spectrum Protect-Server schützen**  
Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.
- **Server stoppen und starten**  
Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.
- **Durchführung eines Upgrades für den Server planen**  
Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.
- **Vorbereitungen für einen Ausfall oder eine Systemaktualisierung**  
Treffen Sie Vorbereitungen in IBM Spectrum Protect, damit Ihr System während eines geplanten Stromausfalls oder einer geplanten Systemaktualisierung in einem konsistenten Zustand verbleibt.
- **Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM**  
IBM Spectrum Protect stellt die Funktion Disaster Recovery Manager (DRM) für die Wiederherstellung Ihrer Server- und Clientdaten bei einem Katastrophenfall zur Verfügung.

## Operations Center verwalten

---

Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit.

### Informationen zu diesem Vorgang

---

Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt. Weitere Informationen zur Verwaltung des Operations Center finden Sie in [Operations Center verwalten](#).

## Clientoperationen verwalten

---

Sie können Clientfehler beheben, Client-Upgrades verwalten und Clientknoten, die nicht mehr erforderlich sind, stilllegen. Um Speicherbereich auf dem Server freizugeben, können Sie veraltete Daten, die von Anwendungsclients gespeichert werden, inaktivieren.

### Informationen zu diesem Vorgang

---

In einigen Fällen können Clientfehler behoben werden, indem der Clientakzeptor gestoppt und gestartet wird. Wenn Clientknoten oder Administrator-IDs gesperrt sind, können Sie das Problem beheben, indem Sie den Clientknoten bzw. die Administrator-ID entsperren und dann das Kennwort zurücksetzen.

Ausführliche Anweisungen zum Identifizieren und Beheben von Clientfehlern finden Sie in [Clientprobleme lösen](#).

Anweisungen zum Hinzufügen von Clients finden Sie in [Anwendungen und Systeme schützen](#).

- Fehler in Clientfehlerprotokollen auswerten  
Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.
- Clientakzeptor stoppen und erneut starten  
Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.
- Kennwörter zurücksetzen  
Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.
- Client-Upgrades verwalten  
Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.
- Clientknoten stilllegen  
Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.
- Daten zum Freigeben von Speicherbereich inaktivieren  
In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegebenen Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

## Fehler in Clientfehlerprotokollen auswerten

---

Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.

### Vorbereitende Schritte

---

(Optional) Um Fehler in einem Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem zu beheben, stellen Sie sicher, dass der Clientverwaltungsservice installiert und gestartet wurde. Installationsanweisungen finden Sie in [Clientverwaltungsservice installieren](#).

### Vorgehensweise

---

Um Clientfehler zu diagnostizieren und zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn der Clientverwaltungsservice auf dem Clientknoten installiert ist, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Details.
  3. Klicken Sie auf der Seite 'Zusammenfassung' auf die Registerkarte Diagnose.
  4. Überprüfen Sie die abgerufenen Protokollnachrichten.  
Tipps:
    - Um das Fenster 'Clientprotokolle' ein- oder auszublenden, doppelklicken Sie auf den Rahmen des Fensters 'Clientprotokolle'.
    - Um die Größe des Fensters 'Clientprotokolle' zu ändern, klicken Sie auf den Rahmen des Fensters 'Clientprotokolle' und ziehen Sie den Rahmen.

Wenn auf der Seite 'Diagnose' Vorschläge angezeigt werden, wählen Sie einen Vorschlag aus. Im Fenster 'Clientprotokolle' sind die Clientprotokollnachrichten, auf die sich der Vorschlag bezieht, hervorgehoben.
- 5. Lösen Sie die in den Fehlernachrichten angegebenen Probleme mithilfe der Vorschläge.  
Tipp: Vorschläge werden nur für einen Teil der Clientnachrichten bereitgestellt.
- Wenn der Clientverwaltungsservice nicht auf dem Clientknoten installiert ist, überprüfen Sie die Fehlerprotokolle für den installierten Client.

## Clientakzeptor stoppen und erneut starten

---

Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.

### Informationen zu diesem Vorgang

---

In einigen Fällen können Clientzeitplanungsprobleme behoben werden, indem der Clientakzeptor gestoppt und erneut gestartet wird. Der Clientakzeptor muss aktiv sein, um sicherzustellen, dass geplante Operationen auf dem Client ausgeführt werden können. Wenn Sie beispielsweise die IP-Adresse oder den Domännennamen des Servers ändern, müssen Sie den Clientakzeptor erneut starten.

### Vorgehensweise

---

Führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

AIX und Oracle Solaris

- Um den Clientakzeptor zu stoppen, führen Sie die folgenden Schritte aus:
  - a. Bestimmen Sie die Prozess-ID für den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

```
ps -ef | grep dsmcad
```

Überprüfen Sie die Ausgabe. In der folgenden Beispielausgabe lautet die Prozess-ID für den Clientakzeptor 6764:

```
root 6764 1 0 16:26:35 ? 0:00 /usr/bin/dsmcad
```

- b. Geben Sie in der Befehlszeile den folgenden Befehl aus:

```
kill -9 PID
```

Dabei gibt *PID* die Prozess-ID für den Clientakzeptor an.

- Um den Clientakzeptor zu starten, geben Sie in der Befehlszeile den folgenden Befehl aus:

```
/usr/bin/dsmcad
```

Linux

- Um den Clientakzeptor zu stoppen, ohne ihn erneut zu starten, geben Sie den folgenden Befehl aus:

```
# service dsmcad stop
```

- Um den Clientakzeptor zu stoppen und erneut zu starten, geben Sie den folgenden Befehl aus:

```
# service dsmcad restart
```

MAC OS X

Klicken Sie auf Applications > Utilities > Terminal.

- Um den Clientakzeptor zu stoppen, geben Sie den folgenden Befehl aus:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Um den Clientakzeptor zu starten, geben Sie den folgenden Befehl aus:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

#### Windows

- Um den Clientakzeptorservice zu stoppen, führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf Start > Verwaltung > Dienste.
  - b. Doppelklicken Sie auf den Clientakzeptorservice.
  - c. Klicken Sie auf Beenden und OK.
- Um den Clientakzeptorservice erneut zu starten, führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf Start > Verwaltung > Dienste.
  - b. Doppelklicken Sie auf den Clientakzeptorservice.
  - c. Klicken Sie auf Starten und OK.

#### Zugehörige Verweise:

 Fehler für Clientzeitplanung beheben

## Kennwörter zurücksetzen

---

Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.

## Vorgehensweise

---

Um Kennwortprobleme zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn ein Client für Sichern/Archivieren auf einem Clientknoten installiert ist und das Kennwort verloren gegangen ist oder Sie das Kennwort vergessen haben, führen Sie die folgenden Schritte aus:

1. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

```
update node Knotenname neues_Kennwort forcepwreset=yes
```

Dabei gibt *Knotenname* den Clientknoten und *neues\_Kennwort* das Kennwort an, das Sie zuordnen.

2. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.

Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf generate gesetzt haben.

- Wenn ein Administrator aufgrund von Kennwortproblemen ausgesperrt ist, führen Sie die folgenden Schritte aus:
  1. Um dem Administrator den Zugriff auf den Server zu ermöglichen, geben Sie den Befehl UNLOCK ADMIN aus. Anweisungen finden Sie in UNLOCK ADMIN (Administrator entsperren).
  2. Legen Sie mit dem Befehl UPDATE ADMIN ein neues Kennwort fest:

```
update admin Administratorname neues_Kennwort forcepwreset=yes
```

Dabei gibt *Administratorname* den Namen des Administrators und *neues\_Kennwort* das Kennwort an, das Sie zuordnen.

- Wenn ein Clientknoten gesperrt ist, führen Sie die folgenden Schritte aus:
  1. Bestimmen Sie, warum der Clientknoten gesperrt ist und ob er entsperret werden muss. Wenn beispielsweise der Clientknoten stillgelegt ist, wird der Clientknoten aus der Produktionsumgebung entfernt. Sie können die Stilllegungsoperation nicht zurücknehmen und der Clientknoten bleibt gesperrt. Ein Clientknoten kann auch gesperrt sein, wenn die Clientdaten Gegenstand einer rechtlichen Untersuchung sind.
  2. Verwenden Sie zum Entsperren eines Clientknotens den Befehl UNLOCK NODE. Anweisungen finden Sie in UNLOCK NODE (Clientknoten entsperren).
  3. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

```
update node Knotenname neues_Kennwort forcepwreset=yes
```

Dabei gibt *Knotenname* den Namen des Knotens und *neues\_Kennwort* das Kennwort an, das Sie zuordnen.

4. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.



Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf generate gesetzt haben.

## Client-Upgrades verwalten

Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.

### Vorbereitende Schritte

1. Überprüfen Sie die Voraussetzungen für die Client/Server-Kompatibilität in Technote 1053218. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden.
2. Überprüfen Sie die Systemvoraussetzungen für den Client in IBM Spectrum Protect Supported Operating Systems.
3. Wenn die Lösung Speicheragenten oder Speicherarchivclients umfasst, überprüfen Sie die Informationen zur Kompatibilität von Speicheragenten bzw. Speicherarchivclients mit Servern, die als Speicherarchivmanager konfiguriert sind. Siehe Technote 1302789.

Wenn Sie planen, ein Upgrade für einen Speicherarchivmanager und einen Speicherarchivclient durchzuführen, müssen Sie zuerst das Upgrade für den Speicherarchivmanager durchführen.

### Vorgehensweise

Um ein Software-Upgrade durchzuführen, führen Sie die in der folgenden Tabelle aufgelisteten Anweisungen aus.

| Software  | Link zu Anweisungen   |
|---|---|
| IBM Spectrum Protect-Client für Sichern/Archivieren   | <ul style="list-style-type: none"><li>• Clientaktualisierungen planen</li></ul>   |
| IBM Spectrum Protect Snapshot                         | <ul style="list-style-type: none"><li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen</li><li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen</li><li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen</li></ul>  |
| IBM Spectrum Protect for Databases                    | <ul style="list-style-type: none"><li>• Upgrade für Data Protection for SQL Server durchführen</li><li>• Installation von Data Protection for Oracle</li><li>• Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li></ul>   |
| IBM Spectrum Protect for Enterprise Resource Planning | <ul style="list-style-type: none"><li>• Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 durchführen</li><li>• Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle durchführen</li></ul>  |
| IBM Spectrum Protect for Mail                         | <ul style="list-style-type: none"><li>• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0)</li><li>• Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0)</li><li>• Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li></ul> |
| IBM Spectrum Protect for Virtual Environments         | <ul style="list-style-type: none"><li>• Installation und Upgrade für Data Protection for VMware durchführen</li><li>• Data Protection for Microsoft Hyper-V installieren</li></ul>  |

## Clientknoten stilllegen

Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.

## Informationen zu diesem Vorgang

---

Wenn Sie den Stilllegungsprozess starten, sperrt der Server den Clientknoten, um zu verhindern, dass dieser auf den Server zugreift. Dateien, die zu dem Clientknoten gehören, werden nacheinander gelöscht; anschließend wird der Clientknoten gelöscht. Sie können die folgenden Typen von Clientknoten stilllegen:

### Anwendungsclientknoten

Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

### Systemclientknoten

Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

### VM-Clientknoten

Clientknoten virtueller Maschinen bestehen aus einem einzelnen Gasthost in einem Hypervisor. Jede virtuelle Maschine wird als ein Dateibereich dargestellt.

Die einfachste Methode zur Stilllegung eines Clientknotens ist die Verwendung des Operations Center. Der Stilllegungsprozess wird im Hintergrund ausgeführt. Wenn der Client für die Replikation von Clientdaten konfiguriert ist, entfernt das Operations Center den Client automatisch aus der Replikation auf dem Quellen- und dem Zielreplikationsserver, bevor es den Client stilllegt.

Tipp: Sie können einen Clientknoten auch stilllegen, indem Sie den Befehl `DECOMMISSION NODE` oder `DECOMMISSION VM` ausgeben. Diese Methode kann beispielsweise in den folgenden Fällen verwendet werden:

- Um den Stilllegungsprozess für einen späteren Zeitpunkt zu planen oder eine Serie von Befehlen unter Verwendung eines Scripts auszuführen, geben Sie die Ausführung des Stilllegungsprozesses im Hintergrund an.
- Um den Stilllegungsprozess zu Zwecken der Fehlerbehebung zu überwachen, geben Sie die Ausführung des Stilllegungsprozesses im Vordergrund an. Wenn Sie den Prozess im Vordergrund ausführen, müssen Sie warten, bis der Prozess abgeschlossen ist, bevor Sie die Arbeit mit anderen Tasks fortsetzen können.

## Vorgehensweise

---

Führen Sie eine der folgenden Aktionen aus:

- Um einen Client mithilfe des Operations Center im Hintergrund stillzulegen, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Weitere > Stilllegen.
- Um einen Clientknoten mithilfe eines Verwaltungsbefehls stillzulegen, führen Sie eine der folgenden Aktionen aus:
  - Um einen Anwendungs- oder Systemclientknoten im Hintergrund stillzulegen, geben Sie den Befehl `DECOMMISSION NODE` aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

```
decommission node austin
```

- Um einen Anwendungs- oder Systemclientknoten im Vordergrund stillzulegen, geben Sie den Befehl `DECOMMISSION NODE` unter Angabe des Parameters `wait=yes` aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

```
decommission node austin wait=yes
```

- Um eine virtuelle Maschine im Hintergrund stillzulegen, geben Sie den Befehl `DECOMMISSION VM` aus. Wenn beispielsweise die virtuelle Maschine den Namen AUSTIN hat, der Dateibereich 7 ist und der Dateibereichsname über die Dateibereichs-ID angegeben wird, geben Sie den folgenden Befehl aus:

```
decommission vm austin 7 nametype=fsid
```

Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Um eine virtuelle Maschine im Vordergrund stillzulegen, geben Sie den Befehl `DECOMMISSION VM` unter Angabe des Parameters `wait=yes` aus. Geben Sie beispielsweise den folgenden Befehl aus:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

## Nächste Schritte

---

Achten Sie auf Fehlermeldungen, die unter Umständen in der Benutzerschnittstelle oder in der Befehlsausgabe unmittelbar nach der Ausführung des Prozesses angezeigt werden.

Um zu überprüfen, ob der Clientknoten stillgelegt wurde, gehen Sie wie folgt vor:

1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients.
2. Überprüfen Sie in der Tabelle 'Clients' in der Spalte 'Gefährdet' den Status:
  - Der Status 'Stillgelegt' (DECOMMISSIONED) gibt an, dass der Knoten stillgelegt wurde.
  - Ein Nullwert gibt an, dass der Knoten nicht stillgelegt wurde.
  - Der Status 'Anstehend' (PENDING) gibt an, dass der Knoten gerade stillgelegt wird oder der Stilllegungsprozess fehlgeschlagen ist.

Tipp: Wenn der Status eines anstehenden Stilllegungsprozesses bestimmt werden soll, geben Sie den folgenden Befehl aus:

```
query process
```

3. Überprüfen Sie die Befehlsausgabe:
  - Wenn für den Stilllegungsprozess ein Status angegeben ist, ist der Prozess in Bearbeitung. Beispiel:

```
query process
  Prozess-      Prozessbeschreibung      Prozesstatus
  nummer
-----
          3      DECOMMISSION NODE      Anzahl der für Knoten NODE1 inaktivierten
                                          Sicherungsobjekte: 8 Objekte inaktiviert.
```

- Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie keine Fehlermeldung empfangen haben, ist der Prozess unvollständig. Ein Prozess kann unvollständig sein, wenn Dateien, die dem Knoten zugeordnet sind, noch nicht inaktiviert wurden. Führen Sie nach der Inaktivierung der Dateien den Stilllegungsprozess erneut aus.
- Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie eine Fehlermeldung empfangen, ist der Prozess fehlgeschlagen. Führen Sie den Stilllegungsprozess erneut aus.

### Zugehörige Verweise:

- [DECOMMISSION NODE \(Clientknoten stilllegen\)](#)
- [DECOMMISSION VM \(Virtuelle Maschine stilllegen\)](#)

## Daten zum Freigeben von Speicherbereich inaktivieren

---

In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegebenen Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

### Informationen zu diesem Vorgang

---

Einige Anwendungsclients sichern Daten immer als aktive Sicherungsdaten auf dem Server. Da aktive Sicherungsdaten nicht durch die Bestandsverfallsmaßnahmen verwaltet werden, werden die Daten nicht automatisch gelöscht und belegen unbegrenzt Serverspeicher. Um den Speicherbereich freizugeben, der von veralteten Daten belegt wird, können Sie die Daten inaktivieren.

Wenn Sie den Inaktivierungsprozess ausführen, werden alle aktiven Sicherungsdaten, die vor dem angegebenen Datum gespeichert wurden, inaktiv. Die Daten werden gelöscht, sobald sie verfallen, und können nicht zurückgeschrieben werden. Die Inaktivierungsfunktion gilt nur für Anwendungsclients, die Oracle-Datenbanken schützen.

### Vorgehensweise

---

1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients.
2. Wählen Sie in der Tabelle 'Clients' einen oder mehrere Clients aus und klicken Sie auf Weitere > Bereinigen.  
Befehlszeilenmethode: Inaktivieren Sie Daten mit dem Befehl DEACTIVATE DATA.

### Zugehörige Verweise:

- [DEACTIVATE DATA \(Daten für einen Clientknoten inaktivieren\)](#)


## Datenspeicher verwalten

---

Verwalten Sie Ihre Daten effizient und fügen Sie dem Server unterstützte Einheiten und Datenträger zum Speichern von Clientdaten hinzu.

- **Bestandskapazität verwalten**  
Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.
- **Geplante Aktivitäten optimieren**  
Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.
- **Operationen durch Aktivierung der Kollokation von Clientdateien optimieren**  
Die Kollokation von Clientdateien reduziert die Anzahl Datenträgermounts, die erforderlich sind, wenn Benutzer viele Dateien aus einem Speicherpool zurückschreiben, abrufen oder zurückrufen. Die Kollokation reduziert somit die Zeit, die für diese Operationen erforderlich ist.

### Zugehörige Verweise:

 [Speicherpooltypen](#)

## Bestandskapazität verwalten

---

Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.

### Vorbereitende Schritte

---

Die aktive Protokolldatei und das Archivprotokoll haben die folgenden Merkmale:

- Die Größe der aktiven Protokolldatei kann maximal 512 GB betragen. Weitere Informationen zum Festlegen der Größe der aktiven Protokolldatei für Ihr System finden Sie in Planung der Speicherarrays.
- Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist. Die Größe des Archivprotokolls ist im Gegensatz zur Größe der aktiven Protokolldatei nicht auf eine vordefinierte Größe festgelegt. Archivprotokolldateien werden automatisch gelöscht, wenn sie nicht mehr benötigt werden.

Als Best Practice können Sie wahlweise ein Archivübernahmeprotokoll erstellen, in dem Archivprotokolldateien gespeichert werden, wenn das Archivprotokollverzeichnis voll ist.

Bestimmen Sie über das Operations Center, welche Komponente des Bestands voll ist. Stellen Sie sicher, dass der Server gestoppt wird, bevor Sie eine der Bestandskomponenten vergrößern.

### Vorgehensweise

---

- Um den Plattenspeicherplatz für die Datenbank zu vergrößern, führen Sie die folgenden Schritte aus:
  - Erstellen Sie in unterschiedlichen Laufwerken oder Dateisystemen ein oder mehrere Verzeichnisse für die Datenbank.
  - Geben Sie den Befehl `EXTEND DBSPACE` aus, um der Datenbank das Verzeichnis oder die Verzeichnisse hinzuzufügen. Die Instanzbenutzer-ID des Datenbankmanagers muss Zugriff auf die Verzeichnisse haben. Standardmäßig erfolgt eine Neuverteilung der Daten auf alle Datenbankverzeichnisse und eine Konsolidierung des Speicherbereichs.  
Tipps:
    - Die Zeit, die für die vollständige Neuverteilung von Daten und die Konsolidierung von Speicherbereich erforderlich ist, variiert abhängig von der Größe Ihrer Datenbank. Stellen Sie sicher, dass Sie dies bei der Planung berücksichtigen.
    - Stellen Sie sicher, dass die Verzeichnisse, die Sie angeben, dieselbe Größe wie vorhandene Verzeichnisse haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorabesezugriff und zur Verteilung der Datenbank verringert.
  - Stoppen Sie den Server und starten Sie ihn erneut, um die neuen Verzeichnisse vollständig nutzen zu können.
  - Reorganisieren Sie die Datenbank, falls erforderlich. Die Index- und Tabellenreorganisation für die Serverdatenbank kann dazu beitragen, unerwartetes Datenbankwachstum und Leistungsprobleme zu verhindern. Weitere Informationen zur Reorganisation der Datenbank finden Sie in Technote 1683633.
- Informationen zur Verringerung der Größe der Datenbank für Server der Version 7.1 und höher finden Sie in Technote 1683633.  
Einschränkung: Die Befehle können die E/A-Aktivität erhöhen und sich unter Umständen auf die Serverleistung auswirken. Um Leistungsprobleme auf ein Mindestmaß zu reduzieren, warten Sie, bis ein Befehl abgeschlossen ist, bevor Sie den nächsten Befehl ausgeben. Die DB2-Befehle können ausgegeben werden, wenn der Server aktiv ist.

- Um die aktive Protokolldatei zu vergrößern oder zu verkleinern, führen Sie die folgenden Schritte aus:
  - Stellen Sie sicher, dass die Position für die aktive Protokolldatei über genügend Speicherbereich für die erhöhte Protokollgröße verfügt.
  - Stoppen Sie den Server.
  - Aktualisieren Sie in der Datei dmserv.opt die Option ACTIVELOGSIZE mit der neuen Größe der aktiven Protokolldatei (angegeben in Megabyte).  
Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option ACTIVELOGSIZE. Die folgende Tabelle enthält Richtlinien für den Speicherbedarf:

Tabelle 1. Schätzen des Speicherbedarfs für Datenträger und Dateibereiche

| Wert für die Option ACTIVELOGSize | Größe des im Verzeichnis für aktive Protokolldateien zu reservierender freier Speicherbereich zusätzlich zum Speicherbereich für ACTIVELOGSize |
|-----------------------------------|--|
| 16 GB bis 128 GB                  | 5120 MB  |
| 129 GB bis 256 GB                 | 10240 MB   |
| 257 GB bis 512 GB                 | 20480 MB   |

Um die Größe der aktiven Protokolldatei in die maximale Größe von 512 GB zu ändern, geben Sie die folgende Serveroption ein:

```
activelogsize 524288
```

- Wenn Sie planen, ein neues Verzeichnis für aktive Protokolldateien zu verwenden, aktualisieren Sie den in der Serveroption ACTIVELOGDIRECTORY angegebenen Verzeichnisnamen. Das neue Verzeichnis muss leer sein und die Benutzer-ID des Datenbankmanagers muss Zugriff auf dieses Verzeichnis haben.
  - Starten Sie den Server erneut.
- Komprimieren Sie die Archivprotokolle, um die Größe des Speicherbereichs, der zum Speichern benötigt wird, zu reduzieren. Aktivieren Sie die dynamische Komprimierung für das Archivprotokoll, indem Sie den folgenden Befehl ausgeben:

```
setopt archlogcompress yes
```

Einschränkung: Gehen Sie mit Vorsicht vor, wenn Sie die Serveroption ARCHLOGCOMPRESS auf Systemen mit kontinuierlich hoher Datenträgerverwendung und hohen Workloads aktivieren. Ein Aktivieren dieser Option in dieser Systemumgebung kann Verzögerungen beim Archivieren von Protokolldateien aus dem Dateisystem für aktive Protokolldateien in das Dateisystem für Archivprotokolle haben. Diese Verzögerung kann zur Folge haben, dass der Speicherbereich im Dateisystem für aktive Protokolldateien knapp wird. Sie müssen den verfügbaren Speicherbereich im Dateisystem für aktive Protokolldateien überwachen, nachdem die Komprimierung für das Archivprotokoll aktiviert wurde. Wenn für das Dateisystem für das Verzeichnis für aktive Protokolldateien fast kein Speicherbereich mehr verfügbar ist, muss die Serveroption ARCHLOGCOMPRESS inaktiviert werden. Mit dem Befehl SETOPT können Sie die Komprimierung für das Archivprotokoll sofort inaktivieren, ohne den Server stoppen zu müssen.

#### Zugehörige Verweise:

- [Serveroption ACTIVELOGSIZE](#)
- [EXTEND DBSPACE \(Speicherbereich für die Datenbank vergrößern\)](#)
- [SETOPT \(Serveroption für dynamische Aktualisierung definieren\)](#)

## Geplante Aktivitäten optimieren

Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

### Vorgehensweise

- Überwachen Sie die Systemleistung regelmäßig, um sicherzustellen, dass Sicherungs- und Verwaltungstasks erfolgreich ausgeführt werden. Weitere Informationen zur Überwachung finden Sie in Bandspeicherlösung überwachen.
- Wenn die Überwachungsdaten anzeigen, dass sich die Server-Workload erhöht hat, müssen Sie die Planungsinformationen gegebenenfalls überprüfen. Überprüfen Sie, ob die Kapazität des Systems in den folgenden Fällen ausreichend ist:
  - Erhöhung der Anzahl Clients
  - Zunahme des Datenvolumens, das gesichert wird
  - Änderung des Zeitraums, der für Sicherungen verfügbar ist
- Bestimmen Sie, ob für Ihre Lösung Leistungsprobleme vorliegen. Überprüfen Sie die Clientzeitpläne dahingehend, ob Tasks innerhalb des geplanten Zeitrahmens ausgeführt werden:
  - Wählen Sie auf der Seite Clients im Operations Center den Client aus.
  - Klicken Sie auf Details.
  - Überprüfen Sie auf der Seite Zusammenfassung des Clients die für Gesichert und Repliziert angegebene Aktivität, um alle Risiken zu ermitteln.

- Passen Sie, falls erforderlich, den Zeitpunkt und die Häufigkeit für die Ausführung von Clientsicherungsoperationen an.
4. Planen Sie ausreichend Zeit ein, um die folgenden Verwaltungstasks innerhalb von 24 Stunden erfolgreich ausführen zu können:
    - a. Sichern der Datenbank
    - b. Ausführen der Verfallsverarbeitung, um Clientsicherungen und Archivierungsdateikopien aus dem Serverspeicher zu entfernen

**Zugehörige Konzepte:**

Leistung

**Zugehörige Tasks:**

Daten deduplizieren (Version 7.1.1)

## Operationen durch Aktivierung der Kollokation von Clientdateien optimieren

Die Kollokation von Clientdateien reduziert die Anzahl Datenträgermounts, die erforderlich sind, wenn Benutzer viele Dateien aus einem Speicherpool zurückschreiben, abrufen oder zurückrufen. Die Kollokation reduziert somit die Zeit, die für diese Operationen erforderlich ist.

### Informationen zu diesem Vorgang

Bei aktivierter Kollokation versucht der Server, Dateien auf möglichst wenigen Speicherdatenträgern mit sequenziellem Zugriff zu speichern. Die Dateien können zu einem einzelnen Clientknoten, einer Gruppe von Clientknoten, einem Clientdateibereich oder einer Gruppe von Dateibereichen gehören. Sie können die Kollokation für jeden Speicherpool mit sequenziellem Zugriff festlegen, wenn Sie den Pool definieren oder aktualisieren.

Abbildung 1 zeigt ein Beispiel für die Kollokation nach Clientknoten mit drei Clients, von denen jeder über einen separaten Datenträger verfügt, der Daten dieses Clients enthält.

Abbildung 1. Beispiel für die aktivierte Kollokation nach Knoten

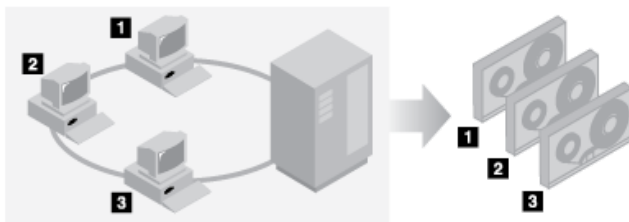


Abbildung 2 zeigt ein Beispiel für die Kollokation nach Clientknotengruppe. Es sind drei Gruppen definiert und die Daten jeder Gruppe werden auf separaten Datenträgern gespeichert.

Abbildung 2. Beispiel für die aktivierte Kollokation nach Knotenkollokationsgruppe

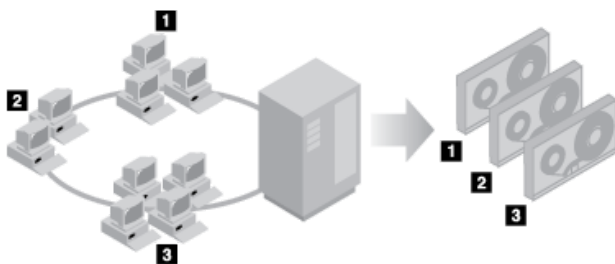
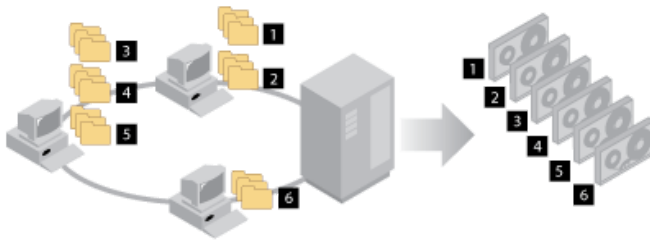


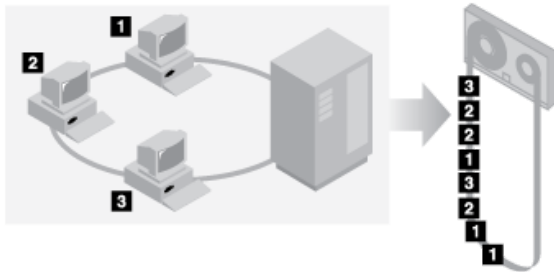
Abbildung 3 zeigt ein Beispiel für die Kollokation nach Dateibereichsgruppe. Es sind sechs Gruppen definiert. Jede Gruppe enthält Daten aus Dateibereichen, die zu einem einzelnen Knoten gehören. Die Daten jeder Gruppe werden auf einem separaten Datenträger gespeichert.

Abbildung 3. Beispiel für die aktivierte Kollokation nach Dateibereichskollokationsgruppe



Bei inaktiverter Kollokation versucht der Server, den gesamten verfügbaren Speicherbereich auf jedem Datenträger zu nutzen, bevor er einen neuen Datenträger auswählt. Dieser Prozess ermöglicht zwar eine bessere Nutzung einzelner Datenträger, Benutzerdateien können jedoch über viele Datenträger verstreut werden. Abbildung 4 zeigt ein Beispiel für die inaktivierte Kollokation mit drei Clients, die den Speicherbereich auf einem einzelnen Datenträger gemeinsam nutzen.

Abbildung 4. Beispiel für die inaktivierte Kollokation



Bei inaktiverter Kollokation sind unter Umständen mehr Datenträgermountoperationen zum Bereitstellen von Datenträgern erforderlich, wenn Benutzer viele Dateien zurückschreiben, abrufen oder zurückrufen.

Die Kollokation nach Gruppe ist der IBM Spectrum Protect-Systemstandardwert für primäre Speicherpools mit sequenziellem Zugriff. Für Kopierspeicherpools erfolgt standardmäßig keine Kollokation.

- Auswirkungen der Kollokation auf Operationen  
Die Auswirkungen der Kollokation auf Ressourcen und die Systemleistung sind vom Typ der Operation abhängig, die ausgeführt wird.
- Datenträger bei aktivierter Kollokation auswählen  
Die Auswahl der Datenträger ist davon abhängig, ob die Kollokation nach Gruppe, nach Knoten oder nach Dateibereich erfolgt.
- Datenträger bei inaktiverter Kollokation auswählen  
Bei inaktiverter Kollokation versucht der Server, den gesamten verfügbaren Speicherbereich in einem Speicherdatenträger zu nutzen, bevor er auf einen neuen Datenträger zugreift.
- Kollokationseinstellungen  
Nach der Definition eines Speicherpools können Sie die Kollokationseinstellung durch Aktualisieren des Speicherpools ändern. Die Änderung der Kollokation für den Pool hat keine Auswirkungen auf Dateien, die bereits in dem Pool gespeichert sind.
- Kollokation von Kopierspeicherpools  
Bei der Verwendung der Kollokation für Kopierspeicherpools müssen bestimmte Hinweise beachtet werden. Die Kollokation von Kopierspeicherpools, insbesondere die Kollokation nach Knoten oder Dateibereich, hat mehr teilweise gefüllte Datenträger und möglicherweise unnötige Konsolidierungsaktivität für ausgelagerte Datenträger zur Folge.
- Kollokation planen und aktivieren  
Zu wissen, welche Auswirkungen die Kollokation hat, kann hilfreich sein, um die Anzahl der Datenträgermounts zu reduzieren, den Speicherbereich auf sequenziellen Datenträgern besser zu nutzen und die Effizienz von Serveroperationen zu verbessern.

## Auswirkungen der Kollokation auf Operationen

Die Auswirkungen der Kollokation auf Ressourcen und die Systemleistung sind vom Typ der Operation abhängig, die ausgeführt wird.

In Tabelle 1 sind die Auswirkungen der Kollokation auf Operationen zusammengefasst.

Tabelle 1. Auswirkungen der Kollokation auf Operationen

| Operation  | Kollokation aktiviert                               | Kollokation inaktiviert                         |
|--|---|---|
| Sichern, Archivieren oder Umlagern von Clientdateien | Mehr Datenträgermounts zum Kollokieren von Dateien. | Es sind weniger Datenträgermounts erforderlich. |

| Operation   | Kollokation aktiviert   | Kollokation inaktiviert   |
|---|---|---|
| Zurückschreiben, Abrufen oder Rückrufen von Clientdateien | Eine große Anzahl Dateien kann schneller zurückgeschrieben, abgerufen oder zurückgerufen werden, da sich die Dateien auf weniger Datenträgern befinden.   | Möglicherweise sind mehrere Datenträgermounts für einen einzelnen Benutzer erforderlich, da Dateien auf mehrere Datenträger verteilt sein können.<br><br>Die Dateien mehrerer Benutzer können auf demselben Speicherdatenträger mit sequenziellem Zugriff gespeichert sein. Wenn beispielsweise zwei Benutzer versuchen, eine Datei wiederherzustellen, die sich auf demselben Datenträger befindet, muss ein Benutzer warten, bis der andere Benutzer seine Dateien wiederhergestellt hat. |
| Speichern von Daten auf Band                              | Der Server versucht, alle verfügbaren Banddatenträger zum Trennen von Benutzerdateien zu verwenden, bevor der gesamte verfügbare Speicherbereich auf jedem Banddatenträger genutzt wird.  | Der Server versucht, den gesamten verfügbaren Speicherbereich auf jedem einzelnen Banddatenträger zu nutzen, bevor ein anderer Banddatenträger verwendet wird.  |
| Datenträgermountoperationen                               | Es sind mehr Mountoperationen erforderlich, wenn Benutzerdateien von Clientknoten direkt auf Datenträger mit sequenziellem Zugriff gesichert, archiviert oder umgelagert werden.<br><br>Während der Konsolidierung und Speicherpoolumlagerung sind mehr Mountoperationen erforderlich.<br><br>Es werden mehr Datenträger verwaltet werden, da Datenträger nicht vollständig genutzt werden. | Während der Zurückschreibung, des Abrufs und des Rückrufs von Clientdateien sind mehr Mountoperationen erforderlich.  |
| Generieren von Sicherungsgruppen                          | Es wird weniger Zeit für die Suche nach Datenbankeinträgen benötigt und es sind weniger Mountoperationen erforderlich.  | Es wird mehr Zeit für die Suche nach Datenbankeinträgen benötigt und es sind weniger Mountoperationen erforderlich.   |

Wenn die Kollokation für eine Gruppe, einen einzelnen Clientknoten oder einen einzelnen Dateibereich aktiviert ist, werden alle Daten, die zu der Gruppe, dem Knoten oder dem Dateibereich gehören, durch einen einzigen Serverprozess versetzt oder kopiert. Wenn beispielsweise Daten nach Gruppe kolloziert werden, werden alle Daten für alle Knoten, die zu derselben Kollokationsgruppe gehören, durch denselben Prozess umgelagert.

Bei der Kollokation von Daten versucht der IBM Spectrum Protect-Server, Dateien auf möglichst wenigen Speicherdatenträgern mit sequenziellem Zugriff zu speichern. Wenn der Server Daten auf Datenträgern in einem Speicherpool mit sequenziellem Zugriff sichert, hat der Sicherungsprozess jedoch Priorität vor den Kollokationseinstellungen. Demzufolge führt der Server die Sicherungsoperation aus, kann aber die Daten möglicherweise nicht kollokieren.

Angenommen, die Kollokation erfolgt nach Knoten und Sie geben an, dass ein Knoten zwei Mountpunkte auf dem Server verwenden kann. Weiterhin sei angenommen, dass die Daten, die von dem Knoten gesichert werden, problemlos auf einen einzigen Banddatenträger passen. Während der Sicherung stellt der Server möglicherweise zwei Banddatenträger bereit und die Daten des Knotens werden möglicherweise auf zwei Bänder verteilt und nicht auf einem einzigen Band gespeichert. Wenn Sie die Kollokation aktivieren, verwenden die folgenden Serveroperationen einen einzigen Serverprozess:

- Versetzen von Daten von Datenträgern mit wahlfreiem Zugriff und sequenziellem Zugriff
- Versetzen von Knotendaten von Datenträgern mit sequenziellem Zugriff
- Sichern eines Speicherpools mit wahlfreiem Zugriff oder sequenziellem Zugriff
- Zurückschreiben eines Speicherpools mit sequenziellem Zugriff
- Konsolidierung von Speicherbereich in einem Speicherpool mit sequenziellem Zugriff oder auf ausgelagerten Datenträgern
- Umlagerung von Daten aus einem Speicherpool mit wahlfreiem Zugriff

Wenn die Umlagerung von Daten aus einem Plattenspeicherpool mit wahlfreiem Zugriff in einen Speicherpool mit sequenziellem Zugriff erfolgt und die Kollokation nach Knoten oder Dateibereich erfolgt, werden Knoten oder Dateibereiche automatisch für die Umlagerung auf der Basis des umzulagernden Datenvolumens ausgewählt. Der Knoten oder Dateibereich mit den meisten Daten wird zuerst umgelagert. Wenn die Kollokation nach Gruppe erfolgt, werden alle Knoten in dem Speicherpool ausgewertet, um den Knoten mit den



meisten Daten zu bestimmen. Der Knoten mit den meisten Daten wird zusammen mit allen Daten für alle Knoten, die zu dieser Kollokationsgruppe gehören, zuerst umgelagert. Dieser Prozess erfolgt unabhängig von dem Datenvolumen, das in den Dateibereichen der Knoten gespeichert ist, und unabhängig davon, ob der untere Umlagerungsschwellenwert erreicht wurde.

Wenn jedoch kollokierte Daten aus einem Speicherpool mit sequenziellem Zugriff in einen anderen Speicherpool mit sequenziellem Zugriff umgelagert werden, ordnet der Server die Datenträger gemäß dem Datum, an dem zuletzt auf den Datenträger zugegriffen wurde. Der Datenträger mit dem frühesten Zugriffsdatum wird zuerst umgelagert und der Datenträger mit dem neuesten Zugriffsdatum wird zuletzt umgelagert.

Ein Grund für die Kollokation nach Gruppe besteht darin, dass einzelne Clientknoten oft nicht über ausreichend Daten verfügen, um Banddatenträger mit hoher Speicherkapazität zu füllen. Durch die Kollokation von Daten nach Gruppen von Knoten kann die nicht verwendete Bandkapazität reduziert werden, indem mehr kollokierte Daten auf einzelnen Bändern gespeichert werden. Durch die Kollokation von Daten nach Gruppen von Dateibereichen wird die nicht verwendete Bandkapazität noch stärker reduziert.

Die Daten, die zu allen Knoten in derselben Kollokationsgruppe gehören, werden durch denselben Prozess umgelagert. Demzufolge kann durch die Kollokation nach Gruppe die Häufigkeit der erforderlichen Mounts für einen Datenträger, der umgelagert werden soll, reduziert werden. Die Kollokation nach Gruppe kann auch das Durchsuchen der Datenbank minimieren und Bandübergaben während der Übertragung von Daten von einem Speicherpool mit sequenziellem Zugriff in einen anderen reduzieren.

## Datenträger bei aktivierter Kollokation auswählen

Die Auswahl der Datenträger ist davon abhängig, ob die Kollokation nach Gruppe, nach Knoten oder nach Dateibereich erfolgt.

Tabelle 1 zeigt, wie der IBM Spectrum Protect-Server den ersten Datenträger auswählt, wenn die Kollokation für einen Speicherpool auf Clientknoten-, Kollokationsgruppen- und Dateibereichsebene aktiviert ist.

Tabelle 1. Wie der Server Datenträger bei aktivierter Kollokation auswählt

| Reihenfolge bei der Auswahl der Datenträger | Bei Kollokation nach Gruppe   | Bei Kollokation nach Knoten   | Bei Kollokation nach Dateibereich   |
|---|---|---|---|
| 1   | Ein Datenträger, der bereits Dateien aus der Kollokationsgruppe enthält, zu der der Client gehört                 | Ein Datenträger, der bereits Dateien desselben Clientknotens enthält  | Ein Datenträger, der bereits Dateien aus demselben Dateibereich dieses Clientknotens enthält                      |
| 2   | Ein leerer vordefinierter Datenträger   | Ein leerer vordefinierter Datenträger   | Ein leerer vordefinierter Datenträger   |
| 3   | Ein leerer Arbeitsdatenträger   | Ein leerer Arbeitsdatenträger   | Ein leerer Arbeitsdatenträger   |
| 4   | Bei Datenträgern, die bereits Daten enthalten, ein Datenträger mit dem meisten verfügbaren freien Speicherbereich | Bei Datenträgern, die bereits Daten enthalten, ein Datenträger mit dem meisten verfügbaren freien Speicherbereich | Ein Datenträger, der Daten desselben Clientknotens enthält  |
| 5   | Nicht zutreffend  | Nicht zutreffend  | Bei Datenträgern, die bereits Daten enthalten, ein Datenträger mit dem meisten verfügbaren freien Speicherbereich |

Wenn der Server das Speichern der Daten auf einem zweiten Datenträger fortsetzen muss, fordert er weiteren Speicherbereich in der folgenden Auswahlreihenfolge an:

1. Ein leerer vordefinierter Datenträger
2. Ein leerer Arbeitsdatenträger
3. Bei Datenträgern, die bereits Daten enthalten, ein Datenträger mit dem meisten verfügbaren freien Speicherbereich
4. Ein beliebiger verfügbarer Datenträger im Speicherpool

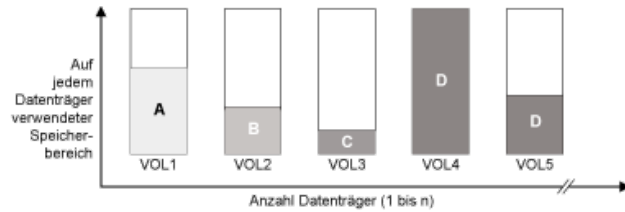
Wenn die Kollokation nach Clientknoten oder Dateibereich erfolgt, versucht der Server, die beste Nutzung einzelner Datenträger zu ermöglichen, und minimiert das Mischen von Dateien von unterschiedlichen Clients oder aus unterschiedlichen Dateibereichen auf Datenträgern. Diese Konfiguration ist in Abbildung 1 dargestellt. Die Abbildung zeigt, dass die Datenträgerauswahl *horizontal* erfolgt, wobei alle verfügbaren Datenträger verwendet werden, bevor der gesamte verfügbare Speicherbereich auf jedem einzelnen Datenträger genutzt wird. A, B, C und D stellen Dateien aus vier verschiedenen Clientknoten dar.

Tipps:

1. Wenn die Kollokation nach Knoten erfolgt und der Knoten mehrere Dateibereiche hat, versucht der Server nicht, diese Dateibereiche zu kollokieren.

2. Wenn die Kollokation nach Dateibereich erfolgt und ein Knoten mehrere Dateibereiche hat, versucht der Server, Daten für verschiedene Dateibereiche auf unterschiedlichen Datenträgern zu speichern.

Abbildung 1. Verwendung aller verfügbaren Speicherdatenträger mit sequenziellem Zugriff bei aktivierter Kollokation auf Knoten- oder Dateibereichsebene

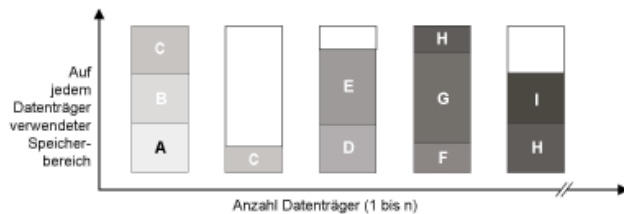


Die Kollokation kann nach Dateibereichsgruppe oder Knotengruppe erfolgen. Wenn die Kollokation nach Knotengruppe (Knotenkollokationsgruppe) erfolgt, versucht der Server, Daten von Knoten, die zu derselben Kollokationsgruppe gehören, zu kollokieren. Eine Dateibereichskollokationsgruppe verwendet dieselben Methoden wie eine Knotenkollokationsgruppe, kann jedoch aufgrund der Granularität der Dateibereichsgrößen mehr Speicherbereich verwenden. Wie in Abbildung 2 gezeigt wurden Daten für die folgenden Gruppen von Knoten kollokiert:

- Gruppe 1 besteht aus Knoten A, B und C.
- Gruppe 2 besteht aus Knoten D und E.
- Gruppe 3 besteht aus Knoten F, G, H und I.

Wenn möglich, kollokiert der IBM Spectrum Protect-Server Daten, die zu einer Gruppe von Knoten gehören, auf einem einzigen Band. Dies ist in der Abbildung durch Gruppe 2 dargestellt. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind (Gruppe 1 und 2). Wenn die Knoten in der Kollokationsgruppe mehrere Dateibereiche haben, versucht der Server nicht, diese Dateibereiche zu kollokieren.

Abbildung 2. Verwendung aller verfügbaren Speicherdatenträger mit sequenziellem Zugriff bei aktivierter Kollokation auf Gruppenebene



Normalerweise schreibt der IBM Spectrum Protect-Server Daten für die aktive Operation immer auf den Datenträger, der gerade gefüllt wird. Gelegentlich kann es jedoch vorkommen, dass sich mehr als ein Datenträger, der mit Daten gefüllt wird, in einem kollokierten Speicherpool befindet. Es kann vorkommen, dass sich mehrere Datenträger, die mit Daten gefüllt werden, in einem kollokierten Speicherpool befinden, wenn verschiedene Serverprozesse oder Clientsitzungen versuchen, Daten gleichzeitig in dem kollokierten Pool zu speichern. In dieser Situation ordnet IBM Spectrum Protect einen Datenträger für jeden Prozess oder jede Sitzung zu, der bzw. die einen Datenträger benötigt, sodass beide Operationen so schnell wie möglich ausgeführt werden.

## Datenträger bei inaktivierter Kollokation auswählen

Bei inaktivierter Kollokation versucht der Server, den gesamten verfügbaren Speicherbereich in einem Speicherdatenträger zu nutzen, bevor er auf einen neuen Datenträger zugreift.

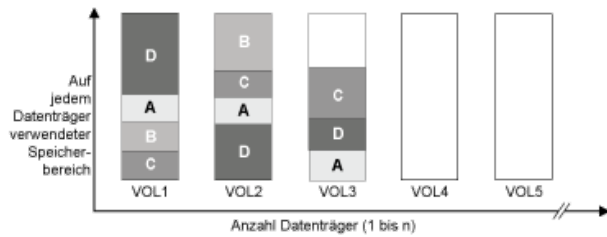
Wenn Sie Clientdateien in einem Speicherpool mit sequenziellem Zugriff speichern, für den die Kollokation inaktiviert ist, erfolgt die Auswahl eines Datenträgers durch den Server in der folgenden Reihenfolge:

1. Ein zuvor verwendeter sequenzieller Datenträger mit verfügbarem Speicherbereich (ein Datenträger mit dem größten Datenvolumen wird zuerst ausgewählt)
2. Ein leerer Datenträger

Wenn der Server das Speichern der Daten auf einem zweiten Datenträger fortsetzen muss, versucht er, einen leeren Datenträger auszuwählen. Wenn kein leerer Datenträger vorhanden ist, versucht der Server, einen der übrigen verfügbaren Datenträger im Speicherpool auszuwählen.

Abbildung 1 zeigt dass die Datenträgerverwendung vertikal erfolgt, wenn die Kollokation inaktiviert ist. In diesem Beispiel werden weniger Datenträger verwendet, da der Server versucht, den gesamten verfügbaren Speicherbereich durch Mischen von Clientdateien auf einzelnen Datenträgern zu nutzen. A, B, C und D stellen Dateien aus vier verschiedenen Clientknoten dar.

Abbildung 1. Verwendung des gesamten verfügbaren Speicherbereichs auf Datenträgern mit sequenziellem Zugriff bei inaktivierter Kollokation



## Kollokationseinstellungen

Nach der Definition eines Speicherpools können Sie die Kollokationseinstellung durch Aktualisieren des Speicherpools ändern. Die Änderung der Kollokation für den Pool hat keine Auswirkungen auf Dateien, die bereits in dem Pool gespeichert sind.

Wenn beispielsweise die Kollokation für einen Speicherpool inaktiviert ist und jetzt aktiviert wird, werden ab diesem Zeitpunkt Clientdateien, die in dem Pool gespeichert werden, kollokiert. Dateien, die zuvor in dem Speicherpool gespeichert wurden, werden nicht versetzt, um kollokiert zu werden. Wenn Datenträger konsolidiert werden, werden die Daten in dem Pool im Laufe der Zeit immer stärker kollokiert. Sie können auch den Befehl MOVE DATA oder MOVE NODEDATA verwenden, um Daten auf neue Datenträger zu versetzen, um die Kollokation zu erhöhen. Das Versetzen von Daten auf neue Datenträger führt jedoch zu einer Verlängerung der Verarbeitungszeit und zu einer Erhöhung der Datenträgermountaktivität.

Tipp: Wenn die Kollokation nach Dateibereich aktiviert ist und ein Knoten über einen Datenträger mit mehreren Dateibereichen verfügt, kann eine Mountwartzeit auftreten oder der Mount länger als üblich dauern. Wenn ein Datenträger für den Datenempfang auswählbar ist, wartet IBM Spectrum Protect auf diesen Datenträger.

## Kollokation von Kopierspeicherpools

Bei der Verwendung der Kollokation für Kopierspeicherpools müssen bestimmte Hinweise beachtet werden. Die Kollokation von Kopierspeicherpools, insbesondere die Kollokation nach Knoten oder Dateibereich, hat mehr teilweise gefüllte Datenträger und möglicherweise unnötige Konsolidierungsaktivität für ausgelagerte Datenträger zur Folge.

Primäre Speicherpools spielen bei der Wiederherstellung eine andere Rolle als Kopierspeicherpools. Normalerweise werden primäre Speicherpools verwendet, um Daten direkt auf Clients wiederherzustellen. Wenn in einem Katastrophenfall sowohl Clients als auch der Server verloren gehen, können Sie ausgelagerte Kopierspeicherpool-Datenträger verwenden, um die primären Speicherpools wiederherzustellen. Mithilfe der Typen von Wiederherstellungsszenarios können Sie bestimmen, ob die Kollokation für Ihre Kopierspeicherpools verwendet werden sollte.

Die Kollokation hat in der Regel teilweise gefüllte Datenträger zur Folge, wenn die Kollokation nach Knoten oder Dateibereich erfolgt. Teilweise gefüllte Datenträger sind jedoch seltener vorhanden, wenn die Kollokation nach Gruppe erfolgt. Teilweise gefüllte Datenträger können für primäre Speicherpools akzeptabel sein, da die Datenträger verfügbar bleiben und während des nächsten Umlagerungsprozesses gefüllt werden können. Teilweise gefüllte Datenträger können jedoch für Kopierspeicherpools, deren Speicherpool-Datenträger sofort ausgelagert werden, inakzeptabel sein. Wenn Sie die Kollokation für Kopierspeicherpools verwenden, müssen Sie die folgenden Entscheidungen treffen:

- Auslagerung einer größeren Anzahl teilweise gefüllter Datenträger, wodurch sich die Konsolidierungsaktivität erhöht, wenn der Konsolidierungsschwellenwert verringert oder erreicht wird.
- Verbleib dieser teilweise gefüllten Datenträger vor Ort, bis sie voll sind, wobei das Risiko besteht, dass keine ausgelagerte Kopie der Daten auf diesen Datenträgern vorhanden ist.
- Angabe, ob die Kollokation nach Gruppe erfolgen soll, um möglichst viel Bandkapazität zu nutzen.

Wenn die Kollokation für einen Kopierspeicherpool inaktiviert ist, sind nach dem Sichern von Daten im Kopierspeicherpool normalerweise nur einige wenige teilweise gefüllte Datenträger vorhanden.

Überprüfen Sie Ihre Optionen sorgfältig, bevor Sie die Kollokation für Kopierspeicherpools verwenden, und wägen Sie ab, ob gleichzeitiges Schreiben verwendet werden soll. Wenn bei Verwendung der Kollokation für Ihre primären Speicherpools kein gleichzeitiges Schreiben verwendet wird, können Sie die Kollokation für Kopierspeicherpools gegebenenfalls inaktivieren. Die Kollokation für Kopierspeicherpools kann sinnvoll sein, wenn nur wenige Clients vorhanden sind und für jeden dieser Clients täglich sehr viele Teilsicherungsdaten anfallen. Wenn die Kollokation zusammen mit gleichzeitigem Schreiben verwendet wird, müssen Sie sicherstellen, dass die Kollokationseinstellungen für die primären Speicherpools und die Kopierspeicherpools identisch sind.

## Kollokation planen und aktivieren

Zu wissen, welche Auswirkungen die Kollokation hat, kann hilfreich sein, um die Anzahl der Datenträgermounts zu reduzieren, den Speicherbereich auf sequenziellen Datenträgern besser zu nutzen und die Effizienz von Serveroperationen zu verbessern.

## Informationen zu diesem Vorgang

In Tabelle 1 sind die vier Kollokationsoptionen aufgeführt, die Sie in den Befehlen DEFINE STGPOOL und UPDATE STGPOOL angeben können. Die Tabelle zeigt auch die Auswirkungen der Kollokation auf Daten, die zu Knoten gehören, die Mitglieder einer Kollokationsgruppe sind, bzw. die zu Knoten gehören, die keine Mitglieder einer Kollokationsgruppe sind.

Tabelle 1. Kollokationsoptionen und Auswirkungen auf Knotendaten

| Kollokationsoption  | Wenn ein Knoten nicht als Mitglied einer Kollokationsgruppe definiert ist  | Wenn ein Knoten als Mitglied einer Kollokationsgruppe definiert ist  |
|---------------------|--|--|
| <b>Keine</b>        | Die Daten für den Knoten werden nicht kollokiert.  | Die Daten für den Knoten werden nicht kollokiert.  |
| <b>Gruppe</b>       | Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern im Speicherpool.  | Der Server speichert die Daten für den Knoten und für andere Knoten, die zu derselben Kollokationsgruppe gehören, auf möglichst wenigen Datenträgern.  |
| <b>Knoten</b>       | Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.  | Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.  |
| <b>Dateibereich</b> | Der Server speichert die Daten für den Dateibereich des Knotens auf möglichst wenigen Datenträgern. Wenn ein Knoten mehrere Dateibereiche hat, speichert der Server die Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern im Speicherpool. | Der Server speichert die Daten für den Dateibereich des Knotens auf möglichst wenigen Datenträgern. Wenn ein Knoten mehrere Dateibereiche hat, speichert der Server die Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern im Speicherpool. |

Tabelle 2. Kollokationsgruppenoptionen und Auswirkungen auf Dateibereichsdaten

| Kollokationsoption  | Wenn ein Dateibereich nicht als Mitglied einer Kollokationsgruppe definiert ist  | Wenn ein Dateibereich als Mitglied einer Kollokationsgruppe definiert ist   |
|---------------------|--|---|
| <b>Keine</b>        | Die Daten für den Dateibereich werden nicht kollokiert.  | Die Daten für den Dateibereich werden nicht kollokiert.   |
| <b>Gruppe</b>       | Der Server speichert die Daten für den Dateibereich auf möglichst wenigen Datenträgern im Speicherpool.  | Der Server speichert die Daten für den Dateibereich und für andere Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf möglichst wenigen Datenträgern.  |
| <b>Knoten</b>       | Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.  | Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.   |
| <b>Dateibereich</b> | Der Server speichert die Daten für den Dateibereich des Knotens auf möglichst wenigen Datenträgern. Wenn ein Knoten mehrere Dateibereiche hat, speichert der Server die Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern im Speicherpool. | Der Server speichert die Daten für die Dateibereiche auf möglichst wenigen Datenträgern. Wenn ein Knoten mehrere Dateibereiche hat, speichert der Server die Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern im Speicherpool. |

## Vorgehensweise

Um festzulegen, ob und wie Daten kollokiert werden, führen Sie die folgenden Schritte aus:

- Legen Sie fest, wie Daten zusammengefasst werden sollen, ob nach Clientknoten, nach Clientknotengruppe oder nach Dateibereich. Bei der Kollokation nach Gruppe müssen Sie entscheiden, wie Knoten in Gruppen zusammengefasst werden sollen:
  - Wenn das Einsparen von Speicherbereich das Ziel ist, möchten Sie möglicherweise kleine Knoten in einer Gruppe zusammenfassen, um Bänder besser zu nutzen.
  - Wenn schnellere Clientzurückschreibungen das Ziel sind, gruppieren Sie Knoten so, dass sie möglichst viele Bänder füllen. Indem Knoten in Gruppen zusammengefasst werden, werden die Daten der einzelnen Knoten auf zwei oder mehr Bänder verteilt und es können mehr Bänder während einer Mehrfachszugung für eine Zurückschreibungsoperation ohne Abfrage gleichzeitig bereitgestellt werden.
  - Wenn die Aufteilung der Daten nach Abteilung das Ziel ist, können Sie Knoten nach Abteilung gruppieren.
- Um Gruppen zu kollokieren, führen Sie die folgenden Schritte aus:
  - Definieren Sie Kollokationsgruppen mit dem Befehl DEFINE COLLOGROUP.
  - Fügen Sie den Kollokationsgruppen mit dem Befehl DEFINE COLLOCMEMBER Clientknoten hinzu.

Die folgenden Abfragebefehle sind zum Kollokieren von Gruppen verfügbar:

```
QUERY COLLOGROUP
```

- Zeigt die Kollokationsgruppen an, die auf dem Server definiert sind.
- QUERY NODE
  - Zeigt die Kollokationsgruppe an (falls vorhanden), zu der ein Knoten gehört.
- QUERY NODEDATA
  - Zeigt Informationen zu den Daten für einen oder mehrere Knoten in einem Speicherpool mit sequenziellem Zugriff an.
- QUERY STGPOOL
  - Zeigt Informationen zur Position von Clientdaten in einem Speicherpool mit sequenziellem Zugriff und zum Umfang des Speicherbereichs an, den ein Knoten auf einem Datenträger belegt.

Sie können auch IBM Spectrum Protect-Server-Scripts oder PERL-Scripts verwenden, um Informationen anzuzeigen, die beim Definieren von Kollokationsgruppen hilfreich sein können.

3. Geben Sie an, wie Daten in einem Speicherpool kolliert werden müssen, indem Sie den Befehl DEFINE STGPOOL oder UPDATE STGPOOL unter Angabe des Parameters COLLOCATE ausgeben.

## Nächste Schritte

---

Tipp: Um die Anzahl Datenträgermounts zu reduzieren, Speicherbereich auf sequenziellen Datenträgern effizienter zu verwenden und die Kollokation zu aktivieren, führen Sie die folgenden Schritte aus:

- Definieren Sie eine Speicherpoolhierarchie und eine Maßnahme, die erfordert, dass gesicherte, archivierte oder speicherverwaltete Dateien anfänglich in Plattenspeicherpools gespeichert werden.
- Wenn Dateien aus einem Plattenspeicherpool umgelagert werden, versucht der Server, alle Dateien umzulagern, die zu dem Clientknoten oder zu der Kollokationsgruppe gehören, der bzw. die den meisten Plattenspeicherplatz in dem Speicherpool belegt. Dieser Prozess funktioniert gut mit der Kollokationsoption, da der Server versucht, alle Dateien eines bestimmten Clients auf demselben Speicherdatenträger mit sequenziellem Zugriff zu speichern.
- Verwenden Sie Arbeitsdatenträger für Speicherpools mit sequenziellem Zugriff, damit der Server neue Datenträger für die Kollokation auswählen kann.
  - Geben Sie die Clientoption COLLOCATEBYFILESPEC an, um die Anzahl Bänder zu begrenzen, auf die Objekte, die einer einzelnen Dateispezifikation zugeordnet sind, geschrieben werden. Diese Kollokationsoption hat eine effizientere Kollokation durch den Server zur Folge; diese Kollokationsoption überschreibt nicht die Kollokation nach Dateibereich oder die Kollokation nach Knoten.

## Bandeinheiten verwalten

---

Routinemäßige Bandoperationen umfassen die Vorbereitung von Banddatenträgern für die Verwendung, die Steuerung, wie und wann Datenträger wiederverwendet werden, und die Sicherstellung, dass genügend Datenträger verfügbar sind. Außerdem müssen Sie auf Bedieneranforderungen antworten und Speicherarchive, Laufwerke, Pfade und Einheiten zum Versetzen von Daten verwalten.

- Austauschbare Datenträger vorbereiten
 

Sie müssen austauschbare Datenträger vorbereiten, bevor sie zum Speichern von Daten verwendet werden können. Typische Vorbereitungstasks umfassen das Zuordnen von Kennsätzen und das Zurückstellen von Datenträgern.
- Datenträgerbestand verwalten
 

Sie können den Datenträgerbestand verwalten, indem Sie den Zugriff des Servers auf Datenträger steuern, Bänder wiederverwenden und Datenträger wiederverwenden, die für Datenbanksicherungs- und Exportoperationen verwendet werden. Sie können den Bestand auch verwalten, indem Sie einen Vorrat an Arbeitsdatenträgern bereithalten.
- Teilweise beschriebene Datenträger
 

Teilweise beschriebene Datenträger sind immer private Datenträger; dies ist auch dann der Fall, wenn ihr Status vor dem Bereitstellen durch den Server PRIVATE lautet. Der Server protokolliert den ursprünglichen Status von Arbeitsdatenträgern und versetzt diese wieder in den Arbeitsstatus, wenn sie leer sind.
- Operationen für gemeinsam genutzte Speicherarchive
 

Gemeinsam genutzte Speicherarchive sind logische Speicherarchive, die physisch durch SCSI-Speicherarchive dargestellt werden. Das physische Speicherarchiv wird durch den IBM Spectrum Protect-Server gesteuert, der als Speicherarchivmanager konfiguriert ist. IBM Spectrum Protect-Server, die den Speicherarchivtyp SHARED verwenden, sind Speicherarchivclients für den IBM Spectrum Protect-Speicherarchivmanager-Server.
- Serveranforderungen für Datenträger verwalten
 

IBM Spectrum Protect zeigt allen Verwaltungsbefehlszeilenclients, die im Konsolenmodus gestartet werden, Anforderungen und Statusnachrichten an. Für diese Anforderungsnachrichten ist häufig ein Zeitlimit festgelegt. Erfolgreiche Serveroperationen müssen innerhalb des angegebenen Zeitlimits abgeschlossen werden; andernfalls tritt für die Operation eine Zeitlimitüberschreitung auf.

## Austauschbare Datenträger vorbereiten

---

Sie müssen austauschbare Datenträger vorbereiten, bevor sie zum Speichern von Daten verwendet werden können. Typische Vorbereitungstasks umfassen das Zuordnen von Kennsätze und das Zurückstellen von Datenträgern.

## Informationen zu diesem Vorgang

---

Wenn IBM Spectrum Protect auf einen austauschbaren Datenträger zugreift, wird der Datenträgername im Kennsatzheader geprüft, um sicherzustellen, dass auf den korrekten Datenträger zugegriffen wird.

Banddatenträgern müssen Kennsätze zugeordnet werden, bevor sie vom Server verwendet werden können.

## Vorgehensweise

---

Um einen Datenträger für die Verwendung vorzubereiten, führen Sie die folgenden Schritte aus:

1. Ordnen Sie dem Datenträger einen Kennsatz zu, indem Sie den Befehl LABEL LIBVOLUME ausgeben.
2. Stellen Sie bei automatisierten Speicherarchiven den Datenträger in das Speicherarchiv zurück. Anweisungen finden Sie in Datenträger in ein automatisiertes Speicherarchiv zurückstellen.  
Tipp: Wenn Sie den Befehl LABEL LIBVOLUME für Laufwerke in einem automatisierten Speicherarchiv verwenden, ist es mit einem einzigen Befehl möglich, den Datenträgern Kennsätze zuzuordnen und die Datenträger zurückzustellen.
3. Wenn der Speicherpool keine Arbeitsdatenträger enthalten kann (MAXSCRATCH=0), identifizieren Sie den Datenträger in IBM Spectrum Protect anhand des Namens, damit später auf den Datenträger zugegriffen werden kann.

Wenn der Speicherpool Arbeitsdatenträger enthalten kann (MAXSCRATCH ist auf einen Wert ungleich null gesetzt), überspringen Sie diesen Schritt.

- Banddatenträgern Kennsätze zuordnen  
Sie müssen Banddatenträgern Kennsätze zuordnen, bevor diese vom Server verwendet werden können.
- Datenträger in ein automatisiertes Speicherarchiv zurückstellen  
Sie können einen Datenträger mithilfe des Befehls CHECKIN LIBVOLUME in ein automatisiertes Speicherarchiv zurückstellen.

## Banddatenträgern Kennsätze zuordnen

---

Sie müssen Banddatenträgern Kennsätze zuordnen, bevor diese vom Server verwendet werden können.

## Informationen zu diesem Vorgang

---

Bei automatisierten Speicherarchiven werden Sie zum Einlegen des Datenträgers in den Eingangs-/Ausgangsschacht des Speicherarchivs aufgefordert. Wenn keine Serviceein-/ausgabestation verfügbar ist, legen Sie den Datenträger in einen leeren Schacht ein. Sie können den Datenträgern Kennsätze zuordnen, wenn Sie die Datenträger zurückstellen oder bevor Sie die Datenträger zurückstellen.

## Vorgehensweise

---

Um Banddatenträgern Kennsätze zuzuordnen, bevor sie zurückgestellt werden, führen Sie die folgenden Schritte aus:

1. Ordnen Sie Banddatenträgern Kennsätze zu, indem Sie den Befehl LABEL LIBVOLUME ausgeben. Um beispielsweise einem Datenträger in einem Speicherarchiv mit dem Namen LIBRARY1 den Namen VOLUME1 zuzuordnen, geben Sie den folgenden Befehl aus:

```
label libvolume library1 volume1
```

Voraussetzung: Es muss mindestens ein Laufwerk verfügbar sein. Das Laufwerk darf nicht von einem anderen IBM Spectrum Protect-Prozess verwendet werden. Wenn ein Laufwerk inaktiv ist, wird das Laufwerk als nicht verfügbar betrachtet.

2. Um einen vorhandenen Kennsatz zu überschreiben, geben Sie den Parameter OVERWRITE=YES an. Standardmäßig wird ein vorhandener Kennsatz mit dem Befehl LABEL LIBVOLUME nicht überschrieben.
- Datenträgern in einem SCSI-Speicherarchiv Kennsätze zuordnen  
Sie können Datenträgern einzeln einen Kennsatz zuordnen oder das Speicherarchiv mithilfe von IBM Spectrum Protect durchsuchen und den gefundenen Datenträgern Kennsätze zuordnen.

### Zugehörige Tasks:

Neuen Datenträgern mit AUTOLABEL Kennsätze zuordnen

### Zugehörige Verweise:

🔗 LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

# Datenträger in ein automatisiertes Speicherarchiv zurückstellen

---

Sie können einen Datenträger mithilfe des Befehls CHECKIN LIBVOLUME in ein automatisiertes Speicherarchiv zurückstellen.

## Vorbereitende Schritte

---

Um Bändern automatisch Kennsätze zuzuordnen, bevor sie zurückgestellt werden, geben Sie den Befehl DEFINE LIBRARY unter Angabe des Parameters AUTOLABEL=YES aus. Wenn der Parameter AUTOLABEL verwendet wird, entfällt die Notwendigkeit, einer Gruppe von Bändern vorab Kennsätze zuzuordnen zu müssen.

## Informationen zu diesem Vorgang

---

Jeder Datenträger, der von einem Server für einen beliebigen Zweck verwendet wird, muss einen eindeutigen Namen haben. Diese Voraussetzung gilt für alle Datenträger, unabhängig davon, ob die Datenträger für Speicherpools oder für Operationen wie beispielsweise Datenbanksicherung oder Export verwendet werden. Die Voraussetzung gilt auch für Datenträger, die sich in unterschiedlichen Speicherarchiven befinden, aber von demselben Server verwendet werden.

Tipps:



- Verwenden Sie nicht ein einzelnes Speicherarchiv für Datenträger mit Barcodeetiketten und Datenträger ohne Barcodeetiketten. Das Scannen von Barcodes kann bei Datenträgern ohne Kennsatz lange dauern.
- Der Server akzeptiert nur Bänder, denen IBM® Standardkennsätze zugeordnet wurden.
- Jeder Datenträger mit einem Barcode, der mit CLN beginnt, wird als Reinigungsband betrachtet.
- Wenn für einen Datenträger ein Eintrag im Datenträgerprotokoll vorhanden ist, kann der Datenträger nicht als Arbeitsdatenträger zurückgestellt werden.

## Vorgehensweise

---

1. Um einen Speicherdatenträger in ein Speicherarchiv zurückzustellen, geben Sie den Befehl CHECKIN LIBVOLUME aus.  
Tipp: Der Befehl wird immer als Hintergrundprozess ausgeführt. Warten Sie, bis die Verarbeitung des Prozesses CHECKIN LIBVOLUME abgeschlossen ist, bevor Sie Datenträger definieren; andernfalls schlägt der Definitionsprozess fehl. Sie können Zeit sparen, indem Sie Datenträger im Rahmen der Operation zum Zuordnen von Kennsätzen zurückstellen.
  2. Geben Sie den Namen des Speicherarchivs an und geben Sie an, ob es sich bei dem Datenträger um einen privaten Datenträger oder einen Arbeitsdatenträger handelt. Führen Sie abhängig davon, ob Sie Arbeitsdatenträger oder private Datenträger verwenden, einen der folgenden Schritte aus:
    - Wenn Sie nur Arbeitsdatenträger verwenden, stellen Sie sicher, dass genügend Arbeitsdatenträger verfügbar sind. Beispielsweise müssen Sie gegebenenfalls weiteren Datenträgern Kennsätze zuordnen. In dem Maße, wie Datenträger verwendet werden, müssen Sie unter Umständen auch die Anzahl zulässiger Arbeitsdatenträger in dem Speicherpool erhöhen, der für dieses Speicherarchiv definiert wurde.
    - Wenn private Datenträger zusätzlich zu oder anstelle von Arbeitsdatenträgern in dem Speicherarchiv verwendet werden sollen, definieren Sie Datenträger für den Speicherpool mithilfe des Befehls DEFINE VOLUME. Sie müssen den Datenträgern, die Sie definieren, Kennsätze zuordnen und die Datenträger zurückstellen.
- Einzelnen Datenträger in ein SCSI-Speicherarchiv zurückstellen  
Sie können einen einzelnen Datenträger zurückstellen, indem Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters SEARCH=NO ausgeben. IBM Spectrum Protect fordert den Bediener, der den Mount durchführt, dazu auf, den Datenträger in den Eingangs-/Ausgangsport des Speicherarchivs zu laden.
  - Datenträger aus Speicherarchivspeicherschächten zurückstellen  
Wenn viele Datenträger zurückgestellt werden müssen und verhindert werden soll, dass für jeden Datenträger ein Befehl CHECKIN LIBVOLUME ausgegeben werden muss, können Sie Speicherschächte nach neuen Datenträgern durchsuchen. Der Server findet Datenträger, die dem Datenträgerbestand noch nicht hinzugefügt wurden.
  - Datenträger aus Eingangs-/Ausgangsports eines Speicherarchivs zurückstellen  
Sie können alle Schächte von Masseneingangs-/Ausgangsports nach Datenträgern mit Kennsätzen durchsuchen und der Server kann diese automatisch zurückstellen.
  - Datenträger mithilfe von Barcodelesern in Speicherarchiven zurückstellen  
Sie können Zeit sparen, wenn Sie Datenträger in Speicherarchive mit Barcodelesern zurückstellen, indem Sie die Zeichen auf den Barcodeetiketten als Namen für die Datenträger verwenden.
  - Datenträger mithilfe eines Barcodelesers zurückstellen  
Sie können Zeit sparen, wenn Sie Datenträger mithilfe eines Barcodelesers zurückstellen, vorausgesetzt, Ihr Speicherarchiv verfügt über einen Barcodeleser.
  - Datenträger mit der Auslagerungsfunktion in ein volles Speicherarchiv zurückstellen  
Wenn beim Zurückstellen von Datenträgern keine leeren Schächte in dem Speicherarchiv verfügbar sind, schlägt die Zurückstelloperation fehl, es sei denn, Sie aktivieren die *Auslagerungsfunktion*. Wenn Sie die Auslagerungsfunktion aktivieren und

das Speicherarchiv voll ist, wählt der Server einen Datenträger zum Ausgeben aus und stellt dann den angeforderten Datenträger zurück.

-  Windows-Betriebssysteme Private Datenträger und Arbeitsdatenträger  
Lesen Sie zur Optimierung von Bandspeicher die Informationen zu privaten Datenträgern und Arbeitsdatenträgern. Verwenden Sie private Datenträger und Arbeitsdatenträger dementsprechend.
-  Windows-Betriebssysteme Elementadressen für Speicherarchivspeicherschächte  
Eine Elementadresse ist eine Zahl, die die physische Position eines Speicherschachts oder Laufwerks in einem automatisierten Speicherarchiv angibt.

#### Zugehörige Tasks:

Banddatenträgern Kennsätze zuordnen

## Einzelnen Datenträger in ein SCSI-Speicherarchiv zurückstellen

Sie können einen einzelnen Datenträger zurückstellen, indem Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters SEARCH=NO ausgeben. IBM Spectrum Protect fordert den Bediener, der den Mount durchführt, dazu auf, den Datenträger in den Eingangs-/Ausgangsport des Speicherarchivs zu laden.

### Vorgehensweise

1. Geben Sie den Befehl CHECKIN LIBVOLUME aus.

Um beispielsweise den Datenträger VOL001 zurückzustellen, geben Sie den folgenden Befehl ein:

```
checkin libvolume tapelib vol001 search=no status=scratch
```

2. Antworten Sie auf die Eingabeaufforderung des Servers.

- Wenn das Speicherarchiv über einen Eingangs-/Ausgangsport verfügt, werden Sie zum Einlegen eines Bands in den Eingangs-/Ausgangsport aufgefordert.
- Wenn das Speicherarchiv über keinen Eingangs-/Ausgangsport verfügt, werden Sie zum Einlegen eines Bands in einen der Schächte im Speicherarchiv aufgefordert. Diese Schächte werden durch Elementadressen angegeben. Wenn der Server beispielsweise erkennt, dass der erste leere Schacht die Elementadresse 5 hat, wird die folgende Nachricht zurückgegeben:

```
ANR8306I 001: 8MM-Datenträger VOL001 R/W innerhalb von 60 Minuten  
in Schacht mit Elementnummer 5 in Kassettenarchiv TAPELIB einlegen;  
wenn bereit, 'REPLY' zusammen mit der Anforderungs-ID ausgeben.
```

Wenn Sie die Position von Elementadresse 5 in dem Speicherarchiv nicht kennen, überprüfen Sie das Arbeitsblatt auf die Einheit. Angaben zur Lokalisation des Arbeitsblattes enthält die Dokumentation zu Ihrem Speicherarchiv. Nachdem Sie den Datenträger wie angefordert eingelegt haben, antworten Sie auf die Nachricht von einem IBM Spectrum Protect-Verwaltungsclient. Geben Sie den Befehl REPLY gefolgt von der Anforderungsnummer (die Nummer am Anfang der Mountanforderung) aus, beispielsweise:

```
reply 1
```

Tipp: Elementadressen beginnen nicht notwendigerweise mit der Zahl 1. Überprüfen Sie das Arbeitsblatt dahingehend. Wenn für Ihre Einheit im IBM® Support Portal for IBM Spectrum Protect kein Arbeitsblatt aufgelistet ist, ziehen Sie die Dokumentation zu Ihrem Speicherarchiv zu Rate.

Wenn Sie über den optionalen Parameter WAITTIME im Befehl CHECKIN LIBVOLUME eine Wartezeit von 0 angeben, ist kein Befehl REPLY erforderlich. Die Standardwartezeit beträgt 60 Minuten.

## Datenträger aus Speicherarchivspeicherschächten zurückstellen

Wenn viele Datenträger zurückgestellt werden müssen und verhindert werden soll, dass für jeden Datenträger ein Befehl CHECKIN LIBVOLUME ausgegeben werden muss, können Sie Speicherschächte nach neuen Datenträgern durchsuchen. Der Server findet Datenträger, die dem Datenträgerbestand noch nicht hinzugefügt wurden.

### Vorgehensweise

1. Öffnen Sie das Speicherarchiv und legen Sie die neuen Datenträger in freie Schächte ein. Öffnen Sie beispielsweise bei einer SCSI-Einheit die Zugangstür des Speicherarchivs, legen Sie alle neuen Datenträger in freie Schächte ein und schließen Sie die Zugangstür.
2. Wenn den Datenträgern kein Kennsatz zugeordnet ist, ordnen Sie dem Datenträger mit dem Befehl LABEL LIBVOLUME einen Kennsatz zu.
3. Geben Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters SEARCH=YES aus.



#### Zugehörige Verweise:

➔ CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

## Datenträger aus Eingangs-/Ausgangsports eines Speicherarchivs zurückstellen

---

Sie können alle Schächte von Masseneingangs-/ausgangsports nach Datenträgern mit Kennsätzen durchsuchen und der Server kann diese automatisch zurückstellen.

### Vorbereitende Schritte

---

Geben Sie den Befehl LABEL LIBVOLUME aus, um allen Datenträgern ohne Kennsatz einen Kennsatz zuzuordnen.

### Informationen zu diesem Vorgang

---

Bei SCSI-Speicherarchiven durchsucht der Server alle Eingangs-/Ausgangsports in dem Speicherarchiv nach Datenträgern. Wenn ein Datenträger gefunden wird, der einen gültigen Datenträgerkennsatz enthält, wird der Datenträger automatisch zurückgestellt.

### Vorgehensweise

---

Geben Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters SEARCH=BULK aus.

- Um ein Band in ein Laufwerk zu laden und den Kennsatz zu lesen, geben Sie den Parameter CHECKLABEL=YES an. Nachdem der Kennsatz vom Server gelesen wurde, versetzt der Server das Band aus dem Laufwerk in einen Speicherschacht.
- Damit der Server den Barcodeleser zur Überprüfung externer Kennsätze auf Bändern verwendet, geben Sie den Parameter CHECKLABEL=BARCODE an. Wenn das Lesen von Barcodes aktiviert ist, liest der Server den Kennsatz und versetzt das Band aus dem Eingangs-/Ausgangsport in einen Speicherschacht.

## Datenträger mithilfe von Barcodelesern in Speicherarchiven zurückstellen

---

Sie können Zeit sparen, wenn Sie Datenträger in Speicherarchive mit Barcodelesern zurückstellen, indem Sie die Zeichen auf den Barcodeetiketten als Namen für die Datenträger verwenden.

### Informationen zu diesem Vorgang

---

Der Server liest die Barcodeetiketten und verwendet die Informationen zum Schreiben der internen Datenträgerkennsätze. Bei Datenträgern ohne Barcodeetiketten stellt der Server die Datenträger in einem Laufwerk bereit und versucht, den internen aufgezeichneten Kennsatz zu lesen.

### Vorgehensweise

---

Geben Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters CHECKLABEL=BARCODE aus. Um beispielsweise mithilfe eines Barcodelesers ein Speicherarchiv mit dem Namen TAPELIB zu durchsuchen und ein Arbeitsband zurückzustellen, geben Sie den folgenden Befehl aus:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

## Datenträger mithilfe eines Barcodelesers zurückstellen

---

Sie können Zeit sparen, wenn Sie Datenträger mithilfe eines Barcodelesers zurückstellen, vorausgesetzt, Ihr Speicherarchiv verfügt über einen Barcodeleser.

### Informationen zu diesem Vorgang

---

Wenn Sie einen Datenträger zurückstellen, können Sie angeben, ob die Datenträgerkennsätze während der Zurückstellungsverarbeitung gelesen werden sollen. Wenn die Kennsatzprüfung aktiviert ist, stellt IBM Spectrum Protect jeden Datenträger bereit, um den internen Kennsatz zu lesen, und stellt einen Datenträger nur dann zurück, wenn der Kennsatz korrekt ist. Mithilfe der Kennsatzprüfung können zukünftige Fehler verhindert werden, wenn Datenträger in Speicherpools verwendet werden; dadurch verlängert sich jedoch die Verarbeitungszeit beim Zurückstellen.

Wenn ein Datenträger kein Barcodeetikett hat, stellt IBM Spectrum Protect die Datenträger in einem Laufwerk bereit und versucht, den aufgezeichneten Kennsatz zu lesen.

## Vorgehensweise


Um Datenträger mithilfe eines Barcodelesers zurückzustellen, geben Sie den Befehl CHECKIN LIBVOLUME unter Angabe von CHECKLABEL=BARCODE aus. Um beispielsweise mithilfe des Barcodelesers alle Datenträger als Arbeitsdatenträger in ein Speicherarchiv mit dem Namen TAPELIB zurückzustellen, geben Sie den folgenden Befehl aus:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

### Zugehörige Tasks:

Austauschbare Datenträger vorbereiten

### Zugehörige Verweise:

 CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

## Datenträger mit der Auslagerungsfunktion in ein volles Speicherarchiv zurückstellen

Wenn beim Zurückstellen von Datenträgern keine leeren Schächte in dem Speicherarchiv verfügbar sind, schlägt die Zurückstelloperation fehl, es sei denn, Sie aktivieren die *Auslagerungsfunktion*. Wenn Sie die Auslagerungsfunktion aktivieren und das Speicherarchiv voll ist, wählt der Server einen Datenträger zum Ausgeben aus und stellt dann den angeforderten Datenträger zurück.

### Informationen zu diesem Vorgang

Bei der Auswahl des auszugebenden Datenträgers prüft der Server zunächst, ob ein verfügbarer Arbeitsdatenträger vorhanden ist und sucht dann nach dem Datenträger mit der geringsten Anzahl Mounts. Der Server gibt den für die Auslagerungsoperation ausgewählten Datenträger aus dem Speicherarchiv aus und ersetzt ihn durch den Datenträger, der zurückgestellt wird.

## Vorgehensweise

Um Datenträger auszulagern, wenn kein leerer Speicherarchivschacht zum Zurückstellen eines Datenträgers verfügbar ist, geben Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters SWAP=YES aus. Um beispielsweise einen Datenträger mit dem Namen VOL1 in ein Speicherarchiv mit dem Namen AUTO zurückzustellen und die Auslagerungsfunktion zu aktivieren, geben Sie den folgenden Befehl aus:

```
checkin libvolume auto voll swap=yes
```

### Zugehörige Tasks:

Volles Speicherarchiv mit einer Überlaufposition verwalten

### Zugehörige Verweise:

 CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

## Private Datenträger und Arbeitsdatenträger

Lesen Sie zur Optimierung von Bandspeicher die Informationen zu privaten Datenträgern und Arbeitsdatenträgern. Verwenden Sie private Datenträger und Arbeitsdatenträger dementsprechend.

Private Datenträger können nicht überschrieben werden, wenn die Bereitstellung eines Arbeitsdatenträgers angefordert wird. Sie können einen Datenträger im Arbeitsstatus nicht zurückstellen, wenn dieser Datenträger von einem Speicherpool verwendet wird, um Daten zu exportieren, eine Datenbank zu sichern oder einen Sicherungsgruppendatenträger zu sichern.

Teilweise beschriebene Datenträger sind immer private Datenträger. Datenträger haben entweder den Status SCRATCH (Arbeitsdatenträger) oder PRIVATE (privater Datenträger); wenn IBM Spectrum Protect jedoch Daten auf ihnen speichert, wird ihnen der Status PRIVATE zugeordnet.

Tabelle 1. Verwendung privater Datenträger und Arbeitsdatenträger

| Datenträgertyp      | Verwendung  |
|---------------------|---|
| Private Datenträger | Verwenden Sie private Datenträger, um die von einzelnen Speicherpools verwendeten Datenträger festzulegen und die Datenträger manuell zu steuern. Geben Sie zum Definieren privater Datenträger den Befehl DEFINE VOLUME aus. Bei Zurückschreibungen, Hauptspeicherauszügen oder Ladevorgängen für Datenbanken oder bei Serverimportoperationen müssen Sie private Datenträger angeben. |

| Datenträgertyp     | Verwendung   |
|--------------------|--|
| Arbeitsdatenträger | <p>In einigen Fällen können Sie die Datenträgerverwaltung durch Verwendung von Arbeitsdatenträgern vereinfachen. Arbeitsdatenträger können unter den folgenden Bedingungen verwendet werden:</p> <ul style="list-style-type: none"> <li>• Es ist nicht erforderlich, jeden einzelnen Speicherpool datenträger zu definieren.</li> <li>• Die Vorteile der Automatisierung automatischer Einheiten sollen genutzt werden.</li> <li>• Verschiedene Speicherpools nutzen ein automatisiertes Speicherarchiv gemeinsam und die Speicherpools können Datenträger dynamisch von den Arbeitsdatenträgern in dem Speicherarchiv anfordern. Die Datenträger müssen den Speicherpools nicht vorab zugeordnet werden.</li> </ul> |

**Zugehörige Tasks:**

Status eines Datenträgers in einem automatisierten Speicherarchiv ändern

**Zugehörige Verweise:**

☞ CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

☞ DELETE VOLUME (Speicherpool datenträger löschen)

## Elementadressen für Speicherarchivspeicherschächte

Eine Elementadresse ist eine Zahl, die die physische Position eines Speicherschachts oder Laufwerks in einem automatisierten Speicherarchiv angibt.

Wenn ein Speicherarchiv über Eingangs-/Ausgangsports verfügt, können Sie Datenträger unter Verwendung der Ports hinzufügen und entfernen. Wenn keine Eingangs-/Ausgangsports vorhanden sind, müssen Sie Bänder in Speicherschächte laden.

Wenn Sie Bänder in Speicherschächte laden, müssen Sie auf Mountanforderungen antworten, die Speicherschächte mit Elementadressen angeben. Wenn Sie im Befehl CHECKIN LIBVOLUME oder im Befehl LABEL LIBVOLUME eine Wartezeit von 0 angeben, müssen Sie nicht auf eine Mountanforderung antworten.

Informationen zu Elementadressen finden Sie in der Dokumentation des Einheitenherstellers oder bei der Suche nach Elementadressen im IBM® Support Portal for IBM Spectrum Protect.

**Zugehörige Verweise:**

☞ CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

☞ LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)


## Datenträgerbestand verwalten

Sie können den Datenträgerbestand verwalten, indem Sie den Zugriff des Servers auf Datenträger steuern, Bänder wiederverwenden und Datenträger wiederverwenden, die für Datenbanksicherungs- und Exportoperationen verwendet werden. Sie können den Bestand auch verwalten, indem Sie einen Vorrat an Arbeitsdatenträgern bereithalten.

### Informationen zu diesem Vorgang

Jeder Datenträger, der von einem Server verwendet wird, muss - unabhängig davon, ob die Datenträger für Speicherpools oder für Operationen wie beispielsweise Datenbanksicherung oder Export verwendet werden - einen eindeutigen Namen haben. Auch Datenträger, die sich in unterschiedlichen Speicherarchiven befinden, aber von demselben Server verwendet werden, müssen einen eindeutigen Namen haben.

- Zugriff auf Datenträger steuern  
Sie können verschiedene Methoden verwenden, um den Zugriff auf Datenträger zu steuern.
- Bänder wiederverwenden  
Um sicherzustellen, dass immer ein ausreichender Vorrat an Bändern verfügbar ist, können Sie alte Dateien verfallen lassen, Datenträger konsolidieren und Datenträger, die das Ende des Lebenszyklus erreicht haben, löschen. Sie können auch einen Vorrat an Arbeitsdatenträgern bereithalten.
- Vorrat an Arbeitsdatenträgern bereithalten  
Sie müssen die die maximale Anzahl Arbeitsdatenträger für einen Speicherpool auf einen entsprechend hohen Wert setzen, um dem erwarteten Bedarf gerecht zu werden.

-  Linux-Betriebssysteme Vorrat an Datenträgern in einem Speicherarchiv mit WORM-Datenträgern bereithalten  
Bei Speicherarchiven, die WORM-Datenträger (WORM = Write Once Read Many) enthalten, können Sie den Abbruch von Datenspeicherungstransaktionen verhindern, indem Sie einen Vorrat an Arbeitsdatenträgern oder neuen privaten Datenträgern in dem Speicherarchiv bereithalten. Abgebrochene Transaktionen können zur Folge haben, dass WORM-Datenträger verschwendet werden.
- Datenträgerbestand in automatisierten Speicherarchiven verwalten  
Der IBM Spectrum Protect-Server verwendet den Datenträgerbestand eines Speicherarchivs, um Arbeitsdatenträger und private Datenträger, die in einem automatisierten Speicherarchiv verfügbar sind, zu verfolgen. Sie müssen sicherstellen, dass der Bestand mit den Datenträgern konsistent ist, die physisch in dem Speicherarchiv vorhanden sind.

## Zugriff auf Datenträger steuern

---

Sie können verschiedene Methoden verwenden, um den Zugriff auf Datenträger zu steuern.

### Vorgehensweise

---

Um den Zugriff auf Datenträger zu steuern, führen Sie eine der folgenden Aktionen aus:

- Um zu verhindern, dass der Server einen Datenträger bereitstellt, geben Sie den Befehl UPDATE VOLUME unter Angabe des Parameters ACCESS=UNAVAILABLE aus.
- Um Datenträger nicht verfügbar zu machen und zum Schutz an einen anderen Standort zu senden, verwenden Sie einen Kopierspeicherpool oder einen Speicherpool für aktive Daten.
- Sie können primäre Speicherpools in einem Kopierspeicherpool sichern und dann die Kopierspeicherpooldatenträger auslagern.
- Sie können aktive Versionen von Clientsicherungsdaten in Speicherpools für aktive Daten kopieren und dann die Datenträger auslagern.
- Sie können Kopierspeicherpooldatenträger und Datenträger in Pools für aktive Daten verfolgen, indem Sie ihren Zugriffsmodus in OFFSITE ändern und das Datenträgerprotokoll aktualisieren, um ihren Standort zu identifizieren.

#### Zugehörige Verweise:

 UPDATE VOLUME (Speicherpooldatenträger aktualisieren)

## Bänder wiederverwenden

---

Um sicherzustellen, dass immer ein ausreichender Vorrat an Bändern verfügbar ist, können Sie alte Dateien verfallen lassen, Datenträger konsolidieren und Datenträger, die das Ende des Lebenszyklus erreicht haben, löschen. Sie können auch einen Vorrat an Arbeitsdatenträgern bereithalten.

### Informationen zu diesem Vorgang

---

Im Laufe der Zeit altern Datenträger und ein Teil der auf den Datenträgern gespeicherten Sicherungsdaten wird unter Umständen nicht mehr benötigt. Sie können Servermaßnahmen definieren, um festzulegen, wie viele Sicherungsversionen und wie lange Sicherungsversionen aufbewahrt werden sollen. Mithilfe der Verfallsverarbeitung können Dateien, die nicht mehr erforderlich sind, gelöscht werden. Sie können die erforderlichen Daten auf den Datenträgern beibehalten. Wenn die Daten nicht mehr benötigt werden, können Sie die Datenträger konsolidieren und wiederverwenden.

### Vorgehensweise

---

1. Löschen Sie nicht benötigte Clientdaten durch regelmäßige Ausführung der Verfallsverarbeitung. Bei der Verfallsverarbeitung werden Daten gelöscht, die nicht mehr gültig sind, da sie den in der Maßnahme angegebenen Aufbewahrungszeitraum überschreiten oder da Benutzer oder Administratoren die aktiven Versionen der Daten gelöscht haben.
2. Verwenden Sie Datenträger in Speicherpools wieder, indem Sie die Konsolidierungsverarbeitung ausführen.

Bei der Konsolidierungsverarbeitung werden alle nicht verfallenen Daten konsolidiert, indem sie von mehreren Datenträgern auf eine geringere Anzahl Datenträger versetzt werden. Die Datenträger können dann wieder in den Speicherpool gestellt und wiederverwendet werden.

3. Verwenden Sie Datenträger wieder, die veraltete Datenbanksicherungen oder exportierte Daten enthalten, die nicht mehr erforderlich sind, indem Sie das Datenträgerprotokoll löschen.

Bevor der Server Datenträger wiederverwenden kann, die im Datenträgerprotokoll protokolliert sind, müssen Sie die Datenträgerinformationen durch Ausgabe des Befehls DELETE VOLHISTORY aus der Protokolldatei für Datenträger löschen.

Tipp: Wenn Ihr Server die Funktion Disaster Recovery Manager (DRM) verwendet, werden die Datenträgerinformationen automatisch während der Verarbeitung des Befehls MOVE DRMEDIA gelöscht.

4. Legen Sie fest, wann Banddatenträger das Ende des Lebenszyklus erreichen. Mithilfe des Servers können Sie Statistikdaten zu Datenträgern anzeigen, die die Anzahl Schreiboperationen für die Datenträger und die Anzahl Schreibfehler umfassen. Für private Datenträger und Arbeitsdatenträger werden die folgenden statistischen Daten angezeigt:

#### Private Datenträger

Bei Datenträgern, die anfänglich als private Datenträger definiert wurden, werden diese statistischen Daten vom Server selbst dann beibehalten, wenn der Datenträger konsolidiert wird. Sie können die Informationen mit der vom Hersteller empfohlenen Anzahl Schreiboperationen und Schreibfehler vergleichen.

#### Arbeitsdatenträger

Bei Datenträgern, die anfänglich als Arbeitsdatenträger definiert wurden, überschreibt der Server diese statistischen Daten bei jeder Konsolidierung der Datenträger.

5. Konsolidieren Sie alle gültigen Daten von Datenträgern, die das Ende des Lebenszyklus erreicht haben. Wenn sich die Datenträger in automatisierten Speicherarchiven befinden, entnehmen Sie diese aus dem Datenträgerbestand. Löschen Sie private Datenträger mit dem Befehl DELETE VOLUME aus der Datenbank.
6. Stellen Sie sicher, dass Datenträger für die Bandrotation verfügbar sind, damit der Speicherbereich im Speicherpool nicht knapp wird. Mithilfe des Operations Center können Sie die Verfügbarkeit von Arbeitsdatenträgern überwachen. Stellen Sie sicher, dass die Anzahl Arbeitsdatenträger hoch genug ist, um den Bedarf zu decken. Weitere Informationen finden Sie in Vorrat an Datenträgern in einem Speicherarchiv mit WORM-Datenträgern bereithalten.  
WORM-Datenträger: WORM-Laufwerke (WORM = Write Once Read Many) können zur Datenträgerverschwendung führen, wenn der Server Transaktionen abbricht, da keine Datenträger zur Ausführung der Sicherungsoperation zur Verfügung stehen. Nachdem Daten vom Server auf WORM-Datenträger geschrieben wurden, kann der Speicherbereich auf den Datenträgern selbst dann nicht wiederverwendet werden, wenn die Transaktionen abgebrochen werden (beispielsweise wenn eine Sicherung wegen Datenträgerknappheit in der Einheit abgebrochen wird). Um die Verschwendung von WORM-Datenträgern zu minimieren, führen Sie die folgenden Aktionen aus:
  - a. Stellen Sie sicher, dass die maximale Anzahl Arbeitsdatenträger für den Speicherpool der Einheit mindestens der Anzahl Speicherschächte in dem Speicherarchiv entspricht.
  - b. Stellen Sie genügend Datenträger in den Datenträgerbestand der Einheit zurück, um dem erwarteten Bedarf gerecht zu werden.

Wenn die meisten Sicherungsoperationen kleine Dateien betreffen, kann sich die Steuerung der Transaktionsgröße auf die Verwendung von WORM-Platten auswirken. Kleinere Transaktionen bedeuten, dass weniger Speicherbereich verschwendet wird, wenn eine Transaktion, wie beispielsweise eine Sicherungsoperation, abgebrochen werden muss. Die Transaktionsgröße wird durch die Serveroption TXNGROUPMAX und die Clientoption TXNBYTELIMIT gesteuert.

#### Zugehörige Tasks:

Daten in Laufwerke umlagern, für die ein Upgrade durchgeführt wurde  
Serveranforderungen für Datenträger verwalten

#### Zugehörige Verweise:

- DELETE VOLHISTORY (Protokolldaten sequenzieller Datenträger löschen)
- DELETE VOLUME (Speicherpooldatenträger löschen)
- Option 'txnbytelimit'
- Serveroption TXNGROUPMAX

#### Zugehörige Informationen:

- EXPIRE INVENTORY (Bestandsverfallsverarbeitung manuell starten)

## Vorrat an Arbeitsdatenträgern bereithalten

---

Sie müssen die maximale Anzahl Arbeitsdatenträger für einen Speicherpool auf einen entsprechend hohen Wert setzen, um dem erwarteten Bedarf gerecht zu werden.

### Informationen zu diesem Vorgang

---

Wenn Sie einen Speicherpool definieren, müssen Sie die maximale Anzahl Arbeitsdatenträger angeben, die der Speicherpool verwenden kann. Der Server fordert bei Bedarf automatisch einen Arbeitsdatenträger an. Wenn die Anzahl Arbeitsdatenträger, die der Server für den Speicherpool verwendet, den angegebenen maximalen Wert überschreitet, kann der Speicherbereich im Speicherpool knapp werden.

### Vorgehensweise

---

Wenn für einen Speicherpool mehr als die maximale Anzahl Arbeitsdatenträger erforderlich ist, können Sie eine oder beide der folgenden Aktionen ausführen:

1. Erhöhen Sie die maximale Anzahl Arbeitsdatenträger, indem Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters MAXSCRATCH ausgeben.
2. Machen Sie Datenträger für die Wiederverwendung verfügbar, indem Sie die Verfallsverarbeitung und die Konsolidierung ausführen, um Daten auf weniger Datenträgern zu konsolidieren.
  - a. Geben Sie den Befehl EXPIRE INVENTORY aus, um die Verfallsverarbeitung auszuführen.  
Tipp: Standardmäßig wird dieser Prozess täglich ausgeführt. Sie können auch die Serveroption EXPINTERVAL in der Serveroptionsdatei dmserv.opt angeben, um die Verfallsverarbeitung automatisch auszuführen. Der Wert 0 gibt an, dass der Befehl EXPIRE INVENTORY zur Ausführung der Verfallsverarbeitung verwendet werden muss.
  - b. Geben Sie den Befehl RECLAIM STGPOOL aus, um die Konsolidierungsverarbeitung auszuführen.  
Tipp: Sie können auch Konsolidierungsschwellenwerte angeben, wenn Sie den Speicherpool definieren, indem Sie den Befehl DEFINE STGPOOL verwenden und den Parameter RECLAIMPROCESS angeben.

## Nächste Schritte

---

Wenn weitere Datenträger für zukünftige Sicherungsoperationen benötigt werden, ordnen Sie weiteren Arbeitsdatenträgern mit dem Befehl LABEL LIBVOLUME Kennsätze zu.

### Zugehörige Tasks:

Vorrat an Arbeitsdatenträgern in einem automatisierten Speicherarchiv bereithalten

### Zugehörige Verweise:

🔗 LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

🔗 UPDATE STGPOOL (Speicherpool aktualisieren)

### Zugehörige Informationen:

🔗 EXPIRE INVENTORY (Bestandsverfallsverarbeitung manuell starten)

🔗 RECLAIM STGPOOL (Datenträger in einem Speicherpool mit sequenziellem Zugriff konsolidieren)

## Vorrat an Datenträgern in einem Speicherarchiv mit WORM-Datenträgern bereithalten

---

Bei Speicherarchiven, die WORM-Datenträger (WORM = Write Once Read Many) enthalten, können Sie den Abbruch von Datenspeicherungstransaktionen verhindern, indem Sie einen Vorrat an Arbeitsdatenträgern oder neuen privaten Datenträgern in dem Speicherarchiv bereithalten. Abgebrochene Transaktionen können zur Folge haben, dass WORM-Datenträger verschwendet werden.

## Informationen zu diesem Vorgang

---

IBM Spectrum Protect bricht eine Transaktion ab, wenn keine Datenträger (private Datenträger oder Arbeitsdatenträger) verfügbar sind, um die Datenspeicherungsoption auszuführen. Nachdem IBM Spectrum Protect eine Transaktion startet, indem Daten auf einen WORM-Datenträger geschrieben werden, kann der beschriebene Bereich auf dem Datenträger selbst dann nicht wiederverwendet werden, wenn die Transaktion abgebrochen wird.

Angenommen, es sind WORM-Datenträger mit einer Speicherkapazität von jeweils 2,6 GB vorhanden und ein Client beginnt mit der Sicherung einer 12-GB-Datei. Wenn IBM Spectrum Protect keinen fünften Arbeitsdatenträger anfordern kann, nachdem vier Datenträger gefüllt wurden, bricht IBM Spectrum Protect die Sicherungsoperation ab. Die vier Datenträger, die IBM Spectrum Protect bereits mit Daten gefüllt hat, können nicht wiederverwendet werden.

Um das Abbrechen von Transaktionen auf ein Mindestmaß zu reduzieren, müssen genügend Datenträger in dem Speicherarchiv verfügbar sein, um die erwarteten Clientoperationen, wie beispielsweise Sicherungen, ausführen zu können.

## Vorgehensweise

---

1. Stellen Sie sicher, dass der Speicherpool, der dem Speicherarchiv zugeordnet ist, über genügend Arbeitsdatenträger verfügt. Geben Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters MAXSCRATCH aus.
2. Um dem erwarteten Bedarf gerecht zu werden, stellen Sie eine ausreichende Anzahl Arbeitsdatenträger oder private Datenträger in das Speicherarchiv zurück, indem Sie den Befehl CHECKIN LIBVOLUME ausgeben.
3. Um die Transaktionsgröße zu steuern, geben Sie die Serveroption TXNGROUPMAX und die Clientoption TXNBYTELIMIT an. Wenn Ihre Clients hauptsächlich kleine Dateien speichern, kann eine Steuerung der Transaktionsgröße die Verwendung von WORM-Datenträgern beeinflussen. Bei kleineren Transaktionen wird weniger Speicherbereich verschwendet, wenn eine Transaktion, wie beispielsweise eine Sicherung, abgebrochen werden muss.

### Zugehörige Verweise:

🔗 CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

🔗 UPDATE STGPOOL (Speicherpool aktualisieren)

🔗 Option 'txnbytelimit'

🔗 Serveroption TXNGROUPMAX

# Datenträgerbestand in automatisierten Speicherarchiven verwalten

---

Der IBM Spectrum Protect-Server verwendet den Datenträgerbestand eines Speicherarchivs, um Arbeitsdatenträger und private Datenträger, die in einem automatisierten Speicherarchiv verfügbar sind, zu verfolgen. Sie müssen sicherstellen, dass der Bestand mit den Datenträgern konsistent ist, die physisch in dem Speicherarchiv vorhanden sind.

Der Datenträgerbestand des Speicherarchivs entspricht nicht dem Datenträgerbestand jedes Speicherpools. Um dem Datenträgerbestand des Speicherarchivs einen Datenträger hinzuzufügen, stellen Sie einen Datenträger in dieses IBM Spectrum Protect-Speicherarchiv zurück.

Eine Liste der Datenträger im Datenträgerbestand des Speicherarchivs ist möglicherweise nicht mit einer Liste der Datenträger im Datenträgerbestand des Speicherpools für die Einheit identisch. Sie können beispielsweise Arbeitsdatenträger in das Speicherarchiv zurückstellen, diese aber nicht für einen Speicherpool definieren. Wenn Arbeitsdatenträger nicht für Sicherungsoperationen ausgewählt werden, können Sie private Datenträger für einen Speicherpool definieren, diese aber nicht in den Datenträgerbestand für die Einheit zurückstellen.

Um sicherzustellen, dass der Datenträgerbestand für das Serverspeicherarchiv immer korrekt ist, entnehmen Sie Datenträger, um die Datenträger physisch aus einem SCSI--Speicherarchiv zu entfernen. Wenn Sie einen Datenträger entnehmen, der von einem Speicherpool verwendet wird, verbleibt der Datenträger in dem Speicherpool. Wenn Sie den Datenträger bereitstellen müssen, während dieser entnommen ist, wird an der Konsole des Bedieners, der den Mount durchführt, eine Nachricht mit der Aufforderung, den Datenträger zurückzustellen, angezeigt. Wenn die Zurückstelloperation nicht erfolgreich ist, markiert der Server den Datenträger als nicht verfügbar.

Wenn sich ein Datenträger im Datenträgerbestand des Speicherarchivs befindet, können Sie den Status des Datenträgers von SCRATCH (Arbeitsdatenträger) in PRIVATE (privater Datenträger) ändern.


Um zu überprüfen, ob der Datenträgerbestand für das Serverspeicherarchiv mit den Datenträgern konsistent ist, die physisch in dem Speicherarchiv vorhanden sind, können Sie das Speicherarchiv prüfen. Der Bestand kann inkonsistent werden, wenn Datenträger in das Speicherarchiv gestellt bzw. aus dem Speicherarchiv entfernt werden, ohne dass der Server über Entnahme- oder Zurückstelloperationen für Datenträger informiert wird.

- Status eines Datenträgers in einem automatisierten Speicherarchiv ändern  
Sie können den Status eines Datenträgers von PRIVATE (privater Datenträger) in SCRATCH (Arbeitsdatenträger) oder umgekehrt ändern.
- Datenträger aus einem automatisierten Speicherarchiv entfernen  
Datenträger können aus einem automatisierten Speicherarchiv entfernt werden, wenn Daten auf einen Datenträger exportiert wurden und die Daten in ein anderes System importiert werden sollen. Möglicherweise sollen auch Datenträger entfernt werden, um Speicherbereich für neue Datenträger zu erstellen.
- Vorrat an Arbeitsdatenträgern in einem automatisierten Speicherarchiv bereithalten  
Wenn Sie einen Speicherpool definieren, der einem automatisierten Speicherarchiv zugeordnet ist, können Sie eine maximale Anzahl Arbeitsdatenträger angeben, die der physischen Kapazität des Speicherarchivs entspricht. Wenn der Server eine größere Anzahl Arbeitsdatenträger für den Speicherpool verwendet, müssen Sie sicherstellen, dass genügend Datenträger verfügbar sind.
- Volles Speicherarchiv mit einer Überlaufposition verwalten  
Mit zunehmendem Speicherbedarf überschreitet die Anzahl Datenträger, die für einen Speicherpool erforderlich sind, unter Umständen die physische Kapazität eines automatisierten Speicherarchivs. Um Speicherbereich für neue Datenträger verfügbar zu machen und vorhandene Datenträger zu überwachen, können Sie eine Überlaufposition für einen Speicherpool definieren.
- Datenträgerbestand in einem Speicherarchiv prüfen  
Sie können ein automatisiertes Speicherarchiv prüfen, um sicherzustellen, dass der Datenträgerbestand des Speicherarchivs mit den Datenträgern konsistent ist, die physisch in dem Speicherarchiv vorhanden sind. Die Prüfung eines Speicherarchivs bietet sich an, wenn der Datenträgerbestand des Speicherarchivs aufgrund manueller Versetzungen der Datenträger in dem Speicherarchiv oder aufgrund von Datenbankproblemen nicht mehr korrekt ist.

## Zugehörige Tasks:

Datenträger in ein automatisiertes Speicherarchiv zurückstellen

## Zugehörige Verweise:

 AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Speicherarchiv prüfen)

# Status eines Datenträgers in einem automatisierten Speicherarchiv ändern

---

Sie können den Status eines Datenträgers von PRIVATE (privater Datenträger) in SCRATCH (Arbeitsdatenträger) oder umgekehrt ändern.

## Vorgehensweise

---

Um den Status eines Datenträgers zu ändern, geben Sie den Befehl UPDATE LIBVOLUME aus. Um beispielsweise den Status eines Datenträgers mit dem Namen VOL1 in PRIVATE (privater Datenträger) zu ändern, geben Sie den folgenden Befehl aus:

```
update libvolume lib1 voll status=private
```

Einschränkungen:

- Sie können den Status eines Datenträgers nicht von PRIVATE (privater Datenträger) in SCRATCH (Arbeitsdatenträger) ändern, wenn der Datenträger zu einem Speicherpool gehört oder in der Protokolldatei für Datenträger definiert ist.
- Private Datenträger müssen vom Administrator definierte Datenträger ohne Daten oder mit ungültigen Daten sein. Sie dürfen keine teilweise beschriebenen Datenträger sein, die aktive Daten enthalten. Die Datenträgerstatistik geht verloren, wenn der Datenträgerstatus geändert wird.

## Datenträger aus einem automatisierten Speicherarchiv entfernen

---

Datenträger können aus einem automatisierten Speicherarchiv entfernt werden, wenn Daten auf einen Datenträger exportiert wurden und die Daten in ein anderes System importiert werden sollen. Möglicherweise sollen auch Datenträger entfernt werden, um Speicherbereich für neue Datenträger zu erstellen.

### Informationen zu diesem Vorgang

---

Standardmäßig wird der Datenträger, der entnommen werden soll, vom Server bereitgestellt und der interne Kennsatz überprüft. Nach der Überprüfung des Kennsatzes entfernt der Server den Datenträger aus dem Datenträgerbestand des Speicherarchivs und versetzt ihn dann in den Eingangs-/Ausgangsport oder die Serviceein-/ausgabestation des Speicherarchivs. Wenn das Speicherarchiv über keinen Eingangs-/Ausgangsport verfügt, fordert der Server den Bediener, der den Mount durchführt, dazu auf, den Datenträger aus einem Schacht oder einer Einheit in dem Speicherarchiv zu entfernen.

### Vorgehensweise

---

- Um einen Datenträger aus einem automatisierten Speicherarchiv zu entfernen, geben Sie den Befehl CHECKOUT LIBVOLUME aus.
- Geben Sie bei automatisierten Speicherarchiven mit mehreren Eingangs-/AusgangSPORTS den Befehl CHECKOUT LIBVOLUME unter Angabe des Parameters REMOVE=BULK aus. Der Server gibt den Datenträger am nächsten verfügbaren Eingangs-/AusgangSPORT aus.

### Nächste Schritte

---

Wenn Sie einen Datenträger entnehmen, der in einem Speicherpool definiert ist, und der Server später auf den Datenträger zugreifen muss, fordert der Server das Zurückstellen des Datenträgers an. Um Datenträger in ein Speicherarchiv zurückzustellen, geben Sie den Befehl CHECKIN LIBVOLUME aus.

**Zugehörige Verweise:**

- ☞ CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
- ☞ CHECKOUT LIBVOLUME (Speicherdatenträger aus einem Speicherarchiv entnehmen)

## Vorrat an Arbeitsdatenträgern in einem automatisierten Speicherarchiv bereithalten

---

Wenn Sie einen Speicherpool definieren, der einem automatisierten Speicherarchiv zugeordnet ist, können Sie eine maximale Anzahl Arbeitsdatenträger angeben, die der physischen Kapazität des Speicherarchivs entspricht. Wenn der Server eine größere Anzahl Arbeitsdatenträger für den Speicherpool verwendet, müssen Sie sicherstellen, dass genügend Datenträger verfügbar sind.

### Vorgehensweise

---

Wenn die Anzahl Arbeitsdatenträger, die der Server für den Speicherpool verwendet, die in der Speicherpooldefinition angegebene Anzahl überschreitet, führen Sie die folgenden Schritte aus:

1. Fügen Sie dem Speicherarchiv Arbeitsdatenträger hinzu, indem Sie den Befehl CHECKIN LIBVOLUME ausgeben.  
Tipp: Möglicherweise müssen Sie eine Überlaufposition verwenden, um Datenträger aus dem Speicherarchiv zu entfernen, um Platz für diese Arbeitsdatenträger zu schaffen. Weitere Informationen finden Sie in Volles Speicherarchiv mit einer Überlaufposition verwalten.
2. Erhöhen Sie die maximale Anzahl Arbeitsdatenträger, die einem Speicherpool hinzugefügt werden können, indem Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters MAXSCRATCH ausgeben.

### Nächste Schritte

---

Da unter Umständen weitere Datenträger für zukünftige Wiederherstellungsoperationen erforderlich sind, ordnen Sie gegebenenfalls zusätzlichen Arbeitsdatenträgern Kennsätze zu und halten Sie diese Datenträger als Vorrat bereit.



### Zugehörige Tasks:

Vorrat an Arbeitsdatenträgern bereithalten

## Volles Speicherarchiv mit einer Überlaufposition verwalten

Mit zunehmendem Speicherbedarf überschreitet die Anzahl Datenträger, die für einen Speicherpool erforderlich sind, unter Umständen die physische Kapazität eines automatisierten Speicherarchivs. Um Speicherbereich für neue Datenträger verfügbar zu machen und vorhandene Datenträger zu überwachen, können Sie eine Überlaufposition für einen Speicherpool definieren.

### Informationen zu diesem Vorgang

Der Server überwacht die Datenträger, die in den Überlaufbereich versetzt werden, und macht Speicherschächte für neue Datenträger verfügbar.

### Vorgehensweise

1. Erstellen Sie eine Überlaufposition für Datenträger. Definieren oder aktualisieren Sie den Speicherpool, der dem automatisierten Speicherarchiv zugeordnet ist, indem Sie den Befehl DEFINE STGPOOL bzw. UPDATE STGPOOL unter Angabe des Parameters OVLOCATION ausgeben. Um beispielsweise eine Überlaufposition mit dem Namen ROOM2948 für einen Speicherpool mit dem Namen ARCHIVEPOOL zu erstellen, geben Sie den folgenden Befehl aus:

```
update stgpool archivepool ovflocation=Room2948
```

2. Wenn in dem Speicherarchiv Speicherbereich für Arbeitsdatenträger erstellt werden muss, versetzen Sie volle Datenträger an die Überlaufposition, indem Sie den Befehl MOVE MEDIA ausgeben. Um beispielsweise alle vollen Datenträger in dem angegebenen Speicherpool aus dem Speicherarchiv zu versetzen, geben Sie den folgenden Befehl aus:

```
move media * stgpool=archivepool
```

3. Stellen Sie Arbeitsdatenträger nach Bedarf zurück.  
Einschränkung: Wenn für einen Datenträger ein Eintrag in der Protokolldatei für Datenträger vorhanden ist, kann der Datenträger nicht als Arbeitsdatenträger zurückgestellt werden. Weitere Informationen finden Sie in Datenträger in ein automatisiertes Speicherarchiv zurückstellen.
4. Identifizieren Sie die leeren Arbeitsbänder an der Überlaufposition, indem Sie den Befehl QUERY MEDIA ausgeben. Geben Sie beispielsweise den folgenden Befehl aus:

```
query media * stg=* whereovflocation=Room2948 wherestatus=empty
```

5. Wenn der Server weitere Datenträger anfordert, lokalisieren Sie Datenträger und stellen Sie diese von der Überlaufposition zurück.

Um Datenträger an einer Überlaufposition zu finden, geben Sie den Befehl QUERY MEDIA aus. Sie können den Befehl QUERY MEDIA auch verwenden, um Befehle zum Zurückstellen von Datenträgern zu generieren.

Um beispielsweise die Datenträger an der Überlaufposition aufzulisten und gleichzeitig die Befehle zum Zurückstellen dieser Datenträger in das Speicherarchiv zu generieren, geben Sie einen ähnlichen Befehl wie in dem folgenden Beispiel aus:

```
query media format=cmd stgpool=archivepool whereovflocation=Room2948  
cmd="checkin libvol autolib &vol status=private"  
cmdfilename="\storage\move\media\checkin.vols"
```

#### Tipps:

- o Mountainforderungen vom Server umfassen den Standort der Datenträger.
- o Um die Anzahl Tage anzugeben, die verstreichen müssen, bevor die Datenträger für die Verarbeitung auswählbar sind, geben Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters REUSEDELAY aus.
- o Die Datei, die die generierten Befehle enthält, kann mit dem IBM Spectrum Protect-Befehl MACRO ausgeführt werden.

### Zugehörige Verweise:

- 🔗 MOVE MEDIA (Speicherpooldatenträger mit sequenziellem Zugriff versetzen)
- 🔗 QUERY MEDIA (Speicherpooldatenträger mit sequenziellem Zugriff abfragen)
- 🔗 UPDATE STGPOOL (Speicherpool aktualisieren)

## Datenträgerbestand in einem Speicherarchiv prüfen

Sie können ein automatisiertes Speicherarchiv prüfen, um sicherzustellen, dass der Datenträgerbestand des Speicherarchivs mit den Datenträgern konsistent ist, die physisch in dem Speicherarchiv vorhanden sind. Die Prüfung eines Speicherarchivs bietet sich an, wenn

der Datenträgerbestand des Speicherarchivs aufgrund manueller Versetzungen der Datenträger in dem Speicherarchiv oder aufgrund von Datenbankproblemen nicht mehr korrekt ist.

## Vorgehensweise

---

1. Stellen Sie sicher, dass keine Datenträger in den Speicherarchivlaufwerken bereitgestellt sind. Wenn Datenträger im Status IDLE (Inaktiv) bereitgestellt sind, geben Sie den Befehl DISMOUNT VOLUME aus, um die Bereitstellung dieser Datenträger aufzuheben.
2. Prüfen Sie den Datenträgerbestand, indem Sie den Befehl AUDIT LIBRARY ausgeben. Führen Sie eine der folgenden Aktionen aus:
  - Wenn das Speicherarchiv über einen Barcodeleser verfügt, können Sie Zeit sparen, indem Sie Datenträger mithilfe des Barcodelesers identifizieren. Um beispielsweise das Speicherarchiv TAPELIB mithilfe seines Barcodelesers zu prüfen, geben Sie den folgenden Befehl aus:

```
audit library tapelib checklabel=barcode
```
  - Wenn das Speicherarchiv über keinen Barcodeleser verfügt, geben Sie den Befehl AUDIT LIBRARY ohne Angabe von CHECKLABEL=BARCODE aus. Jeder Datenträger wird vom Server zur Überprüfung seines Kennsatzes bereitgestellt. Nachdem der Kennsatz überprüft wurde, führt der Server die Überprüfung für alle verbleibenden Datenträger aus.

## Ergebnisse

---

Der Server löscht fehlende Datenträger aus dem Bestand und aktualisiert die Positionen von Datenträgern, die seit der letzten Prüfung versetzt wurden.

Einschränkung: Während einer Prüfoperation kann der Server dem Bestand keine neuen Datenträger hinzufügen.

### Zugehörige Tasks:

Banddatenträgern Kennsätze zuordnen

### Zugehörige Verweise:

- ➔ AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Speicherarchiv prüfen)
- ➔ DISMOUNT VOLUME (Datenträger nach Datenträgername abhängen)

## Teilweise beschriebene Datenträger

---

Teilweise beschriebene Datenträger sind immer private Datenträger; dies ist auch dann der Fall, wenn ihr Status vor dem Bereitstellen durch den Server PRIVATE lautete. Der Server protokolliert den ursprünglichen Status von Arbeitsdatenträgern und versetzt diese wieder in den Arbeitsstatus, wenn sie leer sind.

Mit Ausnahme von Datenträgern in automatisierten Speicherarchiven erkennt der Server einen Arbeitsdatenträger erst nach dessen Bereitstellung. Der Datenträgerstatus ändert sich dann in PRIVATE und der Datenträger wird automatisch als Teil des Speicherpools definiert, für den die Mountanforderung erfolgte.

### Zugehörige Tasks:

Status eines Datenträgers in einem automatisierten Speicherarchiv ändern

## Operationen für gemeinsam genutzte Speicherarchive

---

Gemeinsam genutzte Speicherarchive sind logische Speicherarchive, die physisch durch SCSI-Speicherarchive dargestellt werden. Das physische Speicherarchiv wird durch den IBM Spectrum Protect-Server gesteuert, der als Speicherarchivmanager konfiguriert ist. IBM Spectrum Protect-Server, die den Speicherarchivtyp SHARED verwenden, sind Speicherarchivclients für den IBM Spectrum Protect-Speicherarchivmanager-Server.

Der Speicherarchivclient kontaktiert den Speicherarchivmanager, wenn der Speicherarchivmanager startet und die Speichereinheit initialisiert wird oder nachdem ein Speicherarchivmanager für einen Speicherarchivclient definiert wurde. Der Speicherarchivclient bestätigt, dass der kontaktierte Server der Speicherarchivmanager für die angegebene Speicherarchivereinheit ist. Der Speicherarchivclient vergleicht außerdem die Laufwerkdefinitionen mit dem Speicherarchivmanager auf Konsistenz. Der Speicherarchivclient kontaktiert den Speicherarchivmanager für jede der folgenden Operationen:

### Datenträgermount

Ein Speicherarchivclient sendet eine Zugriffsanforderung für einen bestimmten Datenträger in der gemeinsam genutzten Speicherarchivereinheit an den Speicherarchivmanager. Bei einem Arbeitsdatenträger gibt der Speicherarchivclient keinen Datenträgernamen an. Wenn der Speicherarchivmanager nicht auf den angeforderten Datenträger zugreifen kann oder wenn keine Arbeitsdatenträger verfügbar sind, weist der Speicherarchivmanager die Mountanforderung zurück. Wenn der Mount erfolgreich ist, gibt der Speicherarchivmanager den Namen des Laufwerks zurück, in dem der Datenträger bereitgestellt ist.

### Datenträgerfreigabe

Wenn ein Speicherarchivclient nicht mehr auf einen Datenträger zugreifen muss, teilt er dem Speicherarchivmanager mit, dass der Datenträger wieder als Arbeitsdatenträger verwendet werden kann. Die Datenbank des Speicherarchivmanagers wird mit der

neuen Position des Datenträgers, der sich jetzt im Bestand des Speicherarchivservers befindet, aktualisiert. Der Datenträger wird aus dem Datenträgerbestand des Speicherarchivclients gelöscht.

Tabelle 1 zeigt die Interaktion zwischen Speicherarchivclients und dem Speicherarchivmanager bei der Verarbeitung von IBM Spectrum Protect-Operationen.

Tabelle 1. Wie SAN-fähige Server IBM Spectrum Protect-Operationen verarbeiten

| Operation<br>(Befehl)  | Speicherarchivmanager   | Speicherarchivclient   |
|--|---|--|
| Datenträger im Speicherarchiv abfragen<br><br>(QUERY LIBVOLUME)                                      | Zeigt die in das Speicherarchiv zurückgestellten Datenträger an. Bei privaten Datenträgern wird außerdem der Eignerserver angezeigt.            | Nicht zutreffend   |
| Speicherarchivdatenträger zurückstellen und entnehmen<br><br>(CHECKIN LIBVOLUME, CHECKOUT LIBVOLUME) | Sendet die Befehle an die Speicherarchivereinheit.  | Nicht zutreffend<br><br>Wenn eine Zurückstelloperation aufgrund einer Clientzurückschreibungsoperation erforderlich ist, wird eine Anforderung an den Speicherarchivmanager-Server gesendet. |
| Datenträger und DRM-Datenträger versetzen<br><br>(MOVE MEDIA, MOVE DRMEDIA)                          | Nur gültig für Datenträger, die vom Speicherarchivmanager-Server verwendet werden.  | Fordert die Ausführung der Operationen vom Speicherarchivmanager-Server an. Generiert einen Entnahmeprozess auf dem Speicherarchivmanager-Server.  |
| Speicherarchivbestand prüfen<br><br>(AUDIT LIBRARY)  | Synchronisiert den Bestand mit der Speicherarchivereinheit.   | Synchronisiert den Bestand mit dem Speicherarchivmanager-Server.   |
| Datenträger im Speicherarchiv einen Kennsatz zuordnen<br><br>(LABEL LIBVOLUME)                       | Ordnet Datenträgern Kennsätze zu und stellt Datenträger zurück.   | Nicht zutreffend   |
| Bereitstellung eines Datenträgers aufheben<br><br>(DISMOUNT VOLUME)                                  | Sendet die Anforderung an die Speicherarchivereinheit.  | Fordert die Ausführung der Operationen vom Speicherarchivmanager-Server an.  |
| Datenträger abfragen<br><br>(QUERY VOLUME)   | Prüft, ob der anfordernde Speicherarchivclient Eigner des Datenträgers ist und ob sich der Datenträger in der Speicherarchivereinheit befindet. | Fordert die Ausführung der Operationen vom Speicherarchivmanager-Server an.  |

## Serveranforderungen für Datenträger verwalten

IBM Spectrum Protect zeigt allen Verwaltungsbefehlszeilenclients, die im Konsolenmodus gestartet werden, Anforderungen und Statusnachrichten an. Für diese Anforderungsnachrichten ist häufig ein Zeitlimit festgelegt. Erfolgreiche Serveroperationen müssen innerhalb des angegebenen Zeitlimits abgeschlossen werden; andernfalls tritt für die Operation eine Zeitlimitüberschreitung auf.

### Informationen zu diesem Vorgang

Verwenden Sie bei automatisierten Speicherarchiven die Befehle CHECKIN LIBVOLUME und LABEL LIBVOLUME, um Kassetten in Schächte einzulegen. Wenn Sie einen Wert für den Parameter WAITTIME angeben, wird eine Antwortnachricht angezeigt. Wenn der Wert des Parameters 0 ist, ist keine Antwort erforderlich. Wenn Sie den Befehl CHECKOUT LIBVOLUME ausgeben, müssen Sie Kassetten in Schächte einlegen und es wird in jedem Fall eine Antwortnachricht angezeigt.


## Vorgehensweise

Die folgende Tabelle enthält Informationen zur Handhabung verschiedener Serverdatenträgertasks.

| Task   | Details  |
|--|--|
| Verwaltungsclient für Mountnachrichten verwenden             | <p>Der Server sendet Statusnachrichten für Mountanforderungen an die Serverkonsole und an alle Verwaltungsbefehlszeilenclients im Mountmodus oder Konsolenmodus.</p> <p>Um einen Verwaltungsbefehlszeilenclient im Mountmodus zu starten, geben Sie im Verwaltungsbefehlszeilenclient den Befehl <code>dsmadm -mountmode</code> aus.</p>   |
| Nachrichten zu automatisierten Speicherarchiven empfangen    | <p>Sie können Mountnachrichten und Fehlernachrichten zu automatisierten Speicherarchiven auf Verwaltungsbefehlszeilenclients im Mountmodus oder Konsolenmodus anzeigen. Mountnachrichten werden an das Speicherarchiv und nicht an einen Bediener gesendet. Nachrichten zu Problemen mit dem Speicherarchiv werden an die Mountnachrichtenwarteschlange gesendet.</p>  |
| Informationen zu anstehenden Bedieneranforderungen abrufen   | <p>Um Informationen zu anstehenden Bedieneranforderungen abzurufen, geben Sie den Befehl <code>QUERY REQUEST</code> aus oder zeigen Sie die Mountnachrichtenwarteschlange auf einem Verwaltungsbefehlszeilenclient an, der im Mountmodus gestartet wurde. Wenn Sie den Befehl <code>QUERY REQUEST</code> ausgeben, zeigt der Server angeforderte Aktionen und die verbleibende Zeit, bevor das Zeitlimit für die Anforderungen überschritten wird.</p>   |
| Bedieneranforderungen beantworten                            | <p>Wenn der Server eine explizite Antwort auf eine abgeschlossene Mountanforderung erfordert, verwenden Sie den Befehl <code>REPLY</code>.</p> <p>Der Parameter <i>Anforderungsnummer</i> gibt die Anforderungsidentifikationsnummer an, die dem Server anzeigt, welche anstehende Bedieneranforderung abgeschlossen ist. Diese dreistellige Zahl wird immer in der Anforderungsnachricht angezeigt.</p>   |
| Bedieneranforderung abbrechen                                | <p>Um eine Mountanforderung für ein Speicherarchiv abzubrechen, geben Sie den Befehl <code>CANCEL REQUEST</code> aus. Bei den meisten Anforderungen, die automatisierten SCSI-Speicherarchiven zugeordnet sind, muss ein Bediener eine Hardware- oder Systemaktion ausführen, um den angeforderten Mount abzubrechen. Bei derartigen Anforderungen wird der Befehl <code>CANCEL REQUEST</code> nicht vom Server akzeptiert.</p> <p>Der Befehl <code>CANCEL REQUEST</code> muss die Anforderungsidentifikationsnummer enthalten. Diese Nummer ist in die Anforderungsnachricht eingeschlossen.</p> <p>Wenn der angeforderte Datenträger als <code>UNAVAILABLE</code> markiert werden soll, geben Sie den Befehl <code>CANCEL REQUEST</code> unter Angabe des Parameters <code>PERMANENT</code> aus. Wenn Sie den Parameter <code>PERMANENT</code> angeben, versucht der Server nicht, den angeforderten Datenträger erneut bereitzustellen. Dies ist beispielsweise hilfreich, wenn sich der Datenträger an einem fernen Standort befindet oder aus einem anderen Grund nicht verfügbar ist.</p>  |
| Anforderung zum Zurückstellen eines Datenträgers beantworten | <p>Wenn der Server einen bestimmten Datenträger, der in einem automatisierten Speicherarchiv bereitgestellt werden soll, nicht finden kann, fordert der Server den Bediener zum Zurückstellen des Datenträgers auf.</p> <p>Wenn der angeforderte Datenträger verfügbar ist, legen Sie den Datenträger in das Speicherarchiv ein und stellen Sie ihn zurück. Weitere Informationen finden Sie in <i>Datenträger in ein automatisiertes Speicherarchiv zurückstellen</i>.</p> <p>Wenn der angeforderte Datenträger nicht verfügbar ist, aktualisieren Sie den Zugriffsmodus des Datenträgers, indem Sie den Befehl <code>UPDATE VOLUME</code> unter Angabe des Parameters <code>ACCESS=UNAVAILABLE</code> ausgeben. Brechen Sie dann die Zurückstellenanforderung mit dem Befehl <code>CANCEL REQUEST</code> ab. Brechen Sie nicht den Clientprozess ab, der die Anforderung zur Folge hatte! Rufen Sie mithilfe des Befehls <code>QUERY REQUEST</code> die ID der Anforderung ab, die abgebrochen werden soll.</p> <p>Wenn Sie nicht innerhalb der für die Einheitenklasse des Speicherpools angegebene Mountwartezeit auf die Zurückstellenanforderung des Servers antworten, markiert der Server den Datenträger als nicht verfügbar.</p> |

| Task  | Details  |
|---|--|
| Bereitgestellte Datenträger bestimmen         | Um einen Bericht zu allen Datenträgern anzufordern, die momentan für die Verwendung durch den Server bereitgestellt sind, geben Sie den Befehl QUERY MOUNT aus. Der Bericht zeigt, welche Datenträger bereitgestellt sind, welche Laufwerke auf die Datenträger zugegriffen haben und ob die Datenträger im Gebrauch sind.   |
| Bereitstellung inaktiver Datenträger aufheben | <p>Wenn ein Datenträger inaktiv ist, hebt der Server die Bereitstellung des Datenträgers nicht sofort auf; der Datenträger bleibt vielmehr so lange bereitgestellt, wie im Parameter für den Mount-Aufbewahrungszeitraum für die Einheitenklasse angegeben ist. Durch die Verwendung eines Mount-Aufbewahrungszeitraums kann die Zugriffszeit reduziert werden, wenn Datenträger wiederholt verwendet werden.</p> <p>Um die Bereitstellung eines inaktiven Datenträgers für das Laufwerk aufzuheben, in dem er bereitgestellt ist, geben Sie den Befehl DISMOUNT VOLUME aus.</p> <p>Informationen zum Festlegen des Mount-Aufbewahrungszeitraums finden Sie in Steuern, wie lange ein Datenträger bereitgestellt bleibt.</p> |

#### Zugehörige Informationen:

 QUERY REQUEST (Eine oder mehrere anstehende Mountanforderungen abfragen)

## Bandlaufwerke verwalten

Sie können Bandlaufwerke abfragen, aktualisieren und löschen. Außerdem können Sie Bandlaufwerke reinigen und Bandlaufwerkverschlüsselung und Datenprüfung konfigurieren.

- **Laufwerke aktualisieren**  
Sie können die Attribute einer Laufwerkdefinition ändern, um ein Laufwerk offline zu schalten oder ein Laufwerk zu rekonfigurieren.
- **Datenprüfung während Schreib-/Leseoperationen auf Band**  
Um Daten zu prüfen und beschädigte Daten zu identifizieren, können Sie eine Funktion verwenden, die als 'Schutz logischer Blöcke' bezeichnet wird. Wenn Sie den Schutz logischer Blöcke verwenden, fügt IBM Spectrum Protect einen Wert für zyklische Blockprüfung (CRC = Cyclic Redundancy Check) am Ende jedes logischen Blocks mit Daten ein, während die Daten auf Band geschrieben werden.
- **Bandlaufwerke reinigen**  
Die Steuerung der Bandlaufwerkreinigung kann durch den Server erfolgen. Der Server kann steuern, wie Bandlaufwerke in SCSI-Speicherarchiven gereinigt werden.
- **Bandlaufwerke ersetzen**  
Wenn Sie ein Laufwerk in einem Bandarchiv ersetzen, das für IBM Spectrum Protect definiert ist, müssen Sie die Laufwerk- und Pfaddefinitionen für das alte Laufwerk löschen und das neue Laufwerk samt Pfad definieren.

## Laufwerke aktualisieren

Sie können die Attribute einer Laufwerkdefinition ändern, um ein Laufwerk offline zu schalten oder ein Laufwerk zu rekonfigurieren.

### Informationen zu diesem Vorgang

Sie können die folgenden Attribute eines Laufwerks ändern:

- Die Elementadresse, wenn sich das Laufwerk in einem SCSI-Speicherarchiv befindet
- Die Reinigungshäufigkeit
- Den Laufwerkstatus: ONLINE oder OFFLINE

Einschränkung: Wenn ein Laufwerk im Gebrauch ist, können Sie die Elementnummer oder den Einheitennamen nicht ändern.

Anweisungen zum Offlineschalten von Laufwerken finden Sie in Bandlaufwerke offline schalten.

Wenn ein Datenträger im Laufwerk bereitgestellt, aber inaktiv ist, kann seine Bereitstellung explizit aufgehoben werden. Anweisungen zum Aufheben der Bereitstellung inaktiver Datenträger finden Sie in Serveranforderungen für Datenträger verwalten.

### Vorgehensweise

- Ändern Sie die Elementadresse eines Laufwerks, indem Sie den Befehl UPDATE DRIVE ausgeben. Ändern Sie beispielsweise in einem Speicherarchiv mit dem Namen AUTO die Elementadresse von DRIVE3 in 119, indem Sie den folgenden Befehl ausgeben:

```
update drive auto drive3 element=119
```

- Ändern Sie den Einheitennamen eines Laufwerks, indem Sie den Befehl UPDATE PATH ausgeben. Um beispielsweise den Einheitennamen eines Laufwerks mit dem Namen DRIVE3 zu ändern, geben Sie den folgenden Befehl aus:

#### AIX-Betriebssysteme

```
update path server1 drive3 srctype=server desttype=drive library=scsilib
device=/dev/rmt0
```

#### Linux-Betriebssysteme

```
update path server1 drive3 srctype=server desttype=drive library=scsilib
device=/dev/IBMtape0
```

#### Windows-Betriebssysteme

```
update path server1 drive3 srctype=server desttype=drive library=scsilib
device=mt3.0.0.0
```

- Bandlaufwerke offline schalten  
Sie können ein Bandlaufwerk offline schalten, während es im Gebrauch ist. Sie können ein Laufwerk beispielsweise zur Ausführung der Wartung offline schalten.

#### Zugehörige Verweise:

 UPDATE PATH (Pfad ändern)

#### Zugehörige Informationen:

 UPDATE DRIVE (Laufwerk aktualisieren)

## Datenprüfung während Schreib-/Leseoperationen auf Band

Um Daten zu prüfen und beschädigte Daten zu identifizieren, können Sie eine Funktion verwenden, die als 'Schutz logischer Blöcke' bezeichnet wird. Wenn Sie den Schutz logischer Blöcke verwenden, fügt IBM Spectrum Protect einen Wert für zyklische Blockprüfung (CRC = Cyclic Redundancy Check) am Ende jedes logischen Blocks mit Daten ein, während die Daten auf Band geschrieben werden.

Der Schutz logischer Blöcke ermöglicht es Ihnen, Fehler zu identifizieren, die auftreten, während Daten auf Band geschrieben werden und während Daten über das Speicherbereichsnetz vom Bandlaufwerk an IBM Spectrum Protect übertragen werden. Laufwerke, die den Schutz logischer Blöcke unterstützen, prüfen Daten während Lese- und Schreiboperationen. Der IBM Spectrum Protect-Server prüft Daten während Leseoperationen.

Wenn die Prüfung durch das Laufwerk während Schreiboperationen fehlschlägt, kann dies darauf hinweisen, dass Daten während der Übertragung auf Band beschädigt wurden. In diesem Fall schlägt die Schreiboperation für den IBM Spectrum Protect-Server fehl. Sie müssen die Operation erneut starten, um fortfahren zu können. Wenn die Prüfung durch das Laufwerk während Leseoperationen fehlschlägt, kann dies darauf hinweisen, dass die Banddatenträger beschädigt sind. Wenn die Prüfung durch den IBM Spectrum Protect-Server während Leseoperationen fehlschlägt, kann dies darauf hinweisen, dass die Daten während der Übertragung vom Bandlaufwerk beschädigt wurden; der Server versucht, die Operation erneut auszuführen. Wenn die Prüfung durchgängig fehlschlägt, gibt der IBM Spectrum Protect-Server eine Fehlermeldung aus, die auf Hardwarefehler oder Verbindungsprobleme hinweist.

Wenn der Schutz logischer Blöcke auf einem Bandlaufwerk inaktiviert ist oder das Laufwerk den Schutz logischer Blöcke nicht unterstützt, kann der IBM Spectrum Protect-Server geschützte Daten nur lesen. Die Daten werden jedoch nicht geprüft.

Der Schutz logischer Blöcke hat eine höhere Priorität als die zyklische Blockprüfung, die Sie beim Definieren oder Aktualisieren einer Speicherpooldefinition angeben können. Wenn Sie die zyklische Blockprüfung für einen Speicherpool angeben, werden Daten nur während Datenträgerprüfoperationen geprüft. Fehler werden identifiziert, nachdem die Daten auf Band geschrieben wurden.

Einschränkungen:

- Sie können den Schutz logischer Blöcke nicht für sequenzielle Daten wie Sicherungsgruppen und Datenbanksicherungen verwenden.
- Die CRC-Prüfung hat Auswirkungen auf die Leistung, da mehr Prozessorauslastung auf dem Client und dem Server erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen.
- Ändern Sie bei einem Arbeitsdatenträger, wenn Sie den Schutz logischer Blöcke für Schreib-/Leseoperationen (LBPROTECT=READWRITE) angeben, den Parameterwert nicht, nachdem Daten auf den Datenträger geschrieben wurden. Das Ändern des Parameterwerts während des Lebenszyklus des Datenträgers auf dem IBM Spectrum Protect-Server wird nicht unterstützt.
- Laufwerke, die den Schutz logischer Blöcke unterstützen  
Der Schutz logischer Blöcke ist nur für die Einheitentypen 3592, LTO und ECARTRIDGE verfügbar. 3592-Laufwerke, die diese Art von Schutz bereitstellen, umfassen IBM TS1130, TS1140 und spätere Generationen. LTO-Laufwerke, die diese Art von Schutz bereitstellen, umfassen IBM LTO-5-Laufwerke und unterstützte LTO-6-Laufwerke. Oracle StorageTek-Laufwerke, die diese Art von Schutz bereitstellen, umfassen Laufwerke mit dem T10000C-Format und dem T10000D-Format.

- Schutz logischer Blöcke aktivieren und inaktivieren  
Sie können den Schutz logischer Blöcke für Lese- und Schreiboperationen oder ausschließlich für Schreiboperationen angeben. Es ist auch möglich, den Schutz logischer Blöcke zu inaktivieren. Standardmäßig ist der Schutz logischer Blöcke wegen der Auswirkungen, die die zyklische Blockprüfung auf dem Server und dem Bandlaufwerk auf die Leistung hat, inaktiviert.
- Schreib-/Leseoperationen für Datenträger mit Schutz logischer Blöcke  
Schreib-/Leseoperationen für leere Datenträger oder Datenträger, die mit Daten gefüllt werden, sind davon abhängig, ob für die Datenträger der Schutz logischer Blöcke definiert ist. Geschützte und ungeschützte Datenblöcke können nicht auf demselben Datenträger gemischt werden.
- Speicherpoolverwaltung in einem Bandarchiv  
Um geschützte und ungeschützte Daten in einem Speicherarchiv zu mischen, müssen Sie unterschiedliche Einheitenklassen und unterschiedliche Speicherpools erstellen, um die Daten voneinander zu trennen. Wenn eine Einheitenklasse geschützten Daten zugeordnet ist, können Sie den Schutz logischer Blöcke für Lese- und Schreiboperationen oder ausschließlich für Schreiboperationen angeben.

## Laufwerke, die den Schutz logischer Blöcke unterstützen

Der Schutz logischer Blöcke ist nur für die Einheitentypen 3592, LTO und ECARTRIDGE verfügbar. 3592-Laufwerke, die diese Art von Schutz bereitstellen, umfassen IBM TS1130, TS1140 und spätere Generationen. LTO-Laufwerke, die diese Art von Schutz bereitstellen, umfassen IBM LTO-5-Laufwerke und unterstützte LTO-6-Laufwerke. Oracle StorageTek-Laufwerke, die diese Art von Schutz bereitstellen, umfassen Laufwerke mit dem T10000C-Format und dem T10000D-Format.

In der folgenden Tabelle sind die Datenträger und Formate aufgeführt, die Sie zusammen mit Laufwerken verwenden können, die den Schutz logischer Blöcke unterstützen.

| Laufwerk       | Banddatenträger                        | Laufwerkformate  |
|----------------|--|--|
| IBM TS1130     | 3592 Generation 2                      | 3592-3 und 3592-3C   |
| IBM TS1140     | 3592 Generation 2<br>3592 Generation 3 | Generation 2: 3592-3 und 3592-3C<br>Generation 3: 3592-4 und 3592-4C |
| IBM TS1150     | 3592 Generation 3<br>3592 Generation 4 | Generation 4: 3592-5 und 3592-5C                                     |
| IBM LTO-5      | LTO-5                                  | Ultrium 5 und Ultrium 5C   |
| IBM LTO-6      | LTO-6<br>LTO-5                         | Ultrium 6 und Ultrium 6C<br>Ultrium 5 und Ultrium 5C                 |
| IBM LTO-7      | LTO-7<br>LTO-6                         | Ultrium 7 und Ultrium 7C<br>Ultrium 6 und Ultrium 6C                 |
| Oracle T10000C | Oracle StorageTek T10000 T2            | T10000C und T10000C-C  |
| Oracle T10000D | Oracle StorageTek T10000 T2            | T10000D und T10000D-C  |

Tipps:

- Um den Schutz logischer Blöcke für einen Banddatenträger zu aktivieren und den Datenträger dann zum Sichern von Daten wiederzuverwenden, müssen Sie den Schutz logischer Blöcke für die Einheitenklasse und das Laufwerk aktivieren.
- Bei einem 3592-, LTO- oder Oracle StorageTek-Laufwerk, das keinen Schutz logischer Blöcke bereitstellen kann, können Sie für das Laufwerk ein Upgrade mit Firmware durchführen, die Schutz logischer Blöcke bereitstellt.

Der Schutz logischer Blöcke ist für Laufwerke in Speicherarchiven des Typs SCSI verfügbar. Aktuelle Informationen zur Unterstützung für den Schutz logischer Blöcke finden Sie in Technote 1568108.

Um den Schutz logischer Blöcke für Schreiboperationen verwenden zu können, müssen alle Laufwerke in einem Speicherarchiv den Schutz logischer Blöcke unterstützen. Wenn ein Laufwerk keinen Schutz logischer Blöcke bereitstellen kann, werden Datenträger mit Schreib-/Lesezugriff nicht bereitgestellt. Der Server kann jedoch mithilfe des Laufwerks Datenträger mit Lesezugriff bereitstellen. Die geschützten Daten werden vom IBM Spectrum Protect-Server gelesen und geprüft, wenn der Schutz logischer Blöcke für Schreib-/Leseoperationen aktiviert ist.

## Schutz logischer Blöcke aktivieren und inaktivieren

Sie können den Schutz logischer Blöcke für Lese- und Schreiboperationen oder ausschließlich für Schreiboperationen angeben. Es ist auch möglich, den Schutz logischer Blöcke zu inaktivieren. Standardmäßig ist der Schutz logischer Blöcke wegen der Auswirkungen, die die zyklische Blockprüfung auf dem Server und dem Bandlaufwerk auf die Leistung hat, inaktiviert.

## Informationen zu diesem Vorgang

---

Schreib-/Leseoperationen für leere Datenträger oder Datenträger, die mit Daten gefüllt werden, sind davon abhängig, ob für die Datenträger der Schutz logischer Blöcke definiert ist. Geschützte und ungeschützte Datenblöcke können nicht auf demselben Datenträger gemischt werden. Wenn Sie die Einstellung für den Schutz logischer Blöcke ändern, gilt die Änderung nur für leere Datenträger. Datenträger, die mit Daten gefüllt werden, und volle Datenträger behalten ihren Status für den Schutz logischer Blöcke bei, bis sie leer und zum erneuten Füllen bereit sind. Wenn Sie beispielsweise den Schutz logischer Blöcke inaktivieren und der Server einen Datenträger auswählt, der einer Einheitenklasse zugeordnet ist, für die der Schutz logischer Blöcke definiert ist, schreibt der Server weiterhin geschützte Daten auf den Datenträger.

Einschränkung: Der Schutz logischer Blöcke ist nur für bestimmte Einheitentypen verfügbar. Weitere Informationen finden Sie in Laufwerke, die den Schutz logischer Blöcke unterstützen.

## Vorgehensweise

---

1. Um den Schutz logischer Blöcke für die Einheitentypen 3592, LTO und ECARTRIDGE zu aktivieren, geben Sie den Befehl DEFINE DEVCLASS oder den Befehl UPDATE DEVCLASS unter Angabe des Parameters LBPROTECT aus. Um beispielsweise den Schutz logischer Blöcke während Lese- und Schreiboperationen für eine Einheitenklasse 3592 mit dem Namen 3592\_lbprotect anzugeben, geben Sie den folgenden Befehl aus:

```
define devclass 3592_lbprotect library=3594 lbprotect=readwrite
```

Tipps:

- Wenn Sie den Wert des Parameters LBPROTECT von NO in READWRITE oder WRITEONLY ändern und der Server einen Datenträger auswählt, der mit Daten gefüllt wird und für den kein Schutz logischer Blöcke für Schreiboperationen definiert ist, gibt der Server jedes Mal eine Nachricht aus, wenn der Datenträger bereitgestellt wird. Die Nachricht gibt an, dass Daten auf den Datenträger ohne Schutz logischer Blöcke geschrieben werden. Soll die Anzeige dieser Nachricht verhindert werden oder soll IBM Spectrum Protect nur Daten mit Schutz logischer Blöcke auf den Datenträger schreiben, ändern Sie den Zugriff für Datenträger ohne Schutz logischer Blöcke, die mit Daten gefüllt werden, in Lesezugriff.
  - Um die Leistung zu verbessern, geben Sie den Parameter CRCDATA nicht im Befehl DEFINE STGPOOL oder UPDATE STGPOOL an.
  - Wenn Daten während Leseoperationen sowohl vom Laufwerk als auch vom IBM Spectrum Protect-Server geprüft werden, kann dies die Serverleistung während Zurückschreibungs- und Abrufoperationen verschlechtern. Um die für Zurückschreibungs- und Abrufoperationen erforderliche Zeit zu verringern, ändern Sie die Einstellung des Parameters LBPROTECT von READWRITE in WRITEONLY. Nachdem die Daten zurückgeschrieben oder abgerufen wurden, können Sie den Parameter LBPROTECT auf READWRITE zurücksetzen.
2. Um den Schutz logischer Blöcke zu inaktivieren, geben Sie den Befehl DEFINE DEVCLASS oder den Befehl UPDATE DEVCLASS unter Angabe des Parameters LBPROTECT=NO aus.  
Einschränkung: Wenn der Schutz logischer Blöcke inaktiviert ist, schreibt der Server keine Daten auf ein leeres Band, für das der Schutz logischer Blöcke definiert ist. Wenn jedoch ein Datenträger, der mit Daten gefüllt wird und für den der Schutz logischer Blöcke definiert ist, ausgewählt wird, schreibt der Server weiterhin Daten auf den Datenträger, für den der Schutz logischer Blöcke definiert ist. Um zu verhindern, dass der Server Daten auf Bänder mit Schutz logischer Blöcke schreibt, ändern Sie den Zugriff für Datenträger, die mit Daten gefüllt werden und für die der Schutz logischer Blöcke definiert ist, in Lesezugriff. Wenn Daten gelesen werden, werden die Ergebnisse der zyklischen Blockprüfung nicht vom Laufwerk oder Server geprüft.

Wenn in einem Katastrophenfall der Standort zur Wiederherstellung über keine Laufwerke verfügt, die den Schutz logischer Blöcke unterstützen, müssen Sie den Parameter LBPROTECT=NO angeben. Wenn die Bandlaufwerke für Schreiboperationen verwendet werden, müssen Sie den Datenträgerzugriff für Datenträger mit geschützten Daten in Lesezugriff ändern, um eine Verwendung der Datenträger durch den Server zu verhindern.

Wenn der Server den Schutz logischer Blöcke aktivieren muss, gibt der Server eine Fehlernachricht aus, die angibt, dass das Laufwerk den Schutz logischer Blöcke nicht unterstützt.

## Nächste Schritte

---

Um festzustellen, ob für einen Datenträger der Schutz logischer Blöcke definiert ist, geben Sie den Befehl QUERY VOLUME aus und prüfen Sie den Wert im Feld `Schutz logischer Blöcke`.

### Zugehörige Verweise:

- [DEFINE DEVCLASS \(Einheitenklasse definieren\)](#)
- [UPDATE STGPOOL \(Speicherpool aktualisieren\)](#)

### Zugehörige Informationen:



- ➔ DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)
- ➔ QUERY VOLUME (Speicherpooldatenträger abfragen)
- ➔ UPDATE DEVCLASS (Einheitenklasse aktualisieren)

## Schreib-/Leseoperationen für Datenträger mit Schutz logischer Blöcke

---

Schreib-/Leseoperationen für leere Datenträger oder Datenträger, die mit Daten gefüllt werden, sind davon abhängig, ob für die Datenträger der Schutz logischer Blöcke definiert ist. Geschützte und ungeschützte Datenblöcke können nicht auf demselben Datenträger gemischt werden.

Wenn Sie mit dem Befehl UPDATE DEVCLASS die Einstellung für den Schutz logischer Blöcke ändern, gilt die Änderung nur für leere Datenträger. Datenträger, die mit Daten gefüllt werden, und volle Datenträger behalten ihren Status für den Schutz logischer Blöcke bei, bis sie leer und zum erneuten Füllen bereit sind.

Angenommen, Sie ändern den Wert des Parameters LBPROTECT von READWRITE in NO. Wenn der Server einen Datenträger auswählt, der der Einheitenklasse zugeordnet ist und über Schutz logischer Blöcke verfügt, schreibt der Server weiterhin geschützte Daten auf den Datenträger.

Tipps:

- Wenn ein Laufwerk den Schutz logischer Blöcke nicht unterstützt, können Datenträger mit Schutz logischer Blöcke für Schreiboperationen nicht bereitgestellt werden. Um zu verhindern, dass der Server den geschützten Datenträger für Schreiboperationen bereitstellt, ändern Sie den Datenträgerzugriff in Lesezugriff. Inaktivieren Sie außerdem den Schutz logischer Blöcke, um zu verhindern, dass der Server die Funktion auf dem Bandlaufwerk aktiviert.
- Wenn ein Laufwerk den Schutz logischer Blöcke nicht unterstützt und der Schutz logischer Blöcke inaktiviert ist, liest der Server Daten von geschützten Datenträgern. Die Daten werden jedoch nicht vom Server und dem Bandlaufwerk geprüft.

### Zugehörige Informationen:

- ➔ QUERY VOLUME (Speicherpooldatenträger abfragen)
- ➔ UPDATE DEVCLASS (Einheitenklasse aktualisieren)

## Speicherpoolverwaltung in einem Bandarchiv

---

Um geschützte und ungeschützte Daten in einem Speicherarchiv zu mischen, müssen Sie unterschiedliche Einheitenklassen und unterschiedliche Speicherpools erstellen, um die Daten voneinander zu trennen. Wenn eine Einheitenklasse geschützten Daten zugeordnet ist, können Sie den Schutz logischer Blöcke für Lese- und Schreiboperationen oder ausschließlich für Schreiboperationen angeben.

Um Einheitenklassen und Speicherpools für ein TS3500-Speicherarchiv mit LTO-5-Laufwerken für geschützte und ungeschützte Daten zu definieren, können Sie eine Folge von Befehlen ausgeben wie in dem folgenden Beispiel gezeigt:

```
define library 3584 libtype=scsi
define devclass lbprotect library=3584 devicetype=lto lbprotect=readwrite
define devclass normal library=3584 devicetype=lto lbprotect=no
define stgpool lbprotect_pool lbprotect maxxscratch=10
define stgpool normal_pool normal maxxscratch=10
```

### Zugehörige Verweise:

- ➔ DEFINE DEVCLASS (Einheitenklasse definieren)

### Zugehörige Informationen:

- ➔ DEFINE LIBRARY (Speicherarchiv definieren)
- ➔ DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

## Bandlaufwerke reinigen

---

Die Steuerung der Bandlaufwerkreinigung kann durch den Server erfolgen. Der Server kann steuern, wie Bandlaufwerke in SCSI-Speicherarchiven gereinigt werden.

### Informationen zu diesem Vorgang

---

Um Bandlaufwerke reinigen zu können, müssen Sie über Systemberechtigung oder uneingeschränkte Speicherberechtigung verfügen. Bei automatisierten Speicherarchiven können Sie die Reinigung automatisieren, indem Sie die Häufigkeit der Reinigungsoperationen angeben und eine Reinigungskassette in den Datenträgerbestand des Speicherarchivs zurückstellen. IBM Spectrum Protect stellt die Reinigungskassette wie angegeben bereit. Wenn Sie planen, bei einem SCSI-Speicherarchiv, das in seiner Einheitenhardware die

Unterstützung für die automatische Laufwerkreinigung bereitstellt, die servergesteuerte Laufwerkreinigung zu verwenden, sind spezielle Hinweise zu berücksichtigen.

Tipp: Wenn ein automatisiertes Bandarchiv die Speicherarchivlaufwerkreinigung unterstützt, stellen Sie sicher, dass die Funktion aktiviert ist.

Sie können die vorzeitige Abnutzung der Schreib-/Leseköpfe von Laufwerken verhindern, indem Sie die Speicherarchivreinigungsfunktionen Ihres Einheitenherstellers verwenden.

Bei Laufwerken und Speicherarchiven unterschiedlicher Hersteller bestehen Unterschiede in der Handhabung von Reinigungskassetten und in der Art und Weise, wie das Vorhandensein einer Reinigungskassette in einem Laufwerk zurückgemeldet wird. Möglicherweise kann ein Laufwerk, das eine Reinigungskassette enthält, vom Einheitentreiber nicht geöffnet werden. Die von Einheiten ausgegebenen Prüfcodes und Fehlercodes für die Laufwerkreinigung sind unterschiedlich. Die Speicherarchivlaufwerkreinigung ist normalerweise Anwendungen nicht bekannt. Daher kann IBM Spectrum Protect möglicherweise die Reinigungskassetten in Laufwerken nicht immer erkennen und unter Umständen nicht bestimmen, wann die Reinigung beginnt.

Einige Einheiten erfordern eine kurze Leerlaufzeit zwischen Mountanforderungen, um die Laufwerkreinigung starten zu können. IBM Spectrum Protect versucht jedoch, die Leerlaufzeit für ein Laufwerk zu minimieren. Dies kann dazu führen, dass die Speicherarchivlaufwerkreinigung nicht effektiv funktioniert. Verwenden Sie in diesem Fall IBM Spectrum Protect zur Steuerung der Laufwerkreinigung. Sie können die Häufigkeit so festlegen, dass sie mit den Reinigungsempfehlungen des Herstellers übereinstimmt.

- Methoden zum Reinigen von Bandlaufwerken  
Im Laufe der Zeit können die Leseköpfe für Bänder verschmutzen, was zum Fehlschlagen von Lese- und Schreiboperationen führen kann. Aktivieren Sie die Bandreinigung, um diese Probleme zu verhindern. Sie können die Bandreinigung über das Laufwerk oder IBM Spectrum Protect aktivieren.
- Server für die Laufwerkreinigung in einem automatisierten Speicherarchiv konfigurieren  
Wenn Sie die servergesteuerte Laufwerkreinigung in einem automatisierten Speicherarchiv konfigurieren, können Sie angeben, wie oft die Laufwerke gereinigt werden sollen.
- Fehler bei der Laufwerkreinigung beheben  
Während Kassetten in einem Speicherarchiv versetzt werden, wird eine Datenkassette möglicherweise an eine Stelle versetzt, an der sich eine Reinigungskassette befinden sollte. Überprüfen Sie den Prozess, den der Server ausführt, und die Nachrichten, die ausgegeben werden, sodass Sie das Problem beheben können.

## Methoden zum Reinigen von Bandlaufwerken

---

Im Laufe der Zeit können die Leseköpfe für Bänder verschmutzen, was zum Fehlschlagen von Lese- und Schreiboperationen führen kann. Aktivieren Sie die Bandreinigung, um diese Probleme zu verhindern. Sie können die Bandreinigung über das Laufwerk oder IBM Spectrum Protect aktivieren.

Sie können entweder die Speicherarchivlaufwerkreinigungsmethode oder die IBM Spectrum Protect-Laufwerkreinigungsmethode verwenden, aber nicht beide Methoden gleichzeitig. Einige SCSI-Speicherarchive stellen eine automatische Laufwerkreinigung zur Verfügung. Wählen Sie die Speicherarchivlaufwerkreinigungsmethode aus, sofern diese verfügbar ist. Ist sie nicht verfügbar oder hat sie Probleme zur Folge, verwenden Sie IBM Spectrum Protect zur Steuerung der Speicherarchivlaufwerkreinigung.

### Speicherarchivlaufwerkreinigungsmethode

Die Speicherarchivlaufwerkreinigungsmethode bietet für automatisierte Bandarchive, die diese Funktion verwenden, eine Reihe von Vorteilen:

- Sie verringert den Aufwand, den der IBM Spectrum Protect-Administrator hat, um die Reinigung mithilfe von Kassetten physisch zu handhaben.
- Sie verbessert die Verwendungsraten von Reinigungskassetten. Bei den meisten Bandarchiven wird die Häufigkeit, mit der Laufwerke gereinigt werden können, auf der Basis von Hardwareanzeigen verfolgt. IBM Spectrum Protect verwendet eine Rohzählung.
- Sie reduziert die Häufigkeit unnötiger Reinigungen. Moderne Bandlaufwerke müssen nicht in festen Intervallen gereinigt werden; sie können erkennen, wann eine Reinigung erforderlich ist, und diese dann anfordern.

Hersteller, die eine Speicherarchivlaufwerkreinigungsmethode zur Verfügung stellen, empfehlen die Verwendung dieser Funktion, um eine vorzeitige Abnutzung der Schreib-/Leseköpfe der Laufwerke zu verhindern. Bei Laufwerken und Speicherarchiven unterschiedlicher Hersteller bestehen Unterschiede in der Handhabung von Reinigungskassetten und in der Art und Weise, wie das Vorhandensein einer Reinigungskassette in einem Laufwerk zurückgemeldet wird. Möglicherweise kann ein Laufwerk, das eine Reinigungskassette enthält, vom Einheitentreiber nicht geöffnet werden. Die von Einheiten ausgegebenen Prüfcodes und Fehlercodes für die Laufwerkreinigung sind unterschiedlich. Die Speicherarchivlaufwerkreinigung ist normalerweise für alle Anwendungen transparent. IBM Spectrum Protect kann jedoch möglicherweise Reinigungskassetten in Laufwerken nicht immer erkennen und unter Umständen nicht bestimmen, wann die Reinigung beginnt.

IBM Spectrum Protect-Laufwerkreinigungsmethode

Einige Einheiten erfordern eine kurze Leerlaufzeit zwischen Mountanforderungen, um die Laufwerkreinigung starten zu können. IBM Spectrum Protect versucht jedoch, die Leerlaufzeit für ein Laufwerk zu minimieren. Dies kann dazu führen, dass die Speicherarchivlaufwerkreinigung nicht effektiv funktioniert. Versuchen Sie in diesem Fall, IBM Spectrum Protect zur Steuerung der Laufwerkreinigung zu verwenden. Legen Sie die Häufigkeit so fest, dass sie mit den Reinigungsempfehlungen des Herstellers übereinstimmt.

Wenn der Laufwerkreinigungsprozess durch IBM Spectrum Protect gesteuert wird, inaktivieren Sie die Speicherarchivlaufwerkreinigungsfunktion, um Probleme zu verhindern. Wenn die Speicherarchivlaufwerkreinigungsfunktion aktiviert ist, versetzen einige Einheiten automatisch alle Reinigungskassetten, die im Speicherarchiv gefunden werden, in die Schächte des Speicherarchivs, die für Reinigungskassetten vorgesehen sind. Sie können eine Reinigungskassette erst nach der Inaktivierung der Speicherarchivlaufwerkreinigungsfunktion in den IBM Spectrum Protect-Speicherarchivbestand zurückstellen.

Um die Reinigung über das Laufwerk zu aktivieren, führen Sie die Anweisungen des Laufwerkherstellers aus. Informationen zum Aktivieren der Bereinigung mithilfe von IBM Spectrum Protect finden Sie in Server für die Laufwerkreinigung in einem automatisierten Speicherarchiv konfigurieren.

## Server für die Laufwerkreinigung in einem automatisierten Speicherarchiv konfigurieren

---

Wenn Sie die servergesteuerte Laufwerkreinigung in einem automatisierten Speicherarchiv konfigurieren, können Sie angeben, wie oft die Laufwerke gereinigt werden sollen.

### Vorbereitende Schritte




---

Bestimmen Sie, wie oft das Laufwerk gereinigt werden muss. Dieser Schritt ist erforderlich, damit Sie einen geeigneten Wert für den Parameter CLEANFREQUENCY im Befehl DEFINE DRIVE oder UPDATE DRIVE angeben können. Um beispielsweise ein Laufwerk zu reinigen, nachdem 100 GB Daten in dem Laufwerk verarbeitet wurden, würden Sie CLEANFREQUENCY=100 angeben.

Richtlinien zur Reinigungshäufigkeit enthält die Dokumentation des Laufwerkherstellers. Wenn die Dokumentation Richtlinien zur Reinigungshäufigkeit in Nutzungsstunden angibt, rechnen Sie den Wert in einen Gigabyte wert um, indem Sie die folgenden Schritte ausführen:

1. Verwenden Sie den Wert für Byte pro Sekunde des Laufwerks, um einen Wert für Gigabyte pro Stunde zu ermitteln.
2. Multiplizieren Sie den Wert für Gigabyte pro Stunde mit der empfohlenen Anzahl Nutzungsstunden zwischen Reinigungen.
3. Verwenden Sie das Ergebnis als Wert für die Reinigungshäufigkeit.

Sie können entweder einen Wert für den Parameter CLEANFREQUENCY angeben oder ASNEEDED angeben, um das Laufwerk nach Bedarf zu reinigen.  
Einschränkungen:

1. Bei Laufwerken IBM® 3592 müssen Sie einen numerischen Wert für den Parameter CLEANFREQUENCY angeben. Bei Einhaltung der in der Produktinformation aufgelisteten Reinigungshäufigkeit werden die Laufwerke nicht übermäßig gereinigt.
2. Der Parameterwert CLEANFREQUENCY=ASNEEDED funktioniert nicht für alle Bandlaufwerke. Die Informationen für Ihr Betriebssystem geben Auskunft darüber, ob ein Laufwerk diese Funktion unterstützt:
  - o  AIX-Betriebssysteme  Windows-Betriebssysteme Supported devices for AIX and Windows
  - o  Linux-Betriebssysteme Supported devices for Linux

Klicken Sie in der Technote auf den Laufwerknamen, um detaillierte Informationen anzuzeigen. Wenn der Wert ASNEEDED nicht unterstützt wird, geben Sie die Anzahl Gigabyte an.

### Vorgehensweise

---

Um die servergesteuerte Laufwerkreinigung in einem automatisierten Speicherarchiv zu konfigurieren, führen Sie die folgenden Schritte aus:

Definieren oder aktualisieren Sie die Laufwerke in dem Speicherarchiv unter Angabe des Parameters CLEANFREQUENCY im Befehl DEFINE DRIVE oder UPDATE DRIVE. Um beispielsweise ein Laufwerk mit dem Namen DRIVE1 nach der Verarbeitung von 100 GB Daten zu reinigen, geben Sie den folgenden Befehl aus:

```
update drive autolibl drive1 cleanfrequency=100
```

### Ergebnisse

---

Nachdem die Reinigungskassette zurückgestellt wurde, wird sie vom Server in ein Laufwerk geladen, wenn dieses gereinigt werden muss. Der Server verwendet diese Reinigungskassette gemäß den Angaben für die Reinigungsanzahl. Weitere Informationen finden Sie in Operationen mit Reinigungskassetten.

## Nächste Schritte

---

Stellen Sie die Reinigungskassette in den Datenträgerbestand im Speicherarchiv zurück, indem Sie die Anweisungen in Reinigungskassette in ein Speicherarchiv zurückstellen ausführen.

- **Reinigungskassette in ein Speicherarchiv zurückstellen**  
Um die automatische Bandlaufwerkreinigung zu ermöglichen, müssen Sie eine Reinigungskassette in den Datenträgerbestand des automatisierten Speicherarchivs zurückstellen.
- **Operationen mit Reinigungskassetten**  
Um sicherzustellen, dass Bandlaufwerke wie erforderlich gereinigt werden, und um Probleme mit Bandspeicher zu verhindern, müssen Sie die Richtlinien beachten.

### Zugehörige Informationen:

- 🔗 [DEFINE DRIVE](#) (Laufwerk für ein Speicherarchiv definieren)
- 🔗 [UPDATE DRIVE](#) (Laufwerk aktualisieren)

## Reinigungskassette in ein Speicherarchiv zurückstellen

---

Um die automatische Bandlaufwerkreinigung zu ermöglichen, müssen Sie eine Reinigungskassette in den Datenträgerbestand des automatisierten Speicherarchivs zurückstellen.

### Informationen zu diesem Vorgang

---

Wenn Sie eine Reinigungskassette in ein Speicherarchiv zurückstellen, stellen Sie sicher, dass sie vom Server korrekt als Reinigungskassette erkannt wird. Stellen Sie sicher, dass sich keine Reinigungskassette in einem Schacht befindet, der beim Suchvorgang erkannt wird. Fehler und Verzögerungen von mindestens 15 Minuten können anzeigen, dass eine Reinigungskassette falsch platziert wurde.

Bei der bevorzugten Methode werden Reinigungskassetten einzeln zurückgestellt. Wenn Sie sowohl Datenkassetten als auch Reinigungskassetten zurückstellen müssen, stellen Sie zuerst die Datenkassetten in das Speicherarchiv zurück. Stellen Sie anschließend die Reinigungskassetten in das Speicherarchiv zurück.

### Vorgehensweise

---

Um eine Reinigungskassette in ein Speicherarchiv zurückzustellen, geben Sie den Befehl CHECKIN LIBVOLUME aus. Um beispielsweise eine Reinigungskassette mit dem Namen AUTOLIB1 zurückzustellen, geben Sie den folgenden Befehl aus:

```
checkin libvolume autolib1 cleanv status=cleaner cleanings=10  
checklabel=no
```

Der Server gibt die Anforderung aus, die Kassette in den Eingangs-/Ausgangsport oder in einen bestimmten Schacht einzulegen.

### Zugehörige Verweise:

- 🔗 [CHECKIN LIBVOLUME](#) (Speicherdatenträger in ein Speicherarchiv zurückstellen)

## Operationen mit Reinigungskassetten

---

Um sicherzustellen, dass Bandlaufwerke wie erforderlich gereinigt werden, und um Probleme mit Bandspeicher zu verhindern, müssen Sie die Richtlinien beachten.

### Reinigungsprozess überwachen

Wenn eine Reinigungskassette in ein Speicherarchiv zurückgestellt wird und ein Laufwerk gereinigt werden muss, hebt der Server die Bereitstellung des Datenträgers auf und führt die Reinigungsoperation aus. Wenn die Reinigungsoperation fehlschlägt oder wenn sie abgebrochen wird oder wenn keine Reinigungskassette verfügbar ist, sind Sie sich der Tatsache, dass das Laufwerk gereinigt werden muss, möglicherweise nicht bewusst. Überwachen Sie Reinigungsnachrichten auf diese Probleme, um sicherzustellen, dass Laufwerke wie erforderlich gereinigt werden. Geben Sie, falls erforderlich, den Befehl CLEAN DRIVE aus, damit der Server den Reinigungsversuch wiederholt, oder laden Sie manuell eine Reinigungskassette in das Laufwerk.

### Mehrere Reinigungskassetten verwenden

Der Server verwendet eine Reinigungskassette für die Anzahl Reinigungen, die Sie beim Zurückstellen der Reinigungskassette angeben. Wenn Sie zwei oder mehr Reinigungskassetten zurückstellen, verwendet der Server nur eine der Kassetten, bis die angegebene Anzahl Reinigungen für diese Kassette erreicht ist. Dann verwendet der Server die nächste Reinigungskassette. Wenn Sie zwei oder mehr Reinigungskassetten zurückstellen und zwei oder mehr Befehle CLEAN DRIVE gleichzeitig ausgegeben, verwendet der Server mehrere Kassetten gleichzeitig und verringert die verbleibenden Reinigungen auf jeder Kassette.

#### Zugehörige Verweise:

- ➔ AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Speicherarchiv prüfen)
- ➔ CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
- ➔ CLEAN DRIVE (Laufwerk reinigen)
- ➔ LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

#### Zugehörige Informationen:

- ➔ QUERY LIBVOLUME (Datenträger im Speicherarchiv abfragen)

## Fehler bei der Laufwerkreinigung beheben

---

Während Kassetten in einem Speicherarchiv versetzt werden, wird eine Datenkassette möglicherweise an eine Stelle versetzt, an der sich eine Reinigungskassette befinden sollte. Überprüfen Sie den Prozess, den der Server ausführt, und die Nachrichten, die ausgegeben werden, sodass Sie das Problem beheben können.

Wenn ein Laufwerk gereinigt werden muss, lädt der Server das, was laut Datenbank eine Reinigungskassette sein müsste, in das Laufwerk. Das Laufwerk wird dann in den Bereitstatus (READY) versetzt und IBM Spectrum Protect erkennt, dass es sich bei der Kassette um eine Datenkassette handelt. Der Server führt die folgenden Schritte aus:

1. Der Server versucht, den internen Bandkennsatz der Datenkassette zu lesen.
2. Der Server gibt die Kassette aus dem Laufwerk aus und stellt sie innerhalb des Speicherarchivs in den Ausgangsspeicherschacht der Reinigungskassette zurück. Wenn die Ausgabeoperation fehlschlägt, markiert der Server das Laufwerk als offline und gibt eine Nachricht aus, die besagt, dass sich die Kassette noch im Laufwerk befindet.
3. Der Server entnimmt die Reinigungskassette, um zu verhindern, dass sie für eine weitere Laufwerkreinigungsanforderung ausgewählt wird. Die Reinigungskassette verbleibt im Speicherarchiv, erscheint jedoch nicht mehr im IBM Spectrum Protect-Speicherarchivbestand.
4. Unter Verwendung des internen Bandkennsatzes gleicht der Server den Datenträgernamen mit dem aktuellen Speicherarchivbestand, mit den Speicherpooldatenträgern und mit der Protokolldatei für Datenträger ab.
  - Wenn der Datenträgername im Speicherarchivbestand nicht gefunden wird, wird unter Umständen fälschlicherweise eine Datenkassette als Reinigungskassette zurückgestellt. Wenn der Datenträger entnommen wird, müssen Sie keine weitere Aktion ausführen.
  - Wenn der Datenträgername im Speicherarchivbestand gefunden wird, gibt der Server Nachrichten aus, dass ein manueller Eingriff und eine Speicherarchivprüfung erforderlich sind. Um das Problem zu beheben, führen Sie die Anweisungen in Datenträgerbestand in einem Speicherarchiv prüfen aus.

## Bandlaufwerke ersetzen

---

Wenn Sie ein Laufwerk in einem Bandarchiv ersetzen, das für IBM Spectrum Protect definiert ist, müssen Sie die Laufwerk- und Pfaddefinitionen für das alte Laufwerk löschen und das neue Laufwerk samt Pfad definieren.

Das Ersetzen von Laufwerk- und Pfaddefinitionen ist selbst dann erforderlich, wenn Sie ein Laufwerk durch ein anderes Laufwerk desselben Typs mit derselben logischen Adresse, derselben physischen Adresse, derselben SCSI-ID und derselben Portnummer austauschen. Die Aliasnamen der Einheiten können sich ändern, wenn Sie Ihre Laufwerkverbindungen ändern.

Wenn es sich bei dem neuen Laufwerk um ein Upgrade handelt, das ein neues Datenträgerformat unterstützt, müssen Sie unter Umständen auch ein neues logisches Speicherarchiv, eine neue Einheitenklasse und einen neuen Speicherpool definieren. Die Prozeduren für das Konfigurieren einer Maßnahme für ein neues Laufwerk in einem Speicherarchiv mit mehreren Laufwerken sind je nach Laufwerktyp und Datenträgertyp in dem Speicherarchiv unterschiedlich.

- **Bandlaufwerke löschen**  
Sie können Bandlaufwerke aus einem Speicherarchiv löschen. Beispielsweise können Sie ein Laufwerk, das nicht mehr verwendet wird oder das ersetzt werden soll, löschen.
- **Laufwerke durch andere Laufwerke desselben Typs ersetzen**  
Um ein Laufwerk hinzuzufügen, das dieselben Datenträgerformate wie das zu ersetzende Laufwerk unterstützt, müssen Sie ein neues Laufwerk und einen neuen Pfad definieren.
- **Daten in Laufwerke umlagern, für die ein Upgrade durchgeführt wurde**  
Wenn Sie ein Upgrade für alle Bandlaufwerke in einem Speicherarchiv durchführen, können Sie Ihre vorhandenen Maßnahmendefinitionen für die Umlagerung und den Verfall bestehender Daten beibehalten, während Sie die neuen Laufwerke zum Speichern neuer Daten verwenden können.

## Bandlaufwerke löschen

---

Sie können Bandlaufwerke aus einem Speicherarchiv löschen. Beispielsweise können Sie ein Laufwerk, das nicht mehr verwendet wird oder das ersetzt werden soll, löschen.

## Vorgehensweise

---



1. Stoppen Sie den IBM Spectrum Protect-Server und fahren Sie das Betriebssystem herunter.
2. Entfernen Sie das alte Laufwerk und befolgen Sie zum Installieren des neuen Laufwerks die Anweisungen des Herstellers.
3. Starten Sie das Betriebssystem und den IBM Spectrum Protect-Server erneut.
4. Löschen Sie den Pfad vom Server zum Laufwerk. Um beispielsweise einen Pfad von SERVER1 zu LIB1 zu löschen, geben Sie den folgenden Befehl aus:

```
delete path server1 lib1 srctype=server desttype=drive
```

5. Löschen Sie die Laufwerkdefinition. Geben Sie beispielsweise den folgenden Befehl aus, um ein Laufwerk mit dem Namen DLT1 aus einem Speicherarchiv mit dem Namen LIB1 zu löschen:

```
delete drive lib1 dlt1
```

### Zugehörige Verweise:

-  [DELETE DRIVE \(Laufwerk aus einem Speicherarchiv löschen\)](#)
-  [DELETE PATH \(Pfad löschen\)](#)

## Laufwerke durch andere Laufwerke desselben Typs ersetzen

---

Um ein Laufwerk hinzuzufügen, das dieselben Datenträgerformate wie das zu ersetzende Laufwerk unterstützt, müssen Sie ein neues Laufwerk und einen neuen Pfad definieren.

### Informationen zu diesem Vorgang

---

Wenn ein Speicherarchiv nur ein einziges Laufwerkmodell enthält und ein Laufwerk ersetzt werden soll, müssen Sie das Laufwerk durch ein Laufwerk desselben Modells ersetzen. Wenn ein Speicherarchiv unterschiedliche Laufwerkmodelle enthält und ein Laufwerk ersetzt werden soll, können Sie das Laufwerk durch ein Laufwerk eines beliebigen Modells, das im Speicherarchiv vorhanden ist, ersetzen.

## Vorgehensweise

---

1. Löschen Sie die Pfad- und Laufwerkdefinitionen für das alte Laufwerk. Um beispielsweise ein Laufwerk mit dem Namen DRIVE1 aus einem Speicherarchiv mit dem Namen LIB1 zu löschen, geben Sie den folgenden Befehl ein:

```
delete path server2 drive1 srctype=server desttype=drive library=lib1  
delete drive lib1 drive1
```

2. Schalten Sie das Speicherarchiv aus, entfernen Sie das ursprüngliche Laufwerk, ersetzen Sie es durch das neue Laufwerk und schalten Sie das Speicherarchiv ein.
3. Aktualisieren Sie das Hostsystem, um sicherzustellen, dass das System das neue Laufwerk erkennt.
4. Definieren Sie das neue Laufwerk und den neuen Pfad. Um beispielsweise ein neues Laufwerk mit dem Namen DRIVE2 und einen Pfad von SERVER2 zu diesem Laufwerk zu definieren, wenn der IBM Spectrum Protect-Einheitentreiber verwendet wird, geben Sie die folgenden Befehle ein:

#### AIX-Betriebssysteme

```
define drive lib1 drive2  
define path server2 drive2 srctype=server desttype=drive library=lib1  
device=/dev/mt0
```

#### Linux-Betriebssysteme



```
define drive lib1 drive2  
define path server2 drive2 srctype=server desttype=drive library=lib1  
device=/dev/tmscsi/mt0
```

#### Windows-Betriebssysteme

```
define drive lib1 drive2  
define path server2 drive2 srctype=server desttype=drive library=lib1  
device=mt3.0.0.1
```

Tipp: Sie können Ihre vorhandenen Speicherarchiv-, Einheitenklassen- und Speicherpooldefinitionen verwenden.

### Zugehörige Verweise:

-  [DELETE DRIVE \(Laufwerk aus einem Speicherarchiv löschen\)](#)
-  [DELETE PATH \(Pfad löschen\)](#)

## Daten in Laufwerke umlagern, für die ein Upgrade durchgeführt wurde

---

Wenn Sie ein Upgrade für alle Bandlaufwerke in einem Speicherarchiv durchführen, können Sie Ihre vorhandenen Maßnahmendefinitionen für die Umlagerung und den Verfall bestehender Daten beibehalten, während Sie die neuen Laufwerke zum Speichern neuer Daten verwenden können.

### Vorbereitende Schritte

---

Bei dem folgenden Szenario wird vorausgesetzt, dass bereits ein primärer Speicherpool mit dem Namen POOL1 für eine Einheitenklasse DISK vorhanden ist.

### Vorgehensweise

---

1. Um Daten in einen Speicherpool umzulagern, der für die neuen Laufwerke erstellt wird, geben Sie den Parameter NEXTSTGPOOL an. Um beispielsweise Daten aus einem vorhandenen Speicherpool mit dem Namen POOL1 in den neuen Speicherpool mit dem Namen POOL2 umzulagern, geben Sie den folgenden Befehl aus:

```
update stgpool pool1 nextstgpool=pool2
```

2. Aktualisieren Sie die Verwaltungsklassendefinitionen, um Daten mithilfe des Befehls UPDATE MGMTCLASS in dem neuen DISK-Speicherpool zu speichern.

#### Zugehörige Verweise:

➤ UPDATE MGMTCLASS (Verwaltungsklasse aktualisieren)

➤ UPDATE STGPOOL (Speicherpool aktualisieren)

#### Zugehörige Informationen:

➤ DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

## IBM Spectrum Protect-Server schützen

---

Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.

- Administratoren verwalten  
Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.
- Kennwortanforderungen ändern  
Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.
- Server auf dem System schützen  
Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

## Administratoren verwalten

---

Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.

### Vorgehensweise

---

Führen Sie die folgenden Tasks aus, um Administratoreinstellungen zu ändern.

| Task | Prozedur |
|------|----------|
|------|----------|

| Task  | Prozedur  |
|---|---|
| Administrator hinzufügen                        | <p>Um einen Administrator, ADMIN1, mit Systemberechtigung hinzuzufügen und ein Kennwort anzugeben, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>Registrieren Sie den Administrator und geben Sie Pa\$#\$twO als Kennwort an, indem Sie den folgenden Befehl ausgeben: <pre>register admin admin1 Pa\$#\$twO</pre> </li> <li>Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben: <pre>grant authority admin1 classes=system</pre> </li> </ol> |
| Administratorberechtigung ändern                | <p>Ändern Sie die Berechtigungsstufe für einen Administrator, ADMIN1.</p> <ul style="list-style-type: none"> <li>Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben: <pre>grant authority admin1 classes=system</pre> </li> <li>Entziehen Sie dem Administrator die Systemberechtigung, indem Sie den folgenden Befehl ausgeben: <pre>revoke authority admin1 classes=system</pre> </li> </ul>  |
| Administratoren entfernen                       | <p>Entfernen Sie einen Administrator, ADMIN1, sodass er nicht mehr auf den IBM Spectrum Protect-Server zugreifen kann, indem Sie den folgenden Befehl ausgeben:</p> <pre>remove admin admin1</pre>  |
| Zugriff auf den Server vorübergehend verhindern | <p>Sperren oder entsperren Sie einen Administrator, indem Sie den Befehl LOCK ADMIN bzw. UNLOCK ADMIN verwenden.</p>  |

**Zugehörige Konzepte:**

Planung für Administratorrollen

## Kennwortanforderungen ändern

Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.

### Informationen zu diesem Vorgang

Indem Sie die Kennwortauthentifizierung durchsetzen und Kennworteinschränkungen verwalten, können Sie Ihre Daten und Ihre Server vor möglichen Sicherheitsrisiken schützen.

### Vorgehensweise

Führen Sie die folgenden Tasks aus, um Kennwortanforderungen für IBM Spectrum Protect-Server zu ändern.

Tabelle 1. Authentifizierungstasks für IBM Spectrum Protect-Server

| Task  | Prozedur   |
|---|--|
| Grenzwert für ungültige Kennworteingabeversuche festlegen | <ol style="list-style-type: none"> <li>Wählen Sie auf der Seite Server im Operations Center den Server aus.</li> <li>Klicken Sie auf Details und dann auf die Registerkarte Merkmale.</li> <li>Geben Sie die Anzahl ungültiger Versuche im Feld Grenzwert für ungültige Anmeldeversuche an.</li> </ol> <p>Der Standardwert bei der Installation ist 0.</p> |



| Task  | Prozedur   |
|---|--|
| Mindestlänge für Kennwörter festlegen       | <ol style="list-style-type: none"> <li>Wählen Sie auf der Seite Server im Operations Center den Server aus.</li> <li>Klicken Sie auf Details und dann auf die Registerkarte Merkmale.</li> <li>Geben Sie die Anzahl Zeichen im Feld Mindestlänge für Kennwort an.</li> </ol>   |
| Ablaufzeitraum für Kennwörter festlegen     | <ol style="list-style-type: none"> <li>Wählen Sie auf der Seite Server im Operations Center den Server aus.</li> <li>Klicken Sie auf Details und dann auf die Registerkarte Merkmale.</li> <li>Geben Sie die Anzahl Tage im Feld Allgemeine Kennwortablaufdauer an.</li> </ol>   |
| Kennwortauthentifizierung inaktivieren      | <p>Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer ein Kennwort eingeben, um auf den Server zugreifen zu können.</p> <p>Sie können die Kennwortauthentifizierung nur für Kennwörter inaktivieren, die mit dem Server (LOCAL) authentifiziert werden. Durch das Inaktivieren der Kennwortauthentifizierung erhöht sich das Sicherheitsrisiko für den Server.</p> |
| Standardauthentifizierungsmethode festlegen | <p>Geben Sie den Befehl SET DEFAULTAUTHENTICATION aus. Um beispielsweise den Server als die Standardauthentifizierungsmethode zu verwenden, geben Sie den folgenden Befehl aus:</p> <pre>set defaultauthentication local</pre> <p>Um einen Clientknoten für die Authentifizierung mit dem Server zu aktualisieren, schließen Sie AUTHENTICATION=LOCAL in den Befehl UPDATE NODE ein:</p> <pre>update node authentication=local</pre>                 |

## Server auf dem System schützen

Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

### Vorgehensweise

Stellen Sie sicher, dass nicht berechtigte Benutzer nicht auf die Verzeichnisse für die Serverdatenbank und die Serverinstanz zugreifen können. Behalten Sie die Zugriffseinstellungen für diese Verzeichnisse bei, die Sie während der Implementierung konfiguriert haben.

- Benutzerzugriff auf den Server einschränken  
Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

## Server stoppen und starten

Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.

### Vorbereitende Schritte

Um den IBM Spectrum Protect-Server stoppen und starten zu können, müssen Sie über System- oder Bedienerberechtigung verfügen.

- Server stoppen  
Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen

abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.

- Server für Verwaltungs- oder Rekonfigurationstasks starten  
Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

## Server stoppen

---

Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.

### Informationen zu diesem Vorgang

---

Wenn Sie den Befehl HALT zum Stoppen des Servers ausgeben, werden die folgenden Aktionen ausgeführt:

- Alle Prozesse und Clientknotensitzungen werden abgebrochen.
- Alle aktuellen Transaktionen werden gestoppt. (Die Transaktionen werden rückgängig gemacht, wenn der Server erneut gestartet wird.)

### Vorgehensweise

---

Um das System vorzubereiten und den Server zu stoppen, führen Sie die folgenden Schritte aus:

1. Verhindern Sie, dass neue Clientknotensitzungen gestartet werden, indem Sie den Befehl DISABLE SESSIONS ausgeben:

```
disable sessions all
```

2. Bestimmen Sie, ob Clientknotensitzungen oder -prozesse aktiv sind, indem Sie die folgenden Schritte ausführen:
  - a. Rufen Sie die Seite Übersicht im Operations Center auf, auf der im Bereich Aktivität die Gesamtzahl Prozesse und Sitzungen angezeigt wird, die derzeit aktiv sind. Wenn die Zahlen erheblich von den Zahlen abweichen, die normalerweise während Ihrer täglichen Speicherverwaltungsroutine angezeigt werden, überprüfen Sie mithilfe weiterer Statusanzeiger im Operations Center, ob ein Problem vorliegt.
  - b. Zeigen Sie das Diagramm im Bereich Aktivität an, um den Umfang des Datenaustauschs im Netz für die folgenden Perioden zu vergleichen:
    - Die laufende Periode, d. h. die letzte 24-Stunden-Periode
    - Die vorherige Periode, d. h. die 24 Stunden vor der laufenden PeriodeWenn das Diagramm für die vorherige Periode den erwarteten Umfang des Datenaustauschs darstellt, können deutliche Abweichungen in dem Diagramm für die laufende Periode auf ein Problem hindeuten.
  - c. Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details. Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, rufen Sie mithilfe von Verwaltungsbefehlen Informationen zu Prozessen ab. Geben Sie den Befehl QUERY PROCESS aus, um Prozesse abzufragen; geben Sie den Befehl QUERY SESSION aus, um Informationen zu Sitzungen abzurufen.
3. Warten Sie, bis die Clientknotensitzungen abgeschlossen sind oder brechen Sie diese ab. Um Prozesse und Sitzungen abzubrechen, führen Sie die folgenden Schritte aus:
  - Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details.
  - Klicken Sie auf die Registerkarte Aktive Tasks und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
  - Klicken Sie auf Abbrechen.
  - Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, brechen Sie Sitzungen mithilfe von Verwaltungsbefehlen ab. Geben Sie den Befehl CANCEL SESSION aus, um eine Sitzung abzubrechen; geben Sie den Befehl CANCEL PROCESS aus, um Prozesse abzubrechen.  
Tipp: Wenn der Prozess, der abgebrochen werden soll, auf die Bereitstellung eines Banddatenträgers wartet, wird die Mountanforderung abgebrochen. Wenn Sie beispielsweise einen Befehl EXPORT, IMPORT oder MOVE DATA ausgeben, leitet der Befehl möglicherweise einen Prozess ein, der die Bereitstellung eines Banddatenträgers erfordert. Wenn jedoch ein Banddatenträger durch ein automatisiertes Speicherarchiv bereitgestellt wird, wird die Abbruchoperation unter Umständen erst wirksam, wenn der Bereitstellungsprozess abgeschlossen ist. Abhängig von Ihrer Systemumgebung kann dies mehrere Minuten dauern.
4. Stoppen Sie den Server, indem Sie den Befehl HALT ausgeben:

```
halt
```

## Server für Verwaltungs- oder Rekonfigurationstasks starten

---

Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

## Informationen zu diesem Vorgang

---

Starten Sie den Server im Verwaltungsmodus, indem Sie das Dienstprogramm DSMSEV mit dem Parameter MAINTENANCE ausführen.

Im Verwaltungsmodus sind die folgenden Operationen inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Konsolidierung von Speicherbereich auf dem Server
- Bestandsverfall
- Umlagerung von Speicherpools

Darüber hinaus wird verhindert, dass Clients Sitzungen mit dem Server starten können.

Tipps:

- Sie müssen die Serveroptionsdatei, `dmserv.opt`, nicht editieren, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Speicherbereichskonsolidierung, den Bestandsverfall und Umlagerungsprozesse für Speicherpools manuell starten.

## Vorgehensweise

---

Um den Server im Verwaltungsmodus zu starten, geben Sie den folgenden Befehl aus:

```
dmserv maintenance
```

Tipp: Informationen zum Anzeigen eines Ein Video zum Starten des Servers im Verwaltungsmodus kann über Server im Verwaltungsmodus starten angezeigt werden.




## Nächste Schritte

---

Um Serveroperationen im Produktionsmodus wiederaufzunehmen, führen Sie die folgenden Schritte aus:

1. Fahren Sie den Server herunter, indem Sie den Befehl HALT ausgeben:

```
halt
```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden. Führen Sie die Anweisungen für Ihr Betriebssystem aus:
  -  AIX-BetriebssystemeServerinstanz starten
  -  Linux-BetriebssystemeServerinstanz starten
  -  Windows-BetriebssystemeServerinstanz starten

Operationen, die im Verwaltungsmodus inaktiviert waren, werden wieder aktiviert.

## Durchführung eines Upgrades für den Server planen

---

Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.

## Informationen zu diesem Vorgang

---

Beachten Sie diese Richtlinien:

- Bei der bevorzugten Methode erfolgt das Upgrade für den Server mithilfe des Installationsassistenten. Nachdem Sie den Assistenten gestartet haben, klicken Sie im Fenster IBM Installation Manager auf das Symbol zum Aktualisieren; klicken Sie nicht auf das Symbol zum Installieren oder Ändern!
- Wenn sowohl für die Serverkomponente als auch für die Operations Center-Komponente Upgrades verfügbar sind, wählen Sie die Kontrollkästchen aus, um das Upgrade für beide Komponenten durchzuführen.

## Vorgehensweise

---




1. Überprüfen Sie die Liste der Fixpacks und vorläufigen Fixes. Siehe Technote 1239415.

2. Studieren Sie die Produktverbesserungen, die in der Readme-Datei beschrieben sind.  
Tipp: Wenn Sie die Installationspaketdatei von der IBM Spectrum Protect-Unterstützungsseite abrufen, können Sie auch auf die Readme-Datei zugreifen.
3. Stellen Sie sicher, dass die Version, auf die das Upgrade für Ihren Server durchgeführt wird, mit anderen Komponenten, wie beispielsweise Speicheragenten und Speicherarchivclients, kompatibel ist. Siehe Technote 1302789.
4. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden. Siehe Technote 1053218.
5. Lesen Sie die Upgradeanweisungen. Stellen Sie sicher, dass Sie die Serverdatenbank, die Einheitenkonfigurationsinformationen und die Protokolldatei für Datenträger sichern.

## Nächste Schritte

---

Um ein Fixpack oder einen vorläufigen Fix zu installieren, führen Sie die Anweisungen für Ihr Betriebssystem aus:

-  AIX-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
-  Linux-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
-  Windows-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren

### Zugehörige Informationen:

 Upgrade- und Umlagerungsprozess - Häufig gestellte Fragen

## Vorbereitungen für einen Ausfall oder eine Systemaktualisierung

---

Treffen Sie Vorbereitungen in IBM Spectrum Protect, damit Ihr System während eines geplanten Stromausfalls oder einer geplanten Systemaktualisierung in einem konsistenten Zustand verbleibt.

### Informationen zu diesem Vorgang

---

Stellen Sie sicher, dass Sie die regelmäßige Ausführung von Aktivitäten planen, um den Server zu verwalten und zu schützen. Informationen zum Planen von Aktivitäten wie beispielsweise Sichern der Datenbank, Sichern der Einheitenkonfigurationsdatei und Sichern des Datenträgerprotokolls finden Sie in Zeitpläne für Serververwaltungsaktivitäten definieren.

## Vorgehensweise


---

1. Brechen Sie Prozesse und Sitzungen, die aktiv sind, ab, indem Sie die folgenden Schritte ausführen:
  - a. Wählen Sie im Operations Center auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details.
  - b. Klicken Sie auf die Registerkarte Aktive Tasks und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
  - c. Klicken Sie auf Abbrechen.
2. Stoppen Sie den Server, indem Sie den Befehl HALT ausgeben:

```
halt
```

Tipp: Sie können den Befehl HALT im Operations Center ausgeben, indem Sie den Mauszeiger über das Symbol für Einstellungen bewegen und auf Command Builder klicken. Wählen Sie dann den Server aus, geben Sie `halt` ein und drücken Sie die Eingabetaste.

### Zugehörige Verweise:

 HALT (Server herunterfahren)

## Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM

---

IBM Spectrum Protect stellt die Funktion Disaster Recovery Manager (DRM) für die Wiederherstellung Ihrer Server- und Clientdaten bei einem Katastrophenfall zur Verfügung.

DRM verfolgt die Versetzung ausgelagerter Datenträger und registriert diese Informationen in der IBM Spectrum Protect-Datenbank. DRM konsolidiert Pläne, Scripts und andere Informationen in einer Plandatei, die im Katastrophenfall oder bei einer ungeplanten Betriebsunterbrechung zum Wiederherstellen des IBM Spectrum Protect-Servers erforderlich ist. Wenn mögliche Malware-Angriffe, einschließlich Ransomware-Angriffe, ein Thema für Sie sind, ziehen Sie die Verwendung von DRM in Betracht, das Sie bei der Wiederherstellung Ihrer Server nach einer Attacke unterstützen kann.

Einschränkung: DRM ist nur im Produkt IBM Spectrum Protect Extended Edition verfügbar.

- Plandatei zur Wiederherstellung nach einem Katastrophenfall  
Die Plandatei zur Wiederherstellung nach einem Katastrophenfall, die auch als Wiederherstellungsplandatei bezeichnet wird, enthält die Informationen, die zum Wiederherstellen eines IBM Spectrum Protect-Servers mit dem Stand des Zeitpunkts der letzten Datenbanksicherungsoperation, die vor der Erstellung des Plans abgeschlossen wurde, erforderlich sind.
- Server und Clientdaten mithilfe von DRM wiederherstellen  
Verwenden Sie die Funktion 'Disaster Recovery Manager' (DRM), um den IBM Spectrum Protect-Server und Clientdaten im Katastrophenfall wiederherzustellen.
- Drilloperation für die Wiederherstellung nach einem Katastrophenfall ausführen  
Planen Sie Drilloperationen für die Wiederherstellung nach einem Katastrophenfall als Vorbereitung für Prüfungen, mit denen die Wiederherstellbarkeit des IBM Spectrum Protect-Servers bestätigt wird, und um sicherzustellen, dass nach einem Ausfall Daten zurückgeschrieben und Operationen wiederaufgenommen werden können. Mithilfe einer Drilloperation können Sie außerdem vor dem Eintreten einer kritischen Situation sicherstellen, dass alle Daten zurückgeschrieben und Operationen wiederaufgenommen werden können.
- Datenbank zurückschreiben  
Wenn die Funktion 'Disaster Recovery Manager' (DRM) aktiviert ist und Sie die Prozedur zur Vorbereitung auf einen Katastrophenfall ausgeführt haben, können Sie die Datenbank nach einem Katastrophenfall zurückschreiben. Wenn DRM nicht konfiguriert ist, können Sie die Datenbank dennoch zurückschreiben, vorausgesetzt, Sie verfügen über die erforderlichen Sicherungsdateien.

## Plandatei zur Wiederherstellung nach einem Katastrophenfall

Die Plandatei zur Wiederherstellung nach einem Katastrophenfall, die auch als Wiederherstellungsplandatei bezeichnet wird, enthält die Informationen, die zum Wiederherstellen eines IBM Spectrum Protect-Servers mit dem Stand des Zeitpunkts der letzten Datenbanksicherungsoperation, die vor der Erstellung des Plans abgeschlossen wurde, erforderlich sind.

Der Plan besteht aus Zeilengruppen, die Sie in mehrere Dateien aufteilen können. Jede Zeilengruppe verfügt über eine Anfangsanweisung (begin) und eine Endanweisung (end).

Tabelle 1. Zeilengruppen in der Wiederherstellungsplandatei

| Zeilengruppe                   | Informationen in der Zeilengruppe   |
|--------------------------------|---|
| SERVER.REQUIREMENTS            | Gibt den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll für den Server an.  |
| RECOVERY.INSTRUCTIONS.GENERAL  | Gibt standortspezifische Anweisungen an, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.GENERAL angegebene Datei eingibt. Die Anweisungen umfassen die Wiederherstellungsstrategie, die Namen der wichtigsten Ansprechpartner, eine Übersicht über die wichtigsten Anwendungen, die von diesem Server gesichert werden, und andere relevante Wiederherstellungsanweisungen.  |
| RECOVERY.INSTRUCTIONS.OFFSITE  | Enthält Anweisungen, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.OFFSITE angegebene Datei eingibt. Die Anweisungen umfassen den Namen und den Standort der Vault an einem anderen Standort sowie Informationen dazu, wie Kontakt zum Vaultadministrator aufgenommen werden kann (beispielsweise ein Name und eine Telefonnummer).   |
| RECOVERY.INSTRUCTIONS.INSTALL  | Enthält Anweisungen, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.INSTALL angegebene Datei eingibt. Die Anweisungen umfassen Informationen, die angeben, wie der Basisserver wiederhergestellt wird, und den Aufbewahrungsort der Sicherungskopien des Systemimage.  |
| RECOVERY.INSTRUCTIONS.DATABASE | Enthält Anweisungen, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.DATABASE angegebene Datei eingibt. Die Anweisungen umfassen Informationen, die angeben, wie die Datenbankwiederherstellung vorbereitet wird. Sie können beispielsweise Anweisungen eingeben, die angeben, wie die Sicherungsdatenträger für ein automatisiertes Speicherarchiv initialisiert oder geladen werden sollen. Für diese Zeilengruppe wird kein Beispiel bereitgestellt. |

| <b>Zeilengruppe</b>                    | <b>Informationen in der Zeilengruppe</b>  |
|--|---|
| RECOVERY.INSTRUCTIONS.STGPOOL          | Enthält Anweisungen, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.STGPOOL angegebene Datei eingibt. Die Anweisungen umfassen die Namen Ihrer Softwareanwendungen und der Kopierspeicherpools, die die Sicherung dieser Anwendungen enthalten. Für diese Zeilengruppe wird kein Beispiel bereitgestellt.  |
| RECOVERY.VOLUMES.REQUIRED              | Stellt eine Liste der Datenbanksicherungs- und Kopierspeicherpooldatenträger bereit, die zum Wiederherstellen des Servers erforderlich sind. Ein Datenbanksicherungsdatenträger wird eingeschlossen, wenn er Bestandteil der jüngsten Datenbanksicherungsreihe ist. Ein Kopierspeicherpooldatenträger wird eingeschlossen, wenn er nicht leer und nicht als dauerhaft beschädigt markiert ist.  |
| RECOVERY.DEVICES.REQUIRED              | Stellt Details zu den Einheiten bereit, die zum Lesen der Sicherungsdatenträger erforderlich sind.  |
| RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE | Enthält ein Script mit den Befehlen, die zum Wiederherstellen des Servers erforderlich sind.  |
| RECOVERY.SCRIPT.NORMAL.MODE            | Enthält ein Script mit den Befehlen, die zum Zurückschreiben der primären Speicherpools des Servers erforderlich sind.  |
| DB.STORAGEPATHS                        | Gibt die Verzeichnisse für die IBM Spectrum Protect-Datenbank an.   |
| LICENSE.REGISTRATION                   | Enthält ein Makro zum Registrieren Ihrer Serverlizenzen.  |
| COPYSTGPOOL.VOLUMES.AVAILABLE          | Enthält ein Makro zum Markieren von Kopierspeicherpooldatenträgern, die an einen anderen Standort transportiert wurden und anschließend wieder vor Ort transportiert wurden. Sie können die Informationen als Leitfaden verwenden und die Verwaltungsbefehle ausgeben. Es ist auch möglich, das Makro in eine Datei zu kopieren, zu ändern und auszuführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE gestartet.  |
| COPYSTGPOOL.VOLUMES.DESTROYED          | Enthält ein Makro, mit dem Kopierspeicherpooldatenträger als nicht verfügbar markiert werden können, wenn sich die Datenträger zum Zeitpunkt der Katastrophe vor Ort befanden. Diese Datenträger werden als ausgelagert betrachtet und wurden bei einem Katastrophenfall nicht dauerhaft beschädigt. Sie können die Informationen als Leitfaden verwenden und die Verwaltungsbefehle über eine Befehlszeile ausgeben oder Sie können das Makro in eine Datei kopieren, ändern und ausführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE gestartet. |
| PRIMARY.VOLUMES.DESTROYED              | Enthält ein Makro, mit dem Datenträger für primäre Speicherpools als dauerhaft beschädigt markiert werden können, wenn sich die Datenträger zum Zeitpunkt der Katastrophe vor Ort befanden. Sie können die Informationen als Leitfaden verwenden und die Verwaltungsbefehle über eine Befehlszeile ausführen oder Sie können das Makro in eine Datei kopieren, ändern und ausführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE gestartet.   |
| PRIMARY.VOLUMES.REPLACEMENT            | Enthält ein Makro zum Ermitteln der Ersatzdatenträger für primäre Speicherpools. Sie können die Informationen als Leitfaden verwenden und die Verwaltungsbefehle über eine Befehlszeile ausführen oder Sie können das Makro in eine Datei kopieren, ändern und ausführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE gestartet.  |

| <b>Zeilengruppe</b>              | <b>Informationen in der Zeilengruppe</b>   |
|----------------------------------|--|
| STGPOOLS.RESTORE                 | Enthält ein Makro zum Zurückschreiben der primären Speicherpools. Sie können die Zeilengruppe als Leitfaden verwenden und die Verwaltungsbefehle über eine Befehlszeile ausführen. Es ist auch möglich, das Makro in eine Datei zu kopieren, zu ändern und auszuführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.NORMAL.MODE gestartet.                                    |
| VOLUME.HISTORY.FILE              | Enthält eine Kopie der Datenträgerprotokolldaten zum Erstellungszeitpunkt des Wiederherstellungsplans. Das Dienstprogramm DSMSEV RESTORE DB bestimmt mithilfe der Protokolldatei für Datenträger, welche Datenträger zum Zurückschreiben der Datenbank erforderlich sind. Die Protokolldatei für Datenträger wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE verwendet. |
| DEVICE.CONFIGURATION.FILE        | Enthält eine Kopie der Servereinheitenkonfigurationsdaten zum Erstellungszeitpunkt des Wiederherstellungsplans. Das Dienstprogramm DSMSEV RESTORE DB liest mithilfe der Einheitenkonfigurationsdatei die Datenbanksicherungsdatenträger. Die Einheitenkonfigurationsdatei wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE verwendet.                                    |
| DSMSERV.OPT.FILE                 | Enthält eine Kopie der Serveroptionsdatei. Diese Zeilengruppe wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE verwendet.  |
| LICENSE.INFORMATION              | Enthält eine Kopie der neuesten Ergebnisse der Lizenzprüfung und der Serverlizenzbedingungen.  |
| MACHINE.GENERAL.INFORMATION      | Stellt Informationen für die Servermaschine bereit, wie beispielsweise ihr Standort, die zum Wiederherstellen der Servermaschine erforderlich sind. Diese Zeilengruppe wird in die Plandatei eingeschlossen, wenn die Maschineninformationen mithilfe des Befehls DEFINE MACHINE unter Angabe von ADSMSERVER=YES in der Datenbank gespeichert werden.                          |
| MACHINE.RECOVERY.INSTRUCTIONS    | Stellt die Wiederherstellungsanweisungen für die Servermaschine bereit. Diese Zeilengruppe wird in die Plandatei eingeschlossen, wenn die Wiederherstellungsanweisungen für die Maschine in der Datenbank gespeichert werden.  |
| MACHINE.RECOVERY.CHARACTERISTICS | Stellt die Hardware- und Softwarekenndaten für die Servermaschine bereit. Diese Zeilengruppe wird in die Plandatei eingeschlossen, wenn die Maschinenkenndaten in der Datenbank gespeichert werden.  |
| MACHINE.RECOVERY.MEDIA           | Stellt Informationen zu den Datenträgern bereit, die für die Wiederherstellung der Maschine, die den Server enthält, erforderlich sind. Diese Zeilengruppe wird in die Plandatei eingeschlossen, wenn Informationen zu Wiederherstellungsdatenträgern in der Datenbank gespeichert werden und der Maschine zugeordnet sind, die den Server enthält.                            |

## Server und Clientdaten mithilfe von DRM wiederherstellen

Verwenden Sie die Funktion 'Disaster Recovery Manager' (DRM), um den IBM Spectrum Protect-Server und Clientdaten im Katastrophenfall wiederherzustellen.

### Vorbereitende Schritte

IBM Spectrum Protect ist für die Verwendung des Protokolls Secure Sockets Layer (SSL) für die Client/Server-Authentifizierung konfiguriert. Wenn Sie den Server starten, wird im Rahmen des Prozesses eine Datei mit einem digitalen Zertifikat (cert.kdb) erstellt. Diese Datei enthält den öffentlichen Schlüssel des Servers, der dem Client das Verschlüsseln von Daten ermöglicht. Die Datei mit dem digitalen Zertifikat kann nicht in der Serverdatenbank gespeichert werden, da Global Security Kit (GSKit) eine separate Datei in einem bestimmten Format erfordert.

Der Masterverschlüsselungsschlüssel ist in einer neuen, von GSKit verwalteten Schlüsseldatenbank, `dsmkeydb.kdb`, gespeichert. Wenn der Server über einen vorhandenen Masterverschlüsselungsschlüssel verfügt, wird der Masterverschlüsselungsschlüssel aus der Datei `dsmkeydb.kdb` in die Schlüsseldatenbank `dsmkeydb.kdb` umgelagert. Bewahren Sie Sicherungskopien der Dateien `dsmkeydb.kdb` und `dsmkeydb.sth` auf. Sie können den Befehl `BACKUP DB` zum Sichern des Masterverschlüsselungsschlüssels konfigurieren oder die Dateien `dsmkeydb.kdb` und `dsmkeydb.sth` selbst manuell sichern.

1. Bewahren Sie Sicherungskopien der Dateien `cert.kdb`, `cert.sth` und `cert256.arm` auf.
2. Wenn sowohl die ursprünglichen Zertifikatsdateien als auch alle Kopien verloren gehen oder beschädigt werden, generieren Sie neue Zertifikatsdateien.

## Vorgehensweise

---

1. Rufen Sie den neuesten Wiederherstellungsplan ab.
2. Überprüfen Sie die Wiederherstellungsschritte, die in der Zeilengruppe `RECOVERY.INSTRUCTIONS.GENERAL` des Plans beschrieben sind.
3. Unterteilen Sie die Zeilengruppen der Plandatei nach allgemeinen Vorabanweisungen, Scripts zur Wiederherstellung des IBM Spectrum Protect-Servers und Anweisungen zur Clientwiederherstellung in einzelne Dateien.
4. Rufen Sie alle erforderlichen Wiederherstellungsdatenträger (wie in dem Plan aufgelistet) vom Aufbewahrungsort ab.
5. Überprüfen Sie die Einheitenkonfigurationsdatei, um sicherzustellen, dass die Hardwarekonfiguration am Wiederherstellungsstandort mit der am ursprünglichen Standort identisch ist. Alle Unterschiede müssen in der Einheitenkonfigurationsdatei aktualisiert werden. Für die folgenden Beispielkonfigurationsänderungen sind Aktualisierungen der Konfigurationsinformationen erforderlich:
  - o Unterschiedliche Einheitennamen
  - o Anforderung bei automatisierten Speicherarchiven, die Datenbanksicherungsdatenträger manuell in das automatisierte Speicherarchiv einlegen und die Konfigurationsinformationen aktualisieren zu müssen, um das Element in dem Speicherarchiv zu identifizieren. Dies ermöglicht es dem Server, die erforderlichen Datenbanksicherungsdatenträger zu lokalisieren.
6. Konfigurieren Sie Ersatzhardware für den IBM Spectrum Protect-Server, einschließlich der Installation des Betriebssystems und des IBM Spectrum Protect-Basisreleases.
7. Führen Sie die Scripts zur Wiederherstellung des IBM Spectrum Protect-Servers im Wiederherstellungsplan aus. Die Zeilengruppen `RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE` und `RECOVERY.SCRIPT.NORMAL.MODE` enthalten ausführbare Befehlsdateien, mit denen die Wiederherstellung des IBM Spectrum Protect-Servers gesteuert werden kann, indem andere im Plan generierte Befehlsdateien aufgerufen werden. Mit dem Script `RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE` wird der Server bis zu dem Punkt wiederhergestellt, an dem Clients Zurückschreibungen direkt von den Kopienspeicherpooldatenträgern starten können.
8. Schreiben Sie die primären Speicherpools mithilfe des Scripts `RECOVERY.SCRIPT.NORMAL.MODE` zurück.
9. Starten Sie Clientzurückschreibungsoperationen beginnend mit der höchsten Priorität gemäß der allgemeinen Planung.

## Nächste Schritte

---

Der IBM Spectrum Protect-Server kann jetzt für normale Serveroperationen verwendet werden. Stellen Sie sicher, dass alle erforderlichen Operationen geplant sind. Anweisungen finden Sie in Zeitpläne für Serververwaltungsaktivitäten definieren und Sicherungs- und Archivierungsoperationen planen.

### Zugehörige Verweise:

➔ [PREPARE](#) (Wiederherstellungsplandatei erstellen)

### Zugehörige Informationen:

➔ [Daten in Verzeichniscontainerspeicherpools reparieren und wiederherstellen](#)

## Drilloperation für die Wiederherstellung nach einem Katastrophenfall ausführen

---

Planen Sie Drilloperationen für die Wiederherstellung nach einem Katastrophenfall als Vorbereitung für Prüfungen, mit denen die Wiederherstellbarkeit des IBM Spectrum Protect-Servers bestätigt wird, und um sicherzustellen, dass nach einem Ausfall Daten zurückgeschrieben und Operationen wiederaufgenommen werden können. Mithilfe einer Drilloperation können Sie außerdem vor dem Eintreten einer kritischen Situation sicherstellen, dass alle Daten zurückgeschrieben und Operationen wiederaufgenommen werden können.

## Vorbereitende Schritte

---

Führen Sie die folgenden Tasks aus:

- Planen Sie die regelmäßige Ausführung von Aktivitäten, um den Server zu verwalten und zu schützen. Weitere Informationen zur Planung von Aktivitäten finden Sie in [Zeitpläne für Serververwaltungsaktivitäten definieren](#). Stellen Sie sicher, dass Sie die



folgenden Tasks planen:

- Sichern der Datenbank.
- Versetzen von Datenträgern an einen anderen Standort.
- Sichern der Einheitenkonfigurationsdatei, der Protokolldatei für Datenträger und der Serveroptionsdatei dsmserv.opt.
- **Optional:** Ausgabe des Befehls PREPARE zum Erstellen der Plandatei zur Wiederherstellung nach einem Katastrophenfall.

Tipp:

Wenn Sie den Befehl PREPARE ausgeben, wird von der IBM Spectrum Protect-Funktion 'Disaster Recovery Manager' (DRM) exakt eine Kopie der Plandatei zur Wiederherstellung nach einem Katastrophenfall erstellt.

Sie können die Wiederherstellung nach einem Katastrophenfall mithilfe eines anderen Standorts ohne die Verwendung von DRM ausführen, DRM ist jedoch hilfreich, um Pläne, Scripts und andere Informationen, die während der Wiederherstellung nach einem Katastrophenfall erforderlich sind, zu konsolidieren.

Erstellen Sie zur Sicherheit mehrere Kopien des Plans. Bewahren Sie Kopien beispielsweise in gedruckter Form, auf einem USB-Flashlaufwerk, in Plattenspeicher an einem anderen Standort oder auf einem fernen Server auf. Die Wiederherstellungsplandatei wird täglich zusammen mit den Bändern ausgelagert. Weitere Informationen zu DRM finden Sie in Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM.

- Konfigurieren Sie die folgenden Ressourcen am Standort zur Wiederherstellung nach einem Katastrophenfall:
  1. Einen IBM Spectrum Protect-Wiederherstellungsserver. Der Server am Standort zur Wiederherstellung nach einem Katastrophenfall muss dieselbe Version wie der Server am Produktionsstandort haben.
  2. Ein Bandarchiv zum Speichern der Datenträger, die vom Produktionsstandort geliefert werden. Weitere Informationen zu Auslagerungsstandorten für die Wiederherstellung finden Sie in Auslagerung von Daten.
  3. Plattenspeicherplatz für die Datenbank, das Archivprotokoll, aktive Protokolldateien und Speicherpools.
  4. Clients zum Testen von Zurückschreibungsoperationen.

## Informationen zu diesem Vorgang

---

Testen Sie den Plan zur Wiederherstellung nach einem Katastrophenfall und die Wiederherstellbarkeit des IBM Spectrum Protect-Servers häufig und in einer ähnlichen Umgebung wie der Produktionsumgebung.

## Vorgehensweise

---

1. Stellen Sie sicher, dass Bänder vor Ort verfügbar sind. Geben Sie den Befehl QUERY LIBVOLUME aus, um Datenträger, die in ein automatisiertes Speicherarchiv zurückgestellt wurden, zu ermitteln.
2. Sichern Sie die Datenbank auf den Bändern vor Ort, indem Sie die folgenden Schritte ausführen:
  - a. Wählen Sie auf der Seite Server im Operations Center den Server aus, dessen Datenbank gesichert werden soll.
  - b. Klicken Sie auf Sichern und führen Sie die Anweisungen im Fenster Datenbank sichern aus.
3. Kopieren Sie die folgenden Dateien in das Ausgangsverzeichnis des Servers am Wiederherstellungsstandort:
  - Wiederherstellungsplandatei
  - Protokolldatei für Datenträger
  - Einheitenkonfigurationsdatei
  - Optional: Serveroptionsdatei dsmserv.opt
4. Senden Sie das Band an den Auslagerungsstandort für die Wiederherstellung.
5. Schreiben Sie die Serverdatenbank zurück, indem Sie auf dem Wiederherstellungsserver den Befehl DSMSERV RESTORE DB verwenden. Weitere Informationen zum Zurückschreiben der Serverdatenbank finden Sie in Datenbank zurückschreiben.
6. Geben Sie den Befehl UPDATE VOLUME unter Angabe des Parameters ACCESS=DESTROYED aus, um anzugeben, dass ein Datenträger vollständig zurückgeschrieben werden muss.
7. Schreiben Sie auf dem Wiederherstellungsserver die Speicherpooldatenträger mithilfe des Befehls RESTORE STGPOOL zurück.

## Nächste Schritte


---


Stellen Sie sicher, dass Sie auf die Daten in dem Speicherarchiv zugreifen können, indem Sie einen Banddatenträger in dem zurückgeschriebenen Speicherpool prüfen, um zu verifizieren, dass die Daten konsistent sind. Geben Sie den Befehl AUDIT VOLUME aus, um einen Banddatenträger zu prüfen. Prüfen Sie für eine schnellere Verarbeitung nur zurückgeschriebene Daten.


### Zugehörige Tasks:

Datenträgerbestand in einem Speicherarchiv prüfen

### Zugehörige Verweise:

 AUDIT VOLUME (Datenbankinformationen für einen Speicherpooldatenträger prüfen)

 DSMSERV RESTORE DB (Datenbank zurückschreiben)

 RESTORE STGPOOL (Speicherpooldaten zurückschreiben)

## Datenbank zurückschreiben

---

Wenn die Funktion 'Disaster Recovery Manager' (DRM) aktiviert ist und Sie die Prozedur zur Vorbereitung auf einen Katastrophenfall ausgeführt haben, können Sie die Datenbank nach einem Katastrophenfall zurückschreiben. Wenn DRM nicht konfiguriert ist, können Sie die Datenbank dennoch zurückschreiben, vorausgesetzt, Sie verfügen über die erforderlichen Sicherungsdateien.

## Vorbereitende Schritte

---

Wenn die Verzeichnisse für die Datenbank und das Wiederherstellungsprotokoll nicht mehr vorhanden sind, erstellen Sie diese erneut, bevor Sie das Serverdienstprogramm DSMSEV RESTORE DB ausführen.

## Informationen zu diesem Vorgang

---

Sie können die Datenbank mit dem neuesten Stand oder mit dem Stand eines angegebenen Zeitpunkts zurückschreiben. Um die Datenbank mit dem Stand wiederherzustellen, den sie zu dem Zeitpunkt hatte, zu dem sie verloren ging, stellen Sie die Datenbank mit der neuesten Version wieder her.

Einschränkungen:

- Um die Datenbank mit der neuesten Version zurückzuschreiben, müssen Sie das Archivprotokollverzeichnis lokalisieren. Wenn Sie das Verzeichnis nicht lokalisieren können, kann die Datenbank nur mit dem Stand eines bestimmten Zeitpunkts zurückgeschrieben werden.
- Sie können das Protokoll Secure Sockets Layer (SSL) nicht für Datenbankzurückschreibungsoperationen verwenden.
- Wenn der Release-Level der Datenbanksicherung und der Release-Level des Servers, für den die Zurückschreibung erfolgt, unterschiedlich sind, können Sie die Serverdatenbank nicht zurückschreiben. Wenn Sie beispielsweise einen Server der Version 8.1 verwenden und versuchen, eine Datenbank der Version 7.1 zurückzuschreiben, tritt ein Fehler auf.

## Vorgehensweise

---

Verwenden Sie das Serverdienstprogramm DSMSEV RESTORE DB, um die Datenbank zurückzuschreiben. Wählen Sie abhängig von der Version der Datenbank, die zurückgeschrieben werden soll, eine der folgenden Methoden aus:

- Zurückschreiben einer Datenbank mit der neuesten Version. Verwenden Sie beispielsweise den folgenden Befehl:

```
dsmserv restore db
```

- Zurückschreiben einer Datenbank mit dem Stand eines bestimmten Zeitpunkts. Um beispielsweise die Datenbank mit einer Sicherungsserie zurückzuschreiben, die am 19. April 2017 erstellt wurde, verwenden Sie den folgenden Befehl:

```
dsmserv restore db todate=04/19/2017
```

### Zugehörige Verweise:

[DSMSEV RESTORE DB \(Datenbank zurückschreiben\)](#)

## Serverlöschungsdokumentation in PDF-Dateien

---

Vordefinierte PDF-Dateien für die IBM Spectrum Protect-Dokumentation sind zum Download verfügbar.

Die folgenden vordefinierten PDF-Dateien sind für IBM Spectrum Protect-Datenschutzlösungen verfügbar:

- Einführung in Datenschutzlösungen
- Plattenspeicherlösung für einen einzelnen Standort
- Plattenspeicherlösung für mehrere Standorte
- Bandspeicherlösung

Weitere vordefinierte PDF-Dateien der Serverdokumentation finden Sie in der vollständigen Liste.

## IBM Spectrum Protect-Server

---

IBM Spectrum Protect-Server speichern und verwalten Sicherungsdaten, Archivierungsdaten und speicher verwaltete Daten für Clients für Sichern/Archivieren und andere IBM Spectrum Protect- und IBM Spectrum Protect Snapshot-Komponenten.

- Neuerungen  
Lesen Sie die Informationen zu neuen Funktionen und Aktualisierungen für Serverkomponenten in IBM Spectrum Protect Version 8.1.
- Installieren und Upgrade durchführen  
Sie können einzelne oder mehrere Komponenten in Ihrem Unternehmensnetz installieren oder für die Komponenten ein Upgrade durchführen. Mithilfe der verfügbaren Lösungsdokumentation können Sie eine Best-Practice-Lösung auf der Basis Ihrer

Unternehmensanforderungen auswählen und dann diese Lösung installieren, konfigurieren und überwachen sowie mit dieser Lösung arbeiten.

- Konfigurieren und verwalten  
Lesen Sie die Informationen in der verfügbaren Dokumentation, um Konfigurationstasks für den Server auszuführen.
- Serverbefehle, -optionen und -dienstprogramme  
Verwenden Sie Befehle, um den Server zu verwalten und zu konfigurieren, verwenden Sie Optionen, um den Server anzupassen, und verwenden Sie Dienstprogramme, um spezielle Tasks auszuführen, wenn der Server nicht aktiv ist.
- Serverdokumentation in PDF-Dateien  
Vorgefertigte PDF-Dateien für die IBM Spectrum Protect-Dokumentation sind zum Herunterladen verfügbar.

## Neuerungen

Lesen Sie die Informationen zu neuen Funktionen und Aktualisierungen für Serverkomponenten in IBM Spectrum Protect Version 8.1.

Tipp: Rufen Sie die Videobibliothek auf, um Videos zu den neuen Funktionen und Aktualisierungen anzuzeigen.

Folgen Sie den Links in der Tabelle, um Informationen zu den neuen Funktionen und Aktualisierungen zu erhalten.

| Release       | Neue Funktionen und Aktualisierungen   |
|---------------|--|
| Version 8.1.3 | <p>Server</p> <ul style="list-style-type: none"> <li>• Cloud-Tiering für die langfristige Datenaufbewahrung verwenden</li> <li>• IBM Spectrum Protect unter Linux Ubuntu Server LTS installieren</li> <li>• Sicherheit Ihrer Speicherumgebung erweitern</li> <li>• Maßnahmen zum Schutz Ihres Systems vor Ransomware ergreifen</li> </ul> <p>Operations Center<br/>Aktualisierungen für das Operations Center</p>  |
| Version 8.1.2 | <p>Server</p> <ul style="list-style-type: none"> <li>• Daten in Microsoft Azure, einem cloudbasierten Objektspeichersystem, sichern</li> <li>• Clientdaten in einem Verzeichniscontainerspeicherpool verschlüsseln</li> <li>• NAS-Dateiserver in einem Verzeichniscontainerspeicherpool sichern</li> <li>• IBM Spectrum Protect auf dem Betriebssystem Linux on Power Systems (Little Endian) installieren</li> <li>• Speicherumgebung mit einem verbesserten Sicherheitsprotokoll schützen</li> <li>• Sicherheit mit dem automatisch generierten Masterverschlüsselungsschlüssel optimieren</li> <li>• Speicherumgebung mithilfe der Bandspeicherlösung konfigurieren</li> <li>• Automatische Aktualisierungen für Clients für Sichern/Archivieren planen</li> <li>• Veraltete und nicht mehr verwendete Serveroptionen, Befehle und Parameter</li> </ul> <p>Operations Center<br/>Aktualisierungen für das Operations Center</p> |
| Version 8.1.1 | <p>Server</p> <ul style="list-style-type: none"> <li>• IBM Spectrum Protect unter dem Betriebssystem Linux on Power Systems (Little Endian) installieren</li> <li>• IBM Spectrum Protect unter dem Betriebssystem Microsoft Windows Server 2016 installieren</li> <li>• Speicherarchiv Quantum Scalar i6 verwenden</li> <li>• Gelöste Probleme überprüfen</li> </ul> <p>Operations Center</p> <ul style="list-style-type: none"> <li>• Gelöste Probleme überprüfen</li> </ul>  |

| Release     | Neue Funktionen und Aktualisierungen   |
|-------------|--|
| Version 8.1 | <p>Server</p> <ul style="list-style-type: none"> <li>• Lernen Sie IBM Spectrum Protect kennen</li> <li>• Sichere Kommunikation durch die Verwendung des Protokolls TLS 1.2</li> <li>• Bandspeicherpool in einen Containerspeicherpool konvertieren</li> <li>• Software-Upgrade für den Datenbankmanager des Servers</li> <li>• Mit dem Befehl REGISTER NODE wird eine Benutzer-ID mit Administratorberechtigung nicht mehr standardmäßig erstellt</li> <li>• Benutzerauthentifizierung mit einer Active Directory-Datenbank optimieren</li> <li>• Größere Flexibilität für den Schutz und die Konsolidierung von Banddatenträgern in Containerkopierspeicherpools</li> <li>• Unterstützte Betriebssysteme</li> <li>• System ohne Verwendung von SNMP überwachen</li> </ul> <p>Operations Center<br/>Aktualisierungen für das Operations Center</p> |

- Aktualisierungen für das Operations Center  
Neue Funktionen sind im IBM Spectrum Protect Operations Center Version 8.1.3 verfügbar. Mit dem aktualisierten Operations Center können Sie automatische Updates der IBM Spectrum Protect-Software des Clients für Sichern/Archivieren planen und Daten automatisch aus Plattenspeicher in Cloudspeicher für die langfristige Datenaufbewahrung versetzen.
- Aktualisierungen für den IBM Spectrum Protect-Server  
Neue Funktionen und andere Änderungen sind im IBM Spectrum Protect-Server der Version 8.1.3 verfügbar.
- Releaseinformationen für Serverkomponenten der Version 8.1  
Releaseinformationen sind für V8.1-Komponenten verfügbar.
- Readme-Dateien für Serverkomponenten der Version 8.1  
Readme-Dateien für Fixpacks für Version 8.1 werden auf der IBM Software Support-Website veröffentlicht. Aktualisierungen können für Serverkomponenten, einschließlich für den Server selbst, für die Einheitenunterstützung und für das Operations Center verfügbar sein.

## Aktualisierungen für das Operations Center

Neue Funktionen sind im IBM Spectrum Protect Operations Center Version 8.1.3 verfügbar. Mit dem aktualisierten Operations Center können Sie automatische Updates der IBM Spectrum Protect-Software des Clients für Sichern/Archivieren planen und Daten automatisch aus Plattenspeicher in Cloudspeicher für die langfristige Datenaufbewahrung versetzen.

Die folgenden funktionalen Erweiterungen wurden am Operations Center vorgenommen:

- Sie können Zeitpläne erstellen, um einen oder mehrere Clients für Sichern/Archivieren zu aktualisieren. Wenn neue Aktualisierungspakete freigegeben werden, werden sie automatisch heruntergeladen. Bei der Ausführung eines Plans für die Aktualisierung werden Installationsdateien in das Clientsystem kopiert und der Client wird auf die angegebene Softwareversion aktualisiert. Sie können das Operations Center auch verwenden, um Aktualisierungen zu überwachen, abzubrechen oder erneut zu planen.
- Sie können Speicherregeln erstellen, um Daten automatisch auf der Basis ihres Alters aus Verzeichniscontainerspeicherpools in Cloud-Containerspeicherpools zu versetzen. Die verschiedenen Typen, oder *Tiers*, von Speicher bieten verschiedene Vor- und Nachteile in Bezug auf Kosten und Leistung. Sie können ältere Daten in Speicher mit geringerer Leistung in der Cloud archivieren und neue Datensicherungen auf Hochleistungsplatten für schnellere Zurückschreibungsoperationen aufbewahren.

Weitere Informationen zu diesen funktionalen Erweiterungen finden Sie in der Hilfe des Operations Center.

### Zugehörige Tasks:

Clientaktualisierungen planen

## Aktualisierungen für den IBM Spectrum Protect-Server

Neue Funktionen und andere Änderungen sind im IBM Spectrum Protect-Server der Version 8.1.3 verfügbar.

- Cloud-Tiering für die langfristige Datenaufbewahrung verwenden  
Mit IBM Spectrum Protect Version 8.1.3 können Sie Cloud-Tiering verwenden, um Daten, auf die selten zugegriffen wird, in einen Cloud-Containerspeicherpool zu versetzen.
- IBM Spectrum Protect unter Linux Ubuntu Server LTS installieren  
Sie können IBM Spectrum Protect Version 8.1.3 auf dem Betriebssystem Ubuntu Server 16.04 LTS installieren. Nachdem der

Server der Version 8.1.3 unter Ubuntu Server 16.04 LTS installiert und konfiguriert wurde, können Sie Daten auf Platteneinheiten und im Cloudobjektspeicher sichern.

- Sicherheit Ihrer Speicherumgebung erweitern  
IBM Spectrum Protect Version 8.1.3 stellt Sicherheitsverbesserungen bereit.
- Maßnahmen zum Schutz Ihres Systems vor Ransomware ergreifen  
Die Dokumentation für IBM Spectrum Protect Version 8.1.3 enthält Anleitungen zum Schützen Ihrer Speicherumgebung vor Ransomware-Attacken.

## Cloud-Tiering für die langfristige Datenaufbewahrung verwenden

---

Mit IBM Spectrum Protect Version 8.1.3 können Sie Cloud-Tiering verwenden, um Daten, auf die selten zugegriffen wird, in einen Cloud-Containerspeicherpool zu versetzen.

Sie können IBM Spectrum Protect konfigurieren, um operative Daten auf Hochleistungsplatten zu speichern und dann die Daten im Laufe ihres Alters in Cloud-Containerspeicherpools zu versetzen. Die Cloud-Containerspeicherpools können für die On-Premises- oder Off-Premises-Speicherung in einem Cloud-Computing-System 'Microsoft Azure' oder einem Cloud-Computing-System mit dem Protokoll 'Simple Storage Service' (S3) konfiguriert werden.

Verwenden Sie eine der folgenden Methoden, um das Cloud-Tiering zwischen Speicherpools zu planen:

- Klicken Sie im IBM Spectrum Protect Operations Center auf Speicher > Tiering-Regeln.
- Führen Sie den Befehl DEFINE STGRULE aus.

### Zugehörige Informationen:

Speicherregel für Cloud-Tiering definieren

DEFINE STGRULE (Speicherregel für Speicherpools definieren)

UPDATE STGRULE (Speicherregel für Speicherpools aktualisieren)

## IBM Spectrum Protect unter Linux Ubuntu Server LTS installieren

---

Sie können IBM Spectrum Protect Version 8.1.3 auf dem Betriebssystem Ubuntu Server 16.04 LTS installieren. Nachdem der Server der Version 8.1.3 unter Ubuntu Server 16.04 LTS installiert und konfiguriert wurde, können Sie Daten auf Platteneinheiten und im Cloudobjektspeicher sichern.

Die Installationspakete umfassen den Server und die Lizenz, Einheitentreibertools und den Speicheragenten. Es gelten die folgenden Einschränkungen:

- Sie können keinen Bandeinheitenspeicher verwenden.
- Sie können nicht Disaster Recovery Manager (DRM) verwenden.
- Sie können die Datenübertragung zu fernen Servern nicht optimieren, indem Sie die Aspera® FASP®-Technologie (FASP = Fast Adaptive Secure Protocol) aktivieren.
- Es kann keine Clusterumgebung konfiguriert werden.
- Sie können nicht das Operations Center verwenden, um das System zu überwachen und zu verwalten.
- Sie können Verzeichniscontainerspeicherpools nicht schützen, indem Sie den Befehl PROTECT STGPOOL verwenden.

### Zugehörige Tasks:

Linux: Server installieren

### Zugehörige Verweise:

Linux: Servermindestvoraussetzungen für Linux x86\_64

### Zugehörige Informationen:

Verfügbarkeit von Funktionen nach Betriebssystem

## Sicherheit Ihrer Speicherumgebung erweitern

---

IBM Spectrum Protect Version 8.1.3 stellt Sicherheitsverbesserungen bereit.

Server, Clients und Speicheragenten, die IBM Spectrum Protect-Software der Version 8.1.3 oder höher oder Tivoli Storage Manager-Software der Version 7.1.8 oder höher verwenden, werden automatisch für die Kommunikation miteinander unter Verwendung des Protokolls Transport Layer Security (TLS) 1.2 konfiguriert. Zertifikate werden automatisch verteilt.

Einschränkungen:

- In Version 8.1.2 mussten Speicheragenten manuell für die Verwendung von SSL konfiguriert werden. An Version 8.1.3 werden Speicheragenten automatisch für die Verwendung von SSL konfiguriert. Speicherarchivclients und Speicherarchivmanager-Server verwenden automatisch SSL, um mit Speicheragenten zu kommunizieren, die Software der Version 7.1.8 oder höher oder

Software der Version 8.1.2 oder höher verwenden, aber Sie müssen die Zertifikate manuell konfigurieren. Ein Speicheragent tauscht automatisch Zertifikate mit seinem Datenbankserver aus.

- Nachdem sich ein Administrator erfolgreich mithilfe von IBM Spectrum Protect-Software der Version 8.1.2 oder höher oder Tivoli Storage Manager-Software der Version 7.1.8 oder höher authentifiziert hat, kann sich der Administrator nicht mehr bei Clients oder Servern authentifizieren, die frühere Versionen verwenden. Diese Einschränkung gilt auch, wenn Sie Funktionen wie Befehlsweiterleitung oder Export zwischen Servern verwenden, wenn sich der Administrator beim IBM Spectrum Protect-Server als Administrator von einem anderen Server authentifiziert.

Die neuesten Informationen zu Sicherheitsupdates für Version 8.1.3 finden Sie in Technote 2004844.

**Zugehörige Konzepte:**

Sicherheitskonzepte

**Zugehörige Tasks:**

Speicheragenten, Server, Clients und das Operations Center für die Verbindung zum Server unter Verwendung von SSL konfigurieren

**Zugehörige Verweise:**

Kommunikation schützen

## Maßnahmen zum Schutz Ihres Systems vor Ransomware ergreifen

---

Die Dokumentation für IBM Spectrum Protect Version 8.1.3 enthält Anleitungen zum Schützen Ihrer Speicherumgebung vor Ransomware-Attacken.

Wenn Sie die Anleitungen zum Konfigurieren Ihrer Speicherumgebung und zum Verwalten von Aufbewahrungsmaßnahmen befolgen, können Sie das Risiko einer Ransomware-Attacke reduzieren und die Möglichkeit einer Wiederherstellung Ihrer Speicherumgebung erhöhen, wenn eine Attacke erfolgt. Sie können die Funktion Disaster Recovery Manager (DRM) von IBM Spectrum Protect für die Vorbereitung auf und die Wiederherstellung nach Ransomware-Attacken verwenden. Mit dem Operations Center können Sie Ihre Speicherumgebung genau überwachen und Anzeichen für unbefugten Zugriff erkennen. Überprüfen Sie die Anleitungen und ergreifen Sie die entsprechenden Maßnahmen zum Schützen Ihrer Daten.

**Zugehörige Tasks:**

Speicherumgebung vor Ransomware-Attacken schützen

## Releaseinformationen für Serverkomponenten der Version 8.1

---

Releaseinformationen sind für V8.1-Komponenten verfügbar.

- Releaseinformationen für IBM Spectrum Protect-Server Version 8.1  
Der IBM Spectrum Protect-Server Version 8.1 ist verfügbar. Informationen zur Kompatibilität und Installation sowie andere Informationen zu den ersten Schritten werden bereitgestellt.
- Releaseinformationen für Operations Center Version 8.1  
Das Operations Center ist eine webbasierte Schnittstelle, mit der Sie Ihre IBM Spectrum Protect-Umgebung verwalten können. Die Releaseinformationen bieten Ihnen Zugriff auf die Produktankündigung, bekannte Probleme, Systemvoraussetzungen, Installationsanweisungen und Aktualisierungen.
- Releaseinformationen für IBM Spectrum Protect-Einheitenunterstützung Version 8.1  
Die IBM Spectrum Protect-Einheitenunterstützung für Version 8.1 ist verfügbar. Informationen zur Kompatibilität und Installation sowie andere Informationen zu den ersten Schritten werden bereitgestellt.

## Releaseinformationen für IBM Spectrum Protect-Server Version 8.1

---

Der IBM Spectrum Protect-Server Version 8.1 ist verfügbar. Informationen zur Kompatibilität und Installation sowie andere Informationen zu den ersten Schritten werden bereitgestellt.

### Inhalt

---

- Beschreibung
- Ankündigung
- Kompatibilität mit früheren Versionen
- Systemvoraussetzungen
- IBM Spectrum Protect installieren und Upgrade durchführen
- Aktualisierungen, Einschränkungen und bekannte Probleme

### Beschreibung

---

IBM Spectrum Protect stellt automatisierte, zentral geplante, maßnahmenverwaltete Sicherungs-, Archivierungs- und Speicherverwaltungsfunktionen für Dateiserver, Workstations, virtuelle Maschinen und Anwendungen bereit.

Ein Authorized Program Analysis Report (APAR) ist eine Anforderung für die Korrektur eines Fehlers in einem unterstützten Release eines von IBM gelieferten Programms. Eine Liste der behobenen APARs finden Sie in APARs fixed in IBM Spectrum Protect server Version 8.1.

## Ankündigung

---

Die Ankündigung für die IBM Spectrum Protect-Produktfamilie der Version 8.1 enthält die folgenden Informationen:

- Ausführliche Produktbeschreibung, einschließlich Beschreibungen neuer Funktionen
- Produktpositionierungsanweisung
- Internationale Kompatibilitätsinformationen

Führen Sie die folgenden Schritte aus, um nach der Produktankündigung zu suchen:

1. Rufen Sie die Produktankündigungswebsite auf.
2. Geben Sie in das Feld Search for die Produkt-ID (PID) für Ihr Produkt ein. Die PID für IBM Spectrum Protect lautet 5725-W98.
3. Wählen Sie im Feld Information Type den Eintrag Announcement letters aus und klicken Sie auf Search.
4. Wählen Sie aus der Liste Search in den Eintrag Product Number aus.
5. Optional: Wählen Sie im Teilfenster 'Refine Your Search' auf der linken Seite des Fensters das Land aus, in dem Sie sich befinden.
6. Wählen Sie im Abschnitt Sort by den Eintrag Newest first aus.

## Kompatibilität mit früheren Versionen

---

Informationen zur Kompatibilität mit früheren Versionen befinden sich unter IBM Spectrum Protect Server-Client Compatibility and Upgrade Considerations.

## Systemvoraussetzungen

---

Informationen zu den Systemvoraussetzungen finden Sie unter IBM Spectrum Protect Supported Operating Systems.

## IBM Spectrum Protect installieren und Upgrade durchführen

---

Anweisungen für die Serverinstallation finden Sie in der Prozedur für Ihr Betriebssystem:

IBM AIX

Server installieren

Linux

Server installieren

Microsoft Windows

Server installieren

Upgradeanweisungen finden Sie in Upgrade auf Version 8.1 durchführen.

## Aktualisierungen, Einschränkungen und bekannte Probleme

---

Aktualisierungen beschreiben neue Produktinformationen oder neue Produktfunktionen, die nach der Freigabe des Produkts verfügbar werden. Aktualisierungen, Einschränkungen und bekannte Probleme sind in Form von technischen Hinweisen in der Unterstützungswissensbasis im IBM® Support Portal dokumentiert. Durchsuchen Sie die Wissensbasis, um Fehlerumgehungen oder Lösungen für bekannte Probleme zu finden.

Aktualisierungen

**Mit dem Befehl REGISTER NODE wird eine Benutzer-ID mit Administratorberechtigung nicht mehr standardmäßig erstellt**

Ab IBM Spectrum Protect Version 8.1 wird mit dem Befehl REGISTER NODE nicht automatisch eine Benutzer-ID mit Administratorberechtigung erstellt, die mit dem Knotennamen übereinstimmt. Diese Produktaktualisierung kann Auswirkungen auf den Prozess zum Registrieren von Clientknoten, einschließlich IBM Spectrum Protect-Knoten des Clients für Sichern/Archivieren, haben. In einigen Fällen müssen Sie möglicherweise eine Benutzer-ID mit Administratorberechtigung erstellen, indem Sie den Parameter USERID im Befehl REGISTER NODE angeben. Informationen zu den betroffenen Clienttypen finden Sie in Technote 7048963.

Um nach den neuesten Aktualisierungen zu suchen, rufen Sie die Website Updates for IBM Spectrum Protect V8.1 auf.

Einschränkungen und bekannte Probleme

Zum Zeitpunkt der Veröffentlichung waren keine Einschränkungen oder Probleme bekannt.

Die aktuellen Einschränkungen und bekannten Probleme, die weitere Einträge umfassen können, finden Sie in Limitations and known problems for IBM Spectrum Protect V8.1.

## Releaseinformationen für Operations Center Version 8.1

---

Das Operations Center ist eine webbasierte Schnittstelle, mit der Sie Ihre IBM Spectrum Protect-Umgebung verwalten können. Die Releaseinformationen bieten Ihnen Zugriff auf die Produktankündigung, bekannte Probleme, Systemvoraussetzungen, Installationsanweisungen und Aktualisierungen.

### Inhalt

---

- Beschreibung
- Ankündigung
- Kompatibilität mit dem IBM Spectrum Protect-Server
- Systemvoraussetzungen
- Operations Center installieren oder Upgrade für das Operations Center durchführen
- Aktualisierungen, Einschränkungen und bekannte Probleme

### Beschreibung

---

Mit dem Operations Center können Sie die folgenden Aktionen ausführen:

- Potenzielle Probleme mit Ihrer IBM Spectrum Protect-Umgebung identifizieren
- Schlüsselaspekte der Speicherumgebung überwachen: Alerts, Clients, Server, Maßnahmen, Speicherpools und Speichereinheiten
- Clients registrieren
- Server hinzufügen, die überwacht werden sollen
- Clients, Serverdatenbanken und Speicherpools sichern
- Speicherpoolumlagerung und -konsolidierung starten
- Administratoren Alerts zuordnen und Alerts schließen
- Serverprozesse und Clientsitzungen anzeigen und abbrechen
- Einstellungen für Client, Server, Speicherpool und Speichereinheit ändern
- Clientzeitpläne erstellen und verwalten und Verwaltungszeitpläne anzeigen
- Primäre Speicherpools in Containerspeicherpools konvertieren
- Daten aus Verzeichniscontainerspeicherpools auf Band kopieren
- Replikation konfigurieren
- Maßnahmeneinstellungen ändern
- Clients stilllegen und Daten inaktivieren
- E-Mail-Berichte erstellen
- Front-End- und Back-End-Kapazitätsnutzung anzeigen, um die Lizenz Einhaltung zu überwachen
- Befehle an IBM Spectrum Protect-Server ausgeben

Ein Authorized Program Analysis Report (APAR) ist eine Anforderung für die Korrektur eines Fehlers in einem unterstützten Release eines von IBM gelieferten Programms. Eine Liste der behobenen APARs finden Sie in APARs fixed in IBM Spectrum Protect Operations Center Version 8.1.

### Ankündigung

---

Das Operations Center ist Teil der IBM Spectrum Protect-Produktfamilie Version 8.1. Die Ankündigung für diese Produkte enthält die folgenden Informationen:

- Ausführliche Produktbeschreibung, einschließlich Beschreibungen neuer Funktionen
- Produktpositionierungsanweisung
- Internationale Kompatibilitätswarnungen

Führen Sie die folgenden Schritte aus, um nach der Produktankündigung zu suchen:

1. Rufen Sie die Produktankündigungswebsite auf.
2. Geben Sie in das Feld Search für die Produkt-ID (PID) für Ihr Produkt ein. Die PID für IBM Spectrum Protect lautet 5725-W98.
3. Wählen Sie im Feld Information Type den Eintrag Announcement letters aus und klicken Sie auf Search.
4. Wählen Sie aus der Liste Search in den Eintrag Product Number aus.
5. Optional: Wählen Sie im Teilfenster 'Refine Your Search' auf der linken Seite des Fensters das Land aus, in dem Sie sich befinden.
6. Wählen Sie im Abschnitt Sort by den Eintrag Newest first aus.

### Kompatibilität mit dem IBM Spectrum Protect-Server

---



Kompatibilitätswisseninformationen befinden sich in IBM Spectrum Protect server and Operations Center compatibility.

## Systemvoraussetzungen

---

Systemvoraussetzungen befinden sich in IBM Spectrum Protect Operations Center software and hardware requirements.

## Operations Center installieren oder Upgrade für das Operations Center durchführen

---

Installationsanweisungen oder Informationen zur Durchführung eines Upgrades für die bisherige Version des Operations Center befinden sich in Operations Center installieren und Upgrade für das Operations Center durchführen.

## Aktualisierungen, Einschränkungen und bekannte Probleme

---

Aktualisierungen beschreiben neue Produktinformationen oder neue Produktfunktionen, die nach der Freigabe des Produkts verfügbar werden. Aktualisierungen, Einschränkungen und bekannte Probleme sind in Form von technischen Hinweisen in der Unterstützungswissensbasis im IBM® Support Portal dokumentiert. Durchsuchen Sie die Wissensbasis, um Fehlerumgehungen oder Lösungen für bekannte Probleme zu finden.

### Aktualisierungen

Eine aktuelle Liste der Aktualisierungen befindet sich in Search results for updates to Operations Center V8.1.

### Einschränkungen und bekannte Probleme

- Eine Liste der Einschränkungen und bekannten Probleme befindet sich in Limitations and known issues with Operations Center V8.1.
- Um nach weiteren Problemen zu suchen, die nach der Freigabe des Produkts bekannt werden können, rufen Sie die Website Search results for known issues with Operations Center V8.1 auf.

## Releaseinformationen für IBM Spectrum Protect-Einheitenunterstützung Version 8.1

---

Die IBM Spectrum Protect-Einheitenunterstützung für Version 8.1 ist verfügbar. Informationen zur Kompatibilität und Installation sowie andere Informationen zu den ersten Schritten werden bereitgestellt.

### Inhalt

---

- Beschreibung
- Ankündigung
- Unterstützte Einheiten
- Einheitentreiberanforderungen
- Speicherarchivinformationen
- Aktualisierungen, Einschränkungen und bekannte Probleme

### Beschreibung

---

Dieses Dokument enthält Informationen zu Einheitentreibern von IBM Spectrum Protect Version 8.1.

Ein Authorized Program Analysis Report (APAR) ist eine Anforderung für die Korrektur eines Fehlers in einem unterstützten Release eines von IBM gelieferten Programms. Eine Liste der behobenen APARs finden Sie in APARs Fixed in IBM Spectrum Protect device driver Version 8.1.

### Ankündigung

---

Die IBM Spectrum Protect-Einheitenunterstützung für Version 8.1 wird als Teil der Ankündigung der IBM Spectrum Protect-Produktfamilie angekündigt. Die Ankündigung für diese Produkte enthält die folgenden Informationen:

- Ausführliche Produktbeschreibung, einschließlich Beschreibungen neuer Funktionen
- Produktpositionierungsanweisung
- Internationale Kompatibilitätswisseninformationen

Führen Sie die folgenden Schritte aus, um nach der Produktankündigung zu suchen:

1. Rufen Sie die Produktankündigungswebsite auf.
2. Geben Sie in das Feld Search for die Produkt-ID (PID) für Ihr Produkt ein. Die PID für IBM Spectrum Protect lautet 5725-W98.

3. Wählen Sie im Feld Information Type den Eintrag Announcement letters aus und klicken Sie auf Search.
4. Wählen Sie aus der Liste Search in den Eintrag Product Number aus.
5. Optional: Wählen Sie im Teilfenster 'Refine Your Search' auf der linken Seite des Fensters das Land aus, in dem Sie sich befinden.
6. Wählen Sie im Abschnitt Sort by den Eintrag Newest first aus.

## Unterstützte Einheiten

---

Informationen zu den unterstützten Einheiten und zur unterstützten Hardware für IBM AIX- und Microsoft Windows-Systeme finden Sie unter Supported devices for AIX and Windows.

Informationen zu den unterstützten Einheiten und zur unterstützten Hardware für Linux-Systeme finden Sie unter Supported devices for Linux.

## Einheitentreiberanforderungen

---

### Anforderungen für Hostbusadapter

Um die besten Ergebnisse zu erzielen, sollten Bandlaufwerke und Bandarchive an ihrem eigenen Hostbusadapter mit dem System verbunden werden. Verwenden Sie den Hostbusadapter nicht gemeinsam mit anderen Einheitentypen, wie z. B. DISK oder CD.

### Maximale Anzahl Einheiten, die von IBM Spectrum Protect-Einheitentreibern unterstützt werden

Informationen zur maximalen Anzahl von Einheiten, die von IBM Spectrum Protect-Einheitentreibern auf jedem Betriebssystem unterstützt werden können, befinden sich in Technote 1364225.

### Unterstützung für seriell angeschlossene SCSI-Einheiten (Serial Attached SCSI - SAS)

SAS-Einheiten können auf einigen Betriebssystemen und in einigen Architekturen verwendet werden. Informationen zu Betriebssystemen und Architekturen für SAS-Einheiten befinden sich in Technote 1396706.

### IBM Spectrum Protect-Durchgriffstreiber mit einer Benutzer-ID ohne Rootberechtigung auf Linux-Betriebssystemen ausführen

Informationen darüber, wie ein Benutzer ohne Rootberechtigung Einheiten mit dem IBM Spectrum Protect-Durchgriffstreiber unter Linux verwenden kann, befinden sich in Technote 1321130. Verwenden Sie Option -g oder -a des Einheitendienstprogramms autoconf, um sicherzustellen, dass Benutzer ohne Rootberechtigung Einheiten verwenden können, die mit dem IBM Spectrum Protect-Durchgriffstreiber konfiguriert sind. Verwenden Sie Option -g, um den Einheitsdateien des generischen SCSI-Treibers (sg) Lese- und Schreibberechtigungen für Gruppen hinzuzufügen. Verwenden Sie Option -a, um den sg-Einheitsdateien Lese- und Schreibberechtigungen für alle Benutzer hinzuzufügen.

## Speicherarchivinformationen

---

- IBM Spectrum Protect Extended Edition ist für ein Speicherarchiv mit mehr als vier Laufwerken oder mehr als 48 Speicherschächten erforderlich.
- Die Elementadressen der Speicherschächte entsprechen möglicherweise nicht direkt den Nummern der Speicherschächte. Dies ist wichtig, da der IBM Spectrum Protect-Server auf die Speicherschächte immer mit Elementadressen und nicht mit den Nummern der Speicherschächte verweist. Elementadressen können der Seite für die Speicherarchivkonfiguration für jedes Speicherarchiv entnommen werden.
- Für ein Speicherarchiv mit mehreren Laufwerken ist eine Laufwerkelementadresse für die Befehle DEFINE und UPDATE DRIVE erforderlich. Meldet das Speicherarchiv jedoch Laufwerkseriennummern zurück, können Sie ELEMENT=AUTODETECT angeben und die Elementadresse ist nicht erforderlich.
- Die Prozedur zum Konfigurieren des Datenträgerwechslers und zum separaten Konfigurieren jedes Laufwerks befindet sich in Speichereinheiten konfigurieren und verwalten.

## Aktualisierungen, Einschränkungen und bekannte Probleme

---

### Aktualisierungen

Einige Einheiten, die von früheren Releases von IBM Spectrum Protect unterstützt wurden, werden vom IBM Spectrum Protect-Server der Version 8.1 nicht mehr unterstützt. Für die aktuelle Liste der unterstützten Einheiten siehe die folgenden Links:

- Supported devices for AIX and Windows
- Supported devices for Linux

Die neuesten Aktualisierungen, Einschränkungen und bekannten Probleme, die weitere Einträge umfassen können, finden Sie in Updates, limitations, and known problems for IBM Spectrum Protect V8.1 device support.

## Readme-Dateien für Serverkomponenten der Version 8.1

---

Readme-Dateien für Fixpacks für Version 8.1 werden auf der IBM Software Support-Website veröffentlicht. Aktualisierungen können für Serverkomponenten, einschließlich für den Server selbst, für die Einheitenunterstützung und für das Operations Center verfügbar sein.

## Installieren und Upgrade durchführen

- IBM Spectrum Protect-Lösung implementieren  
Wenn Sie eine neue IBM Spectrum Protect-Serverumgebung implementieren, ziehen Sie die Implementierung einer Best-Practice-Konfiguration in Betracht.
- Server installieren und Upgrade durchführen  
Der IBM Spectrum Protect-Server stellt Sicherungs-, Archivierungs- und Speicherverwaltungsservices für Clients zur Verfügung. Sie können einzelne oder mehrere Server in Ihrem Unternehmensnetz installieren oder für die Server ein Upgrade durchführen.
- Operations Center installieren und Upgrade für das Operations Center durchführen  
Das Operations Center ist die webbasierte Schnittstelle zum Verwalten Ihrer Speicherumgebung.

## IBM Spectrum Protect-Lösung implementieren

Wenn Sie eine neue IBM Spectrum Protect-Serverumgebung implementieren, ziehen Sie die Implementierung einer Best-Practice-Konfiguration in Betracht.

Mithilfe der verfügbaren IBM Spectrum Protect-Lösungsdokumentation können Sie eine Best-Practice-Lösung auf der Basis Ihrer Unternehmensanforderungen auswählen und dann diese Lösung installieren, konfigurieren und überwachen sowie mit dieser Lösung arbeiten.

Ausführliche Informationen finden Sie in IBM Spectrum Protect-Lösung auswählen.

## Verfügbarkeit von Funktionen nach Betriebssystem

Die meisten IBM Spectrum Protect-Funktionen sind auf allen Betriebssystemen verfügbar, die für den Server unterstützt werden.

In der folgenden Tabelle gibt ein Haken an, dass eine Funktion verfügbar ist.

Tabelle 1. Verfügbarkeit von IBM Spectrum Protect-Funktionen nach Betriebssystem

| Funktion   | IBM® AIX | Linux x86_64  | Linux on System z | Linux on Power Systems (Little Endian) | Microsoft Windows |
|--|----------|---|-------------------|--|-------------------|
| Aspera FASP-Technologie (FASP = Fast Adaptive Secure Protocol):<br>Datenübertragung zu einem fernen Server optimieren. |          | ☑<br>Einschränkung: Aspera FASP-Technologie wird unter Ubuntu Server LTS nicht unterstützt. |                   |  |                   |
| Cloudspeicher unter Verwendung von Amazon S3-Technologie (Amazon Simple Storage Service).                              | ☑        | ☑   |                   | ☑                                      | ☑                 |
| Cloudspeicher unter Verwendung von IBM Cloud Object Storage-Technologie.   | ☑        | ☑   |                   | ☑                                      | ☑                 |
| Cloudspeicher unter Verwendung von IBM SoftLayer-Technologie (IBM Bluemix).  | ☑        | ☑   |                   | ☑                                      | ☑                 |
| Cloudspeicher unter Verwendung von Microsoft Azure-Technologie.  | ☑        | ☑   |                   | ☑                                      | ☑                 |
| Cloudspeicher unter Verwendung von OpenStack Swift-Technologie.  | ☑        | ☑   |                   | ☑                                      | ☑                 |

| Funktion  | IBM® AIX | Linux x86_64  | Linux on System z | Linux on Power Systems (Little Endian) | Microsoft Windows |
|---|----------|---|-------------------|--|-------------------|
| Datendeduplizierung:<br>Verwenden Sie die <i>Inline-Datendeduplizierung</i> , um doppelte Daten zu eliminieren, während die Daten in einen Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool geschrieben werden. Mithilfe der Inline-Datendeduplizierung können Sie die Notwendigkeit der Offlinereorganisation reduzieren, die Serverleistung verbessern und die Kosten für Speicherhardware verringern. | ✓        | ✓   | ✓                 | ✓                                      | ✓                 |
| Datendeduplizierung:<br>Verwenden Sie die <i>nachgeordnete Datendeduplizierung</i> , um doppelte Daten aus Plattenspeicherpools mit sequenziellem Zugriff zu eliminieren. Diese Option kann zu längeren Verarbeitungszeiten führen, da der Server die Daten identifizieren und dann die Daten aus dem Speicherpool entfernen muss.  | ✓        | ✓   | ✓                 | ✓                                      | ✓                 |
| Disaster Recovery Manager (DRM):<br>Bereiten Sie einen Plan für die Wiederherstellung Ihrer Server- und Clientdaten vor, wenn ein Katastrophenfall eintritt.  | ✓        | ✓   | ✓                 | ✓                                      | ✓                 |
| Inline-Datenkomprimierung:<br>Komprimieren Sie Daten, wenn sie in einen Cloud-Containerspeicherpool oder Verzeichniscontainerspeicherpool geschrieben werden, um den Umfang des Speicherbereichs zu reduzieren, der von den Daten belegt wird.  | ✓        | ✓   | ✓                 | ✓                                      | ✓                 |
| LDAP-Authentifizierung (LDAP = Lightweight Directory Access Protocol):<br>Authentifizieren Sie Benutzer bei einer Active Directory-Datenbank auf einem LDAP-Server.   | ✓        | ✓   | ✓                 | ✓                                      | ✓                 |
| Knotenreplikation:<br>Kopieren Sie inkrementell Daten, die zu Knoten des Clients für Sichern/Archivieren gehören, von einem Server auf einen anderen Server.  | ✓        | ✓   | ✓                 | ✓                                      | ✓                 |
| Operations Center:<br>Überwachen und verwalten Sie die Speicherumgebung mithilfe des Operations Center, einer webbasierten Benutzerschnittstelle.   | ✓        | ✓<br>Einschränkung: Das Operations Center wird unter Ubuntu Server LTS nicht unterstützt. | ✓                 | ✓                                      | ✓                 |

| Funktion  | IBM® AIX | Linux x86_64   | Linux on System z | Linux on Power Systems (Little Endian) | Microsoft Windows |
|---|----------|--|-------------------|--|-------------------|
| Schutz von Verzeichniscontainerspeicherpools:<br>Schützen Sie Daten in Verzeichniscontainerspeicherpools mithilfe des Befehls PROTECT STGPOOL. Sie können eine Kopie der Daten in einem anderen Verzeichniscontainerspeicherpool auf einem Zielreplikationsserver speichern oder eine Kopie auf Band in einem Containerkopierspeicherpool auf demselben Server speichern. | ✓        | ✓<br>Einschränkung: Diese Funktion wird unter Ubuntu Server LTS nicht unterstützt. | ✓                 | ✓                                      | ✓                 |
| Speicherpoolverschlüsselung:<br>Verschlüsseln Sie Daten in Cloud-Containerspeicherpools.  | ✓        | ✓  |                   | ✓                                      | ✓                 |
| Speicherpoolverschlüsselung:<br>Verschlüsseln Sie Daten in Verzeichniscontainerspeicherpools.   | ✓        | ✓  | ✓                 | ✓                                      | ✓                 |
| Bandspeicher:<br>Speichern Sie Daten auf Band. Dadurch wird eine flexible und kosteneffiziente Option für die langfristige Datenaufbewahrung bereitgestellt.  | ✓        | ✓<br>Einschränkung: Bandspeicher wird unter Ubuntu Server LTS nicht unterstützt.   | ✓                 | ✓                                      | ✓                 |
| Protokoll Transport Layer Security (TLS) 1.2:<br>Schützen Sie die Kommunikation mithilfe von TLS 1.2.   | ✓        | ✓  | ✓                 | ✓                                      | ✓                 |

## Server installieren und Upgrade durchführen

Der IBM Spectrum Protect-Server stellt Sicherheits-, Archivierungs- und Speicherverwaltungsservices für Clients zur Verfügung. Sie können einzelne oder mehrere Server in Ihrem Unternehmensnetz installieren oder für die Server ein Upgrade durchführen.

- Server auf AIX-Systemen installieren
- Server auf Linux-Systemen installieren
- Server auf Windows-Systemen installieren
- Upgrade für den Server durchführen

## AIX: Server installieren

Zur Installation des Servers gehören Planung, Installation und Erstkonfiguration.



- AIX
- AIX: Installation des Servers planen  
Installieren Sie die Server-Software auf dem Computer, der Speichereinheiten verwaltet, und die Client-Software auf jeder Workstation, die Daten an den vom IBM Spectrum Protect-Server verwalteten Speicher überträgt.
- AIX: Serverkomponenten installieren  
Für die Installation der Serverkomponenten der Version 8.1.3 können Sie den Installationsassistenten, die Befehlszeile im Konsolenmodus oder den unbeaufsichtigten Modus verwenden.
- AIX: Die ersten Schritte nach der Installation von IBM Spectrum Protect  
Nach der Installation von Version 8.1.3 bereiten Sie die Konfiguration vor. Bevorzugte Methode für die Konfiguration der IBM Spectrum Protect-Instanz ist die Verwendung des Konfigurationsassistenten.

- AIX: IBM Spectrum Protect-Server-Fixpack installieren  
IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe.
- AIX: Von Version 8.1.3 auf eine vorherige Serverversion zurücksetzen  
Wenn Sie nach einem Upgrade auf die vorherige Version des Servers zurücksetzen müssen, benötigen Sie eine Datenbankgesamticherung der ursprünglichen Version. Außerdem benötigen Sie die Serverinstallationsmedien für Ihre ursprüngliche Version und Schlüsselkonfigurationsdateien. Führen Sie die Schritte zur Vorbereitung sorgfältig aus, bevor Sie das Upgrade des Servers durchführen. Dadurch könnte das Zurücksetzen auf die vorherige Version des IBM Spectrum Protect-Servers mit minimalem Datenverlust möglich sein.
- AIX: Referenz: DB2-Befehle für IBM Spectrum Protect-Serverdatenbanken  
Verwenden Sie diese Liste als Referenz, wenn der IBM® Support Sie anweist, DB2-Befehle auszugeben.
- AIX: IBM Spectrum Protect deinstallieren  
Sie können IBM Spectrum Protect mit den folgenden Methoden deinstallieren. Vor dem Entfernen von IBM Spectrum Protect müssen Sie sicherstellen, dass Ihre Sicherungs- und Archivierungsdaten nicht verloren gehen.

## AIX: Installation des Servers planen

---

Installieren Sie die Server-Software auf dem Computer, der Speichereinheiten verwaltet, und die Client-Software auf jeder Workstation, die Daten an den vom IBM Spectrum Protect-Server verwalteten Speicher überträgt.


- AIX: Vorausgesetzte Kenntnisse  
Sie müssen mit Ihren Betriebssystemen, Speichereinheiten, Übertragungsprotokollen und Systemkonfigurationen vertraut sein, bevor Sie IBM Spectrum Protect installieren.
- AIX: Planung für optimale Leistung  
Überprüfen Sie vor der Installation des IBM Spectrum Protect-Servers die Merkmale und die Konfiguration des Systems, um sicherzustellen, dass der Server für die optimale Leistung konfiguriert ist.
-  AIX-BetriebssystemeAIX: Systemmindestvoraussetzungen für AIX-Systeme  
Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem AIX-Betriebssystem ohne Datenduplizierung installieren.
-  AIX-BetriebssystemeAIX: Kompatibilität des IBM Spectrum Protect-Servers mit anderen DB2-Produkten auf dem System  
Sie können andere Produkte, die DB2-Produkte auf demselben System wie der IBM Spectrum Protect-Server der Version 8.1.3 implementieren und verwenden, mit einigen Einschränkungen installieren.
- AIX: IBM Installation Manager  
IBM Spectrum Protect verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositories installiert oder aktualisiert werden können.
- AIX: Arbeitsblätter für Planungsdetails für den Server  
Sie können die Arbeitsblätter für die Planung der Größe und der Position des für den IBM Spectrum Protect-Server benötigten Speichers verwenden. Sie können darauf auch Namen und Benutzer-IDs aufzeichnen.
- AIX: Kapazitätsplanung  
Zur Kapazitätsplanung für IBM Spectrum Protect gehört die Verwaltung von Ressourcen wie z. B. die Datenbank, das Wiederherstellungsprotokoll und der Bereich für gemeinsam genutzte Ressourcen. Sie müssen den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll schätzen, um die Ressourcen als Teil der Kapazitätsplanung zu maximieren. Der verfügbare Speicherplatz für den Bereich für gemeinsam genutzte Ressourcen muss für jede Installation bzw. jedes Upgrade ausreichen.
- AIX: Empfehlungen für die Serverbenennung  
Verwenden Sie diese Beschreibungen als Referenz bei der Installation oder beim Upgrade eines IBM Spectrum Protect-Servers.
- AIX: Installationsverzeichnisse  
Zu den Installationsverzeichnissen für den IBM Spectrum Protect-Server gehören die Verzeichnisse für den Server, DB2, die Einheiten, die Sprache und andere Verzeichnisse. Jedes Verzeichnis enthält mehrere zusätzliche Verzeichnisse.

## AIX: Vorausgesetzte Kenntnisse

---

Sie müssen mit Ihren Betriebssystemen, Speichereinheiten, Übertragungsprotokollen und Systemkonfigurationen vertraut sein, bevor Sie IBM Spectrum Protect installieren.

Wartungsreleases, Client-Software und Veröffentlichungen für den Server stehen im IBM® Support Portal zur Verfügung.

 AIX-BetriebssystemeEinschränkung: Sie können den Server der Version 8.1.3 mit einigen Einschränkungen auf einem System installieren und ausführen, auf dem bereits DB2 installiert ist. Das gilt unabhängig davon, ob DB2 separat oder als Teil einer anderen Anwendung installiert wurde. Ausführliche Informationen finden Sie in dem Abschnitt über die Kompatibilität mit anderen DB2-Produkten.

Erfahrene DB2-Administratoren können erweiterte SQL-Abfragen durchführen und mithilfe von DB2-Tools die Datenbank überwachen. Sie dürfen die DB2-Tools jedoch nicht zur Änderung der von IBM Spectrum Protect vorgegebenen DB2-Konfigurationseinstellungen

verwenden oder die DB2-Umgebung für IBM Spectrum Protect auf andere Weise ändern (z. B. mit anderen Produkten). Der Server der Version 8.1.3 wurde mit der Datendefinitionssprache (DDL) und der vom Server implementierten Datenbankkonfiguration erstellt und ausführlich getestet.

Achtung: Sie dürfen die DB2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der DB2-Software und führen Sie kein Upgrade durch, da dies die Datenbank beschädigen kann.

## AIX: Planung für optimale Leistung

---

Überprüfen Sie vor der Installation des IBM Spectrum Protect-Servers die Merkmale und die Konfiguration des Systems, um sicherzustellen, dass der Server für die optimale Leistung konfiguriert ist.

### Vorgehensweise

---


1. Lesen Sie den Abschnitt AIX: Vorausgesetzte Kenntnisse.
2. Lesen Sie jeden der folgenden Unterabschnitte.
  - AIX: Planung für die Server-Hardware und das Betriebssystem  
Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
  - AIX: Planung für Platten für die Serverdatenbank  
Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
  - AIX: Planung für Platten für das Serverwiederherstellungsprotokoll  
Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
  - AIX: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools  
Überprüfen Sie die Konfiguration Ihrer Verzeichniscontainer- und Cloud-Containerspeicherpools, um eine optimale Leistung zu gewährleisten.
  - AIX: Planung für Speicherpools auf DISK- oder FILE-Einheiten  
Überprüfen Sie mithilfe der Prüfliste, wie Ihre Plattenspeicherpools konfiguriert sind. Diese Prüfliste umfasst Tipps für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden.
  - AIX: Planung für die Auswahl des korrekten Speichertechnologietyps  
Speichereinheiten haben eine unterschiedliche Kapazität und unterschiedliche Leistungsmerkmale. Diese Merkmale wirken sich darauf aus, welche Einheiten besser für die Verwendung mit IBM Spectrum Protect geeignet sind.
  - AIX: Bewährte Verfahren bei der Serverinstallation anwenden  
Normalerweise hat die Konfiguration und Auswahl der Hardware die deutlichsten Auswirkungen auf die Leistung einer IBM Spectrum Protect-Lösung. Weitere Faktoren, die sich auf die Leistung auswirken, sind die Auswahl und Konfiguration des Betriebssystems sowie die Konfiguration von IBM Spectrum Protect.

## AIX: Planung für die Server-Hardware und das Betriebssystem

---


Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

| Frage | Tasks, Merkmale, Optionen oder Einstellungen | Weitere Informationen |
|-------|--|-----------------------|
|-------|--|-----------------------|

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen   |
|---|---|---|
| <p>Werden die Betriebssystem- und Hardwarevoraussetzungen erfüllt oder mehr als erfüllt?</p> <ul style="list-style-type: none"> <li>• Anzahl und Geschwindigkeit der Prozessoren</li> <li>• Systemspeicher</li> <li>• Unterstützte Betriebssystemversion</li> </ul> | <p>Wenn Sie die erforderliche Mindestspeicherkapazität verwenden, können Sie eine minimale Arbeitslast unterstützen.</p> <p>Sie können versuchsweise mehr Systemspeicher hinzufügen, um bestimmen zu können, ob sich die Leistung verbessert. Entscheiden Sie dann, ob der Systemspeicher dem Server zugeordnet bleiben soll. Testen Sie die verschiedenen Speicherkapazitäten jeweils anhand des gesamten Tageszyklus der Serverlast.</p> <p>Wenn Sie mehrere Server auf dem System ausführen, addieren Sie die Voraussetzungen für jeden Server, um die Voraussetzungen für das System zu bestimmen.</p> <p> AIX-Betriebssysteme<br/>Einschränkung: Active Memory Expansion (AME) darf nicht verwendet werden. Bei Verwendung von AME verwendet die IBM DB2-Software 4-KB-Seiten anstelle von 64-KB-Seiten. Jede 4-KB-Seite muss dekomprimiert werden, wenn auf sie zugegriffen wird; wird sie nicht benötigt, muss sie komprimiert werden. Bei der Komprimierung und Dekomprimierung warten DB2 und der Server auf den Zugriff auf die Seite, wodurch sich die Serverleistung verschlechtert.</p> | <p>Überprüfen Sie die Betriebssystemvoraussetzungen in Technote 1243309.</p> <p>Lesen Sie außerdem die Anweisungen in Tasks für Betriebssysteme und andere Anwendungen optimieren.</p> <p>Weitere Informationen zu Voraussetzungen, wenn die entsprechenden Funktionen verwendet werden, finden Sie in den folgenden Abschnitten:</p> <ul style="list-style-type: none"> <li>• Prüfliste für Datenduplizierung</li> <li>• Prüfliste für Knotenreplikation</li> </ul> <p>Weitere Informationen zu Anforderungen in Bezug auf die Größe des Servers und des Speichers finden Sie im IBM Spectrum Protect-Blueprint.</p> |
| <p>Sind Platten für die optimale Leistung konfiguriert?</p>   | <p>Der Umfang der Optimierung, der für verschiedene Plattensysteme erfolgen kann, variiert. Stellen Sie sicher, dass die Warteschlangenlänge und andere Plattensystemoptionen entsprechend definiert sind.</p>  | <p>Weitere Informationen finden Sie in:</p> <ul style="list-style-type: none"> <li>• "Planung für Platten für die Serverdatenbank"</li> <li>• "Planung für Platten für das Serverwiederherstellungsprotokoll"</li> <li>• "Planung für Speicherpools auf DISK- oder FILE-Einheiten"</li> </ul>   |



| Frage   | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen   |
|---|--|---|
| <p>Verfügt der Server über genügend Speicher?</p>   | <p>Höhere Arbeitslasten und erweiterte Funktionen wie beispielsweise Datendeduplizierung und Knotenreplikation erfordern mehr Systemspeicher als den Mindestspeicher, der im Dokument mit den Systemvoraussetzungen angegeben ist. Verwenden Sie die folgenden Richtlinien, um den Speicherbedarf für Datenbanken anzugeben, die nicht für die Datendeduplizierung aktiviert sind:</p> <ul style="list-style-type: none"> <li>• Für Datenbanken mit einer Größe unter 500 GB benötigen Sie 16 GB Speicher.</li> <li>• Für Datenbanken mit einer Größe von 500 GB bis 1 TB benötigen Sie 24 GB Speicher.</li> <li>• Für Datenbanken mit einer Größe von 1 TB bis 1,5 TB benötigen Sie 32 GB Speicher.</li> <li>• Für Datenbanken mit einer Größe über 1,5 TB benötigen Sie 40 GB Speicher.</li> </ul> <p>Stellen Sie sicher, dass Sie für die Replikationsverarbeitung zusätzlichen Speicherbereich für die aktive Protokolldatei und das Archivprotokoll zuordnen.</p> | <p>Weitere Informationen zu Voraussetzungen, wenn die entsprechenden Funktionen verwendet werden, finden Sie in den folgenden Abschnitten:</p> <ul style="list-style-type: none"> <li>• Prüfliste für Datendeduplizierung</li> <li>• Prüfliste für Knotenreplikation</li> <li>• Speicherbedarf</li> </ul> |
| <p>Verfügt das System über genügend Hostbusadapter (HBAs), um die Datenoperationen, die der IBM Spectrum Protect-Server gleichzeitig ausführen muss, handhaben zu können?</p> | <p>Sie müssen wissen, für welche Operationen die gleichzeitige Verwendung von Hostbusadaptern erforderlich ist.</p> <p>Ein Server muss beispielsweise Sicherungsdaten mit 1 GB/s speichern, während er gleichzeitig eine Speicherpoolumlagerung ausführt, für deren Ausführung eine Kapazität von 0,5 GB/s erforderlich ist. Die Hostbusadapter müssen alle Daten mit der erforderlichen Geschwindigkeit handhaben können.</p>   | <p>Siehe HBA-Kapazität optimieren.</p>  |

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen  |
|--|---|--|
| Ist die Netzbandbreite größer als der geplante maximale Durchsatz für Sicherungen? | <p>Die Netzbandbreite muss dem System die Ausführung von Operationen wie Sicherungen innerhalb der zulässigen Zeit oder gemäß den vereinbarten Service-Levels ermöglichen.</p> <p>Bei der Knotenreplikation muss die Netzbandbreite größer als der geplante maximale Durchsatz sein.</p>  | <p>Weitere Informationen finden Sie in:</p> <ul style="list-style-type: none"> <li>• Netzleistung optimieren</li> <li>• Prüfliste für Knotenreplikation</li> </ul> |
| Verwenden Sie ein bevorzugtes Dateisystem für IBM Spectrum Protect-Serverdateien?  | <p>Verwenden Sie ein Dateisystem, das optimale Leistung und Datenverfügbarkeit gewährleistet. Der Server verwendet die direkte E/A mit Dateisystemen, die die Funktion unterstützen. Die Verwendung der direkten E/A kann den Durchsatz verbessern und die Prozessornutzung verringern. Weitere Informationen zum bevorzugten Dateisystem für Ihr Betriebssystem finden Sie in IBM Spectrum Protect server-supported file systems.</p>  | <p>Weitere Informationen finden Sie in Betriebssystem für die Plattenleistung konfigurieren.</p>   |
| Planen Sie, genügend Seitenauslagerungsbereich zu konfigurieren?                   | <p>Seitenauslagerungsbereich (oder Auslagerungsspeicher) erweitert den Speicher, der für die Verarbeitung verfügbar ist. Wenn der freie Arbeitsspeicher im System knapp wird, werden Programme oder Daten, die nicht im Gebrauch sind, aus dem Speicher in den Seitenauslagerungsbereich versetzt. Mit dieser Aktion wird Speicherbereich für andere Aktivitäten, wie z. B. Datenbankoperationen, freigegeben.</p> <p> AIX-Betriebssysteme<br/>Verwenden Sie den größeren der beiden folgenden Werte:<br/>mindestens 32 GB<br/>Seitenauslagerungsbereich<br/>oder 50 % des Arbeitsspeichers.</p> |  |

## AIX: Planung für Platten für die Serverdatenbank

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen   |
|---|--|---|
| <p>Befindet sich die Datenbank auf schnellen Platten mit kurzer Latenzzeit?</p>   | <p>Verwenden Sie die folgenden Laufwerke nicht für die IBM Spectrum Protect-Datenbank:</p> <ul style="list-style-type: none"> <li>• Nearline SAS (NL-SAS)</li> <li>• Serial Advanced Technology Attachment (SATA)</li> <li>• Parallel Advanced Technology Attachment (PATA)</li> </ul> <p>Verwenden Sie keine internen Platten, die standardmäßig Teil der Hardware der meisten Server ist.</p> <p>Enterprise-Solid-State-Laufwerke mit Fibre Channel- oder SAS-Schnittstellen bieten die beste Leistung.</p> <p>Wenn Sie planen, die Datendeduplizierungsfunktionen von IBM Spectrum Protect zu verwenden, legen Sie den Schwerpunkt auf die Plattenleistung (gemessen in E/A-Operationen pro Sekunde).</p> | <p>Weitere Informationen finden Sie in Prüfliste für Datendeduplizierung.</p>   |
| <p>Ist die Datenbank auf anderen Platten oder LUNs gespeichert als die aktive Protokolldatei, das Archivprotokoll und die Speicherpooldatenträger?</p>                      | <p>Das Trennen der Serverdatenbank von anderen Serverkomponenten trägt zur Reduktion von Konkurrenzsituationen für dieselben Ressourcen durch unterschiedliche Operationen, die gleichzeitig ausgeführt werden müssen, bei.</p> <p>Tipp: Die Datenbank und das Archivprotokoll können ein Array gemeinsam nutzen, wenn Sie die Solid-State-Laufwerk-Technologie (SSD-Technologie) verwenden.</p>   |   |
| <p>Wissen Sie bei Verwendung von RAID, wie die optimale RAID-Stufe für Ihr System ausgewählt wird? Definieren Sie alle LUNs mit derselben Größe und demselben RAID-Typ?</p> | <p>Wenn ein System viele Schreibvorgänge ausführen muss, ist die Leistung bei RAID 10 besser als bei RAID 5. RAID 10 benötigt jedoch mehr Platten als RAID 5, um dieselbe nutzbare Speichermenge bereitzustellen.</p> <p>Handelt es sich bei Ihrem Plattensystem um ein RAID-System, definieren Sie alle LUNs mit derselben Größe und demselben RAID-Typ. Verwenden Sie beispielsweise nicht gleichzeitig 4+1 RAID 5 mit 4+2 RAID 6.</p>   |   |
| <p>Planen Sie, wenn eine Option zum Definieren der Stripgröße oder der Segmentgröße verfügbar ist, die Größe beim Konfigurieren des Plattensystems zu optimieren?</p>       | <p>Wenn Sie die Stripgröße oder Segmentgröße definieren können, verwenden Sie auf Plattensystemen für die Datenbank Größen von 64 KB oder 128 KB.</p>  | <p>Die Blockgröße, die für die Datenbank verwendet wird, variiert abhängig vom Tabellenbereich. Die meisten Tabellenbereiche verwenden 8-KB-Blöcke; einige verwenden jedoch 32-KB-Blöcke.</p> |

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen   |
|---|---|---|
| <p>Planen Sie, mindestens vier Verzeichnisse, die auch als Speicherpfade bezeichnet werden, auf vier verschiedenen LUNs für die Datenbank zu erstellen?</p> <p>Erstellen Sie exakt ein Verzeichnis pro Array in dem Subsystem. Wenn weniger als drei Arrays vorhanden sind, erstellen Sie in jedem Array einen anderen LUN-Datenträger.</p> | <p>Für größere Arbeitslasten und bei Verwendung einiger Funktionen sind mehr Datenbankspeicherpfade als die Mindestvoraussetzungen erforderlich.</p> <p>Serveroperationen wie die Datenduplizierung verursachen eine hohe Anzahl Ein-/Ausgabeoperationen pro Sekunde (IOPS) für die Datenbank. Die Leistung derartiger Operationen ist besser, wenn die Datenbank über mehr Verzeichnisse verfügt.</p> <p>Verwenden Sie für Serverdatenbanken, die größer als 2 TB sind oder die wahrscheinlich auf diese Größe anwachsen, acht Verzeichnisse.</p> <p>Berücksichtigen Sie das geplante Wachstum des Systems bei der Bestimmung der Anzahl zu erstellender Speicherpfade. Die höhere Anzahl Speicherpfade wird vom Server effizienter genutzt, wenn die Speicherpfade bei der Ersterstellung des Servers bereits vorhanden sind.</p> <p>Verwenden Sie die Variable <i>DB2_PARALLEL_IO</i>, um die parallele E/A für Tabellenbereiche mit einem einzelnen Container zu erzwingen oder für Tabellenbereiche, die über Container auf mehr als einer physischen Platte verfügen. Wenn Sie die Variable <i>DB2_PARALLEL_IO</i> nicht definieren, entspricht die E/A-Parallelität der Anzahl Container, die von dem Tabellenbereich verwendet werden. Wenn ein Tabellenbereich beispielsweise vier Container umfasst, beträgt der verwendete Grad an E/A-Parallelität 4.</p> | <p>Weitere Informationen finden Sie in:</p> <ul style="list-style-type: none"> <li>• Prüfliste für Datenduplizierung</li> <li>• Prüfliste für Knotenreplikation</li> </ul> <p>Hilfreiche Informationen zur Vorhersage des Wachstums beim Duplizieren von Daten durch den Server finden Sie in Technote 1596944.</p> <p>Aktuelle Informationen zur Datenbankgröße, zur Datenbankreorganisation und zu Leistungsaspekten für IBM Spectrum Protect-Server finden Sie in Technote 1683633.</p> <p>Informationen zum Definieren der Variable <i>DB2_PARALLEL_IO</i> finden Sie in Empfohlene Einstellungen für IBM DB2-Registry-Variablen.</p> |
| <p>Haben alle Verzeichnisse für die Datenbank dieselbe Größe?</p>   | <p>Verzeichnisse, die alle dieselbe Größe haben, stellen einen konsistenten Grad an Parallelität für Datenbankoperationen sicher. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als andere sind, verringert sich dadurch das Potenzial für den optimierten parallelen Vorabesezugriff.</p> <p>Diese Richtlinie gilt auch, wenn Sie nach der Erstkonfiguration des Servers Speicherpfade hinzufügen müssen.</p>  |   |
| <p>Planen Sie, die Warteschlangenlänge der Datenbank-LUNs auf AIX-Systemen zu erhöhen?</p>  | <p>Die Standardwarteschlangenlänge ist häufig zu niedrig definiert.</p>   | <p>Siehe AIX-Systeme für die Plattenleistung konfigurieren.</p>   |

## AIX: Planung für Platten für das Serverwiederherstellungsprotokoll

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen  |
|---|---|--|
| Sind die aktive Protokolldatei und das Archivprotokoll auf anderen Platten oder LUNs gespeichert als die Datenbank und die Speicherpooldatenträger? | Stellen Sie sicher, dass die Platten, auf die die aktive Protokolldatei gestellt wird, auf dem Server oder System nicht für andere Zwecke verwendet werden. Stellen Sie die aktive Protokolldatei nicht auf Platten, die die Serverdatenbank, das Archivprotokoll oder Systemdateien, wie Seitenauslagerungsbereich oder Auslagerungsspeicher, enthalten.   | Das Trennen der Serverdatenbank von der aktiven Protokolldatei und dem Archivprotokoll trägt zur Reduktion von Konkurrenzsituationen für dieselben Ressourcen durch unterschiedliche Operationen, die gleichzeitig ausgeführt werden müssen, bei.  |
| Befinden sich die Protokolle auf Platten mit nicht flüchtigem Schreibcache?   | Nicht flüchtiger Schreibcache ermöglicht es, Daten so schnell wie möglich in die Protokolle zu schreiben. Schnellere Schreiboperationen für die Protokolle können die Leistung für Serveroperationen verbessern.  |  |
| Legen Sie für die Protokolle eine Größe fest, die der Arbeitslast entspricht?   | Wenn Sie sich über die Arbeitslast im Unklaren sind, verwenden Sie die größtmögliche Größe.<br><br>Aktive Protokolldatei<br>Die maximale Größe beträgt 512 GB; sie wird über die Serveroption ACTIVELOGSIZE festgelegt.<br><br>Stellen Sie sicher, dass mindestens 8 GB freier Speicherbereich im Dateisystem für aktive Protokolldateien verfügbar sind, nachdem die aktiven Protokolldateien mit fester Größe erstellt wurden.<br><br>Archivprotokoll<br>Die Größe des Archivprotokolls wird durch die Größe des Dateisystems begrenzt, in dem es sich befindet, und nicht durch eine Serveroption. Das Archivprotokoll muss mindestens so groß wie die aktive Protokolldatei sein. | <ul style="list-style-type: none"> <li>• Ausführliche Informationen zur Festlegung der Protokollgröße enthalten die Informationen zum Wiederherstellungsprotokoll in Technote 1421060.</li> <li>• Informationen zur Festlegung der Größe bei Verwendung der Datendeduplizierung finden Sie in Prüfliste für Datendeduplizierung.</li> </ul>            |
| Definieren Sie ein Archivübernahmeprotokoll? Stellen Sie dieses Protokoll auf eine andere Platte als das Archivprotokoll?                           | Das Archivübernahmeprotokoll dient der Verwendung durch den Server im Notfall, wenn das Archivprotokoll voll ist. Für das Archivübernahmeprotokoll können langsamere Platten verwendet werden.  | Geben Sie die Position des Archivübernahmeprotokolls mithilfe der Serveroption ARCHFAILOVERLOGDIRECTORY an.<br><br>Überwachen Sie die Belegung des Verzeichnisses für das Archivübernahmeprotokoll. Wenn das Archivübernahmeprotokoll vom Server verwendet werden muss, ist der Speicherplatz für das Archivprotokoll möglicherweise nicht groß genug. |
| Verwenden Sie, wenn Sie die aktive Protokolldatei spiegeln, nur einen einzigen Typ von Spiegelung?  | Sie können das Protokoll mithilfe einer der folgenden Methoden spiegeln. Verwenden Sie für das Protokoll nur einen einzigen Typ von Spiegelung. <ul style="list-style-type: none"> <li>• Verwenden Sie die Option MIRRORLOGDIRECTORY, die für den IBM Spectrum Protect-Server verfügbar ist, um eine Position für die Spiegelung anzugeben.</li> <li>• Verwenden Sie die Softwarespiegelung, wie z. B. Logical Volume Manager (LVM) unter AIX.</li> <li>• Verwenden Sie die Spiegelung in der Hardware des Plattensystems.</li> </ul>   | Stellen Sie, wenn Sie die aktive Protokolldatei spiegeln, sicher, dass die Platten für die aktive Protokolldatei und die Spiegelkopie dieselbe Geschwindigkeit und Zuverlässigkeit haben.<br><br>Weitere Informationen finden Sie in Wiederherstellungsprotokoll konfigurieren und optimieren.   |

## AIX: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools

Überprüfen Sie die Konfiguration Ihrer Verzeichniscontainer- und Cloud-Containerspeicherpools, um eine optimale Leistung zu gewährleisten.

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen   |
|--|--|---|
| <p>Verwenden Sie, gemessen in Anzahl Ein-/Ausgabeoperationen pro Sekunde (IOPS), schnellen Plattenspeicher für die IBM Spectrum Protect-Datenbank?</p> | <p>Verwenden Sie eine Hochleistungsplatte für die Datenbank. Verwenden Sie die Solid-State-Laufwerk-Technologie (SSD-Technologie) für die Datendeduplizierungsverarbeitung.</p> <p>Stellen Sie sicher, dass die Datenbank über eine Mindestkapazität von 3000 E/A-Operationen pro Sekunde (IOPS) verfügt. Addieren Sie zu diesem Mindestwert pro TB Daten, die täglich (vor der Datendeduplizierung) gesichert werden, 1000 E/A-Operationen pro Sekunde.</p> <p>Beispielsweise würde ein IBM Spectrum Protect-Server, der täglich 3 TB Daten aufnimmt, 6000 E/A-Operationen pro Sekunde (IOPS) für die Datenbankplatten benötigen:</p> $\text{mindestens } 3000 \text{ IOPS} + 3000 (3 \text{ TB} \times 1000 \text{ IOPS}) = 6000 \text{ IOPS}$   | <p>Empfehlungen zur Plattenauswahl finden Sie in "Planung für Platten für die Serverdatenbank".</p> <p>Weitere Informationen zu IOPS finden Sie in den IBM Spectrum Protect-Blueprints.</p> |
| <p>Ist genügend Speicherplatz für die Größe Ihrer Datenbank vorhanden?</p>   | <p>Verwenden Sie mindestens 40 GB Systemspeicher für IBM Spectrum Protect-Server, die Daten deduplizieren, mit einer Datenbankgröße von 100 GB. Wenn die Speicherkapazität für Sicherungsdaten wächst, ist unter Umständen ein höherer Speicherbedarf erforderlich.</p> <p>Überwachen Sie regelmäßig die Speicherbelegung, um festzustellen, ob mehr Speicherplatz erforderlich ist.</p> <p>Verwenden Sie weiteren Systemspeicher, um das Caching von Datenbankseiten zu verbessern. Die folgenden Richtlinien für die Speichergröße basieren auf dem Volumen an neuen Daten, das jeden Tag gesichert wird:</p> <ul style="list-style-type: none"> <li>• 128 GB Systemspeicher für tägliche Sicherungen von Daten, wobei die Datenbankgröße zwischen 1 und 2 TB liegt</li> <li>• 192 GB Systemspeicher für tägliche Sicherungen von Daten, wobei die Datenbankgröße zwischen 2 und 4 TB liegt</li> </ul> | <p>Speicherbedarf</p>   |

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen   |
|---|--|---|
| <p>Haben Sie die Speicherkapazität für die die aktive Protokolldatei und das Archivprotokoll der Datenbank korrekt festgelegt?</p>  | <p>Geben Sie in der Konfiguration des Servers eine minimale Größe von 128 GB für die aktive Protokolldatei an, indem Sie die Serveroption ACTIVELOGSIZE auf den Wert 131072 setzen.</p> <p>Als Anfangsgröße für das Archivprotokoll wird eine Größe von 1 TB vorgeschlagen. Die Größe des Archivprotokolls wird durch die Größe des Dateisystems begrenzt, in dem es sich befindet, und nicht durch eine Serveroption. Stellen Sie sicher, dass im Vergleich zur Größe des Archivprotokolls mindestens 10 % zusätzlicher Plattenspeicher für das Dateisystem vorhanden sind.</p> <p>Verwenden Sie für die Datenbankarchivprotokolle ein Verzeichnis mit einer anfänglichen freien Kapazität von mindestens 1 TB. Geben Sie das Verzeichnis mithilfe der Serveroption ARCHLOGDIRECTORY an.</p> <p>Definieren Sie Speicherbereich für das Archivübernahmeprotokoll mithilfe der Serveroption ARCHFAILOVERLOGDIRECTORY.</p> | <p>Weitere Informationen zur Kapazitätsermittlung für Ihr System finden Sie in den IBM Spectrum Protect-Blueprints.</p>   |
| <p>Ist die Komprimierung für die Archivprotokoll- und Datenbanksicherungen aktiviert?</p>   | <p>Aktivieren Sie die Serveroption ARCHLOGCOMPRESS, um Speicherbereich einzusparen.</p> <p>Diese Komprimierungsoption unterscheidet sich von der Inline-Komprimierung. Die Inline-Komprimierung ist ab IBM Spectrum Protect Version 7.1.5 und höher standardmäßig aktiviert.</p> <p>Einschränkung: Sie dürfen diese Option nicht verwenden, wenn das Volumen der pro Tag gesicherten Daten 6 TB überschreitet.</p>   | <p>Weitere Informationen zur Komprimierung für Ihr System finden Sie in den IBM Spectrum Protect-Blueprints.</p>  |
| <p>Befinden sich die Datenbank und Protokolle von IBM Spectrum Protect auf separaten Plattendatenträgern (LUNs)?</p> <p>Ist der Datenträger, der für die Datenbank verwendet wird, gemäß den bewährten Verfahren für eine transaktionsorientierte Datenbank konfiguriert?</p> | <p>Die Datenbank darf keine Plattendatenträger mit IBM Spectrum Protect-Datenbankprotokollen oder -Speicherpools oder mit einer anderen Anwendung oder einem anderen Dateisystem gemeinsam nutzen.</p>   | <p>Weitere Informationen zur Konfiguration der Serverdatenbank und des Wiederherstellungsprotokolls finden Sie in Konfiguration und Optimierung der Serverdatenbank und des Wiederherstellungsprotokolls.</p> |
| <p>Verwenden Sie mindestens acht Prozessorkerne (2,2-GHz-Prozessorkerne oder entsprechende Prozessorkerne) für jeden IBM Spectrum Protect-Server, der mit Datendeduplizierung verwendet werden soll?</p>  | <p>Wenn die clientseitige Datendeduplizierung verwendet werden soll, müssen Sie sicherstellen, dass für Clientsysteme während einer Sicherungsoperation genügend Ressourcen zur Ausführung der Datendeduplizierungsverarbeitung verfügbar sind. Verwenden Sie pro Sicherungsprozess mit clientseitiger Datendeduplizierung einen Prozessor, der mindestens einem 2,2-GHz-Prozessorkern entspricht.</p>   | <ul style="list-style-type: none"> <li>• Effektive Planung und Verwendung der Deduplizierung</li> <li>• IBM Spectrum Protect Blueprints</li> </ul>  |

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen   |
|--|---|---|
| <p>Haben Sie genügend Speicherplatz für die Datenbank zugeordnet?</p>  | <p>Als grobe Schätzung sollten Sie 100 GB Datenbankspeicher für jeweils 50 TB Daten einplanen, die in deduplizierten Speicherpools geschützt werden sollen. <i>Geschützte Daten</i> ist das Datenvolumen vor der Dateneduplizierung, einschließlich aller Versionen gespeicherter Objekte.</p> <p>Als bewährtes Verfahren sollten Sie einen neuen Containerspeicherpool ausschließlich für die Dateneduplizierung definieren. Die Dateneduplizierung erfolgt auf der Speicherpoolebene; mit Ausnahme von verschlüsselten Daten werden alle Daten in einem Speicherpool dedupliziert.</p>  |   |
| <p>Haben Sie die Speicherpoolkapazität geschätzt, um genügend Speicherplatz für die Größe Ihrer Umgebung zu konfigurieren?</p> | <p>Sie können den Kapazitätsbedarf für einen deduplizierten Speicherpool wie folgt schätzen:</p> <ol style="list-style-type: none"> <li>1. Schätzen Sie die Basisgröße der Quelldaten.</li> <li>2. Schätzen Sie die Größe der täglichen Sicherung anhand einer geschätzten Änderungs- und Wachstumsrate.</li> <li>3. Bestimmen Sie die Anforderungen in Bezug auf die Aufbewahrungsdauer.</li> <li>4. Schätzen Sie das Gesamtvolumen an Quelldaten unter Berücksichtigung der Basisgröße, der Größe der täglichen Sicherung und der Anforderungen in Bezug auf die Aufbewahrungsdauer.</li> <li>5. Wenden Sie den Faktor für das Deduplizierungsverhältnis an.</li> <li>6. Wenden Sie den Faktor für das Komprimierungsverhältnis an.</li> <li>7. Runden Sie die Schätzung auf, um die Nutzung transienter Speicherpools zu berücksichtigen.</li> </ol> | <p>Ein Beispiel zur Verwendung dieses Verfahrens finden Sie in Effektive Planung und Verwendung der Deduplizierung.</p> |



| Frage  | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen  |
|--|--|--|
| Haben Sie die Platten-E/A auf viele Platteneinheiten und Controller verteilt?    | <p>Verwenden Sie Arrays, die aus so vielen Platten wie möglich bestehen; dies wird auch als "Wide-Striping" bezeichnet. Stellen Sie sicher, dass Sie exakt ein Datenbankverzeichnis pro Array in dem Subsystem verwenden.</p> <p>Definieren Sie die Registry-Variable <i>DB2_PARALLEL_IO</i>, um die parallele E/A für jeden verwendeten Tabellenbereich zu aktivieren, wenn sich die Container in dem Tabellenbereich über mehrere physische Platten erstrecken.</p> <p>Wenn E/A-Bandbreite verfügbar ist und die Dateien groß sind (beispielsweise 1 MB), kann der Prozess zur Suche nach Duplikaten die Ressourcen eines gesamten Prozessors in Anspruch nehmen. Wenn Dateien kleiner sind, können andere Engpässe auftreten.</p> <p>Geben Sie acht oder mehr Dateisysteme für die Einheitenklasse des deduplizierten Speicherpools an, damit die Ein-/Ausgabe auf so viele LUNs und physische Einheiten wie möglich verteilt wird.</p> | <p>Richtlinien zur Konfiguration von Speicherpools finden Sie in "Planung für Speicherpools auf DISK- oder FILE-Einheiten".</p> <p>Informationen zum Definieren der Variable <i>DB2_PARALLEL_IO</i> finden Sie in Empfohlene Einstellungen für IBM DB2-Registry-Variablen.</p> |
| Haben Sie tägliche Operationen auf der Basis Ihrer Sicherheitsstrategie geplant? | <p>Die Operationsfolge sieht gemäß den bewährten Verfahren wie folgt aus:</p> <ol style="list-style-type: none"> <li>1. Clientsicherung</li> <li>2. Speicherpoolschutz</li> <li>3. Knotenreplikation</li> <li>4. Datenbanksicherung</li> <li>5. Bestandsverfall</li> </ol>   | <ul style="list-style-type: none"> <li>• Datendeduplizierungs- und Knotenreplikationsprozesse planen</li> <li>• Tägliche Operation für Verzeichniscontainerspeicherpools</li> </ul>  |
| Ist genügend Speicher zur Verwaltung der DB2-Sperrenliste vorhanden?             | <p>Wenn Sie Daten deduplizieren, die große Dateien oder gleichzeitig eine große Anzahl Dateien umfassen, kann der Prozess zur Speicherknappheit führen. Wenn der Sperrenlistenspeicher nicht ausreichend ist, können Sicherheitsfehler, Datenverwaltungsprozessfehler oder Serverausfälle auftreten.</p> <p>Bei Dateigrößen über 500 GB, die durch die Datendeduplizierung verarbeitet werden, ist es sehr wahrscheinlich, dass der Speicherplatz knapp wird. Wenn jedoch viele Sicherungsoperationen die clientseitige Datendeduplizierung verwenden, kann dieses Problem auch bei Dateien mit geringerer Größe auftreten.</p>  | <p>Informationen zur Optimierung des DB2-Parameters LOCKLIST finden Sie in Serverseitige Datendeduplizierung optimieren.</p>   |

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen  |
|--|--|--|
| Ist genügend Bandbreite verfügbar, um Daten auf einen IBM Spectrum Protect-Server zu übertragen?       | <p>Um Daten auf einen IBM Spectrum Protect-Server zu übertragen, verwenden Sie die clientseitige oder serverseitige Datenduplizierung und die Komprimierung, um die erforderliche Bandbreite zu verringern.</p> <p>Verwenden Sie einen Server der Version 7.1.5 oder höher, um die Inline-Komprimierung verwenden zu können, und einen Client der Version 7.1.6 oder höher, um die erweiterte Komprimierungsverarbeitung zu aktivieren.</p>  | Weitere Informationen finden Sie in der Beschreibung der Clientoption <code>enablededup</code> . |
| Haben Sie festgelegt, wie viele Speicherpoolverzeichnisse jedem Speicherpool zugeordnet werden sollen? | <p>Ordnen Sie Verzeichnisse einem Speicherpool mithilfe des Befehls <code>DEFINE STGPOOLDIRECTORY</code> zu.</p> <p>Erstellen Sie mehrere Speicherpoolverzeichnisse und stellen Sie sicher, dass jedes Verzeichnis auf einem anderen Plattendatenträger (LUN) gesichert wird.</p>  |  |
| Haben Sie genügend Plattenspeicherplatz in dem Cloud-Containerspeicherpool zugeordnet?                 | <p>Um Sicherungsfehler zu verhindern, stellen Sie sicher, dass das lokale Verzeichnis über genügend Speicherplatz verfügt. Verwenden Sie die folgende Liste als Leitfaden für optimalen Plattenspeicherplatz:</p> <ul style="list-style-type: none"> <li>• Berechnen Sie für SAS-Platten (SAS = Serial-Attached SCSI) und rotierende Platten das Volumen neuer Daten, das nach der täglichen Datenreduktion (Komprimierung und Datenduplizierung) erwartet wird. Ordnen Sie bis zu 100 Prozent dieses Volumens (in Terabyte) für den Plattenspeicherplatz zu.</li> <li>• Stellen Sie 3 TB für flash-basierte Speichersysteme mit schnellen Netzverbindungen zu leistungsfähigen On-Premises-Cloudsystemen bereit.</li> <li>• Stellen Sie 5 TB für Systeme mit Solid-State-Laufwerk (SSD) mit schnellen Netzverbindungen zu leistungsfähigen Cloudsystemen bereit.</li> </ul> |  |

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen |
|---|---|-----------------------|
| <p>Haben Sie den geeigneten Typ des lokalen Speichers ausgewählt?</p> | <p>Stellen Sie sicher, dass Datenübertragungen aus dem lokalen Speicher in die Cloud beendet werden, bevor der nächste Sicherungszyklus beginnt.</p> <p>Tipp: Daten werden kurz nach dem Versetzen in die Cloud aus dem lokalen Speicher entfernt.</p> <p>Verwenden Sie die folgenden Richtlinien:</p> <ul style="list-style-type: none"> <li>• Verwenden Sie Flash- oder SSD-Speicher für große Systeme, die über leistungsfähige Cloudsysteme verfügen. Stellen Sie sicher, dass Sie über eine dedizierte 10-GB-WAN-Verbindung mit einer Hochgeschwindigkeitsverbindung zum Objektspeicher verfügen. Verwenden Sie beispielsweise Flash- oder SSD-Speicher, wenn Sie über eine dedizierte 10-GB-WAN-Verbindung sowie eine Hochgeschwindigkeitsverbindung zu einem IBM® Cloud Object Storage-Speicherort oder zu einem Amazon S3-Datencenter (Amazon S3 = Amazon Simple Storage Service) verfügen.</li> <li>• Verwenden Sie SAS-Platten mit 15000 U/min mit größerer Kapazität für die folgenden Szenarios: <ul style="list-style-type: none"> <li>◦ Systeme mittlerer Größe</li> <li>◦ Langsamere Cloudverbindungen, z. B. 1 GB</li> <li>◦ Bei Verwendung von IBM Cloud Object Storage als Service-Provider in mehreren Regionen</li> </ul> </li> <li>• Berechnen Sie für SAS-Platten oder rotierende Platten das Volumen neuer Daten, das nach der täglichen Datenreduktion (Komprimierung und Datendeduplizierung) erwartet wird. Ordnen Sie bis zu 100 Prozent dieses Volumens (in Terabyte) für den Plattenspeicherplatz zu.</li> </ul> |                       |

## AIX: Planung für Speicherpools auf DISK- oder FILE-Einheiten

Überprüfen Sie mithilfe der Prüfliste, wie Ihre Plattenspeicherpools konfiguriert sind. Diese Prüfliste umfasst Tipps für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden.

| Frage | Tasks, Merkmale, Optionen oder Einstellungen | Weitere Informationen |
|-------|--|-----------------------|
|-------|--|-----------------------|

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen  |
|---|--|--|
| <p>Können die Speicherpool-LUNs Durchsatzraten von 256 KB für sequenzielle Lese- und Schreibvorgänge aufrechterhalten, um die Arbeitslast innerhalb der Zeitvorgaben adäquat handhaben zu können?</p> | <p>Bei der Planung für Spitzenbelastungen müssen Sie alle Daten berücksichtigen, die der Server gleichzeitig aus Plattenspeicherpools lesen oder in Plattenspeicherpools schreiben soll. Berücksichtigen Sie beispielsweise den Spitzenwert für den Datenfluss bei Clientsicherungsoperationen und Serverdatenversetzungsoperationen, wie z. B. Umlagerung, die gleichzeitig ausgeführt werden.</p> <p>Der IBM Spectrum Protect-Server verwendet beim Lesen aus Speicherpools und Schreiben in Speicherpools in erster Linie 256-KB-Blöcke.</p> <p>Wenn das Plattensystem über die entsprechende Funktionalität verfügt, konfigurieren Sie das Plattensystem für die optimale Leistung mit sequenziellen Lese-/Schreiboperationen statt mit wahlfreien Lese-/Schreiboperationen.</p> | <p>Weitere Informationen finden Sie in Basisleistung von Plattensystemen analysieren.</p>  |
| <p>Ist die Platte für die Verwendung von Lese- und Schreibcache konfiguriert?</p>   | <p>Verwenden Sie mehr Cache, um eine bessere Leistung zu erzielen.</p>   |  |
| <p>Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, eine geeignete Größe für die Speicherpooldatenträger festgelegt?</p>  | <p>Lesen Sie die Informationen in Optimale Anzahl und Größe von Datenträgern für Speicherpools, die Platten verwenden. Wenn Sie nicht über die nötigen Informationen zum Schätzen der Größe für Datenträger mit der Einheitenklasse FILE verfügen, beginnen Sie mit einer Datenträgergröße von 50 GB.</p>  | <p>In der Regel treten häufiger Probleme auf, wenn die Datenträger zu klein sind. Wenn Datenträger größer als erforderlich sind, treten nur selten Probleme auf. Wenn Sie die zu verwendende Datenträgergröße festlegen, sollten Sie als Vorsichtsmaßnahme eine größere Größe als erforderlich wählen.</p> |
| <p>Verwenden Sie für Speicherpools, die die Einheitenklasse FILE verwenden, vorab zugeordnete Datenträger?</p>  | <p>Arbeitsdatenträger können eine Dateifragmentierung zur Folge haben.</p> <p>Um sicherzustellen, dass für einen Speicherpool immer genügend Datenträger verfügbar sind, setzen Sie den Parameter MAXSCRATCH auf einen Wert größer als null.</p>   | <p>Ordnen Sie mithilfe des Befehls DEFINE VOLUME Datenträger in dem Speicherpool vorab zu.</p> <p>Verwenden Sie den Serverbefehl DEFINE STGPOOL oder UPDATE STGPOOL, um den Parameter MAXSCRATCH zu definieren.</p>  |
| <p>Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, die maximale Anzahl Clientsitzungen mit der Anzahl definierter Datenträger verglichen?</p>                                    | <p>Es müssen immer genügend verwendbare Datenträger in den Speicherpools vorhanden sein, um die erwartete maximale Anzahl gleichzeitig ausgeführter Clientsitzungen handhaben zu können. Bei den Datenträgern kann es sich um Arbeitsdatenträger, leere Datenträger oder teilweise gefüllte Datenträger handeln.</p>   | <p>Bei Speicherpools, die die Einheitenklasse FILE verwenden, kann jeweils nur eine einzige Sitzung oder ein einziger Prozess auf einen Datenträger schreiben.</p>   |

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen  |
|--|---|--|
| Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, den Parameter MOUNTLIMIT für die Einheitenklasse auf einen Wert gesetzt, der für die Anzahl Datenträger, die parallel angehängt werden könnten, ausreichend hoch ist? | <p>Für Speicherpools, die die Datenduplizierung verwenden, liegt der Wert für den Parameter MOUNTLIMIT in der Regel zwischen 500 und 1000. Setzen Sie den Wert für MOUNTLIMIT auf die maximale Anzahl Mountpunkte, die für alle aktiven Sitzungen erforderlich sind. Berücksichtigen Sie Parameter, die sich auf die maximale Anzahl erforderlicher Mountpunkte auswirken:</p> <ul style="list-style-type: none"> <li>Die Serveroption MAXSESSIONS, die die maximal zulässige Anzahl gleichzeitig ablaufender IBM Spectrum Protect-Sitzungen angibt</li> <li>Der Parameter MAXNUMMP, der die maximale Anzahl Mountpunkte definiert, die jeder Clientknoten verwenden kann</li> </ul> <p>Wenn beispielsweise die maximalen Anzahl Sicherungssitzungen für Clientknoten normalerweise 100 ist und für jeden der Knoten MAXNUMMP=2 definiert ist, multiplizieren Sie 100 Knoten mit 2 Mountpunkten für jeden Knoten, um den Wert 200 für den Parameter MOUNTLIMIT zu erhalten.</p> | Verwenden Sie den Serverbefehl REGISTER NODE oder UPDATE NODE, um den Parameter MAXNUMMP für Clientknoten zu definieren.   |
| Haben Sie für Speicherpools, die die Einheitenklasse DISK verwenden, festgelegt, wie viele Speicherpooldatenträger in jedes Dateisystem gestellt werden sollen?  | <p>Die Konfiguration des Speichers für einen Speicherpool, der eine Einheitenklasse DISK verwendet, ist davon abhängig, ob Sie RAID für das Plattensystem verwenden.</p> <p>Wenn Sie RAID nicht verwenden, konfigurieren Sie ein einziges Dateisystem pro physischer Platte und definieren Sie exakt einen Speicherpooldatenträger für jedes Dateisystem.</p> <p>Wenn Sie RAID 5 mit <math>n + 1</math> Datenträgern verwenden, konfigurieren Sie den Speicher auf eine der folgenden Arten:</p> <ul style="list-style-type: none"> <li>Konfigurieren Sie <math>n</math> Dateisysteme auf der LUN und definieren Sie exakt einen Speicherpooldatenträger pro Dateisystem.</li> <li>Konfigurieren Sie ein einziges Dateisystem und <math>n</math> Speicherpooldatenträger für die LUN.</li> </ul>  | Ein Beispiellayout, bei dem diese Richtlinie eingehalten wird, zeigt Beispiellayout für Serverspeicherpools.   |
| Haben Sie Ihre Speicherpools für die Verteilung der Ein-/Ausgabe auf mehrere Dateisysteme erstellt?  | <p>Stellen Sie sicher, dass sich jedes Dateisystem auf einer anderen LUN auf dem Plattensystem befindet.</p> <p>Normalerweise sind 10-30 Dateisysteme ein geeigneter Wert, Sie müssen jedoch sicherstellen, dass die Dateisysteme nicht kleiner als etwa 250 GB sind.</p>   | <p>Ausführliche Informationen finden Sie in:</p> <ul style="list-style-type: none"> <li>Plattenspeicher für den Server optimieren</li> <li>Speicherpools und Datenträger optimieren und konfigurieren</li> </ul> |

## AIX: Planung für die Auswahl des korrekten Speichertechnologietyps

Speichereinheiten haben eine unterschiedliche Kapazität und unterschiedliche Leistungsmerkmale. Diese Merkmale wirken sich darauf aus, welche Einheiten besser für die Verwendung mit IBM Spectrum Protect geeignet sind.

### Vorgehensweise

Die folgende Tabelle unterstützt Sie bei der Auswahl des korrekten Speichertechnologietyps für die Speicherressourcen, die der Server erfordert.

Tabelle 1. Speichertechnologietypen für IBM Spectrum Protect-Speicherbedarf

| <b>Speichertechnologietyp</b>  | <b>Datenbank</b>   | <b>Aktive Protokolldatei</b>  | <b>Archivprotokoll und Archivübernahmeprotokoll</b>  | <b>Speicherpools</b>   |
|--|--|---|--|--|
| <b>Solid-State-Laufwerk (SSD)</b>  | <p>Stellen Sie die Datenbank auf ein Solid-State-Laufwerk, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Sie verwenden die IBM Spectrum Protect-Dateneduplizierung.</li> <li>• Sie sichern täglich mehr als 8 TB neuer Daten.</li> </ul>   | <p>Wenn Sie die IBM Spectrum Protect-Datenbank auf ein Solid-State-Laufwerk stellen (dies ist das bewährte Verfahren), stellen Sie auch die aktive Protokolldatei auf ein Solid-State-Laufwerk. Wenn kein Speicherplatz verfügbar ist, verwenden Sie stattdessen eine Hochleistungsplatte.</p>  | <p>Reservieren Sie die Solid-State-Laufwerke für die Verwendung mit der Datenbank und der aktiven Protokolldatei. Das Archivprotokoll und die Archivübernahmeprotokolle können auf langsamere Speichertechnologietypen gestellt werden.</p>                          | <p>Reservieren Sie die Solid-State-Laufwerke für die Verwendung mit der Datenbank und der aktiven Protokolldatei. Speicherpools können auf langsamere Speichertechnologietypen gestellt werden.</p>  |
| <p><b>Hochleistungsplatte mit den folgenden Kenndaten:</b></p> <ul style="list-style-type: none"> <li>• <b>Platte mit 15.000 U/min</b></li> <li>• <b>Fibre Channel - oder Serial-attache d SCSI-Schnittstelle (SAS-Schnittstelle)</b></li> </ul> | <p>Verwenden Sie Hochleistungsplatten, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Der Server führt keine Dateneduplizierung aus.</li> <li>• Der Server führt keine Knotenreplikation aus.</li> </ul> <p>Trennen Sie die Serverdatenbank von den zugehörigen Protokollen und Speicherpools sowie von Daten für andere Anwendungen.</p> | <p>Verwenden Sie Hochleistungsplatten, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Der Server führt keine Dateneduplizierung aus.</li> <li>• Der Server führt keine Knotenreplikation aus.</li> </ul> <p>Trennen Sie aus Gründen der Leistung und Verfügbarkeit die aktive Protokolldatei von der Serverdatenbank, den Archivprotokollen und den Speicherpools.</p> | <p>Sie können Hochleistungsplatten für das Archivprotokoll und die Archivübernahmeprotokolle verwenden. Trennen Sie aus Gründen der Verfügbarkeit diese Protokolle von der Datenbank und der aktiven Protokolldatei.</p>   | <p>Verwenden Sie Hochleistungsplatten für Speicherpools, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Daten werden häufig gelesen.</li> <li>• Daten werden häufig geschrieben.</li> </ul> <p>Trennen Sie aus Gründen der Leistung und Verfügbarkeit die Speicherpooldaten von der Serverdatenbank und den Protokollen sowie von Daten für andere Anwendungen.</p>   |
| <p><b>Platte mit mittlerer Leistung oder Hochleistungsplatte mit den folgenden Kenndaten:</b></p> <ul style="list-style-type: none"> <li>• <b>Platte mit 10.000 U/min</b></li> <li>• <b>Fibre Channel - oder SAS-Schnittstelle</b></li> </ul>    | <p>Wenn das Plattensystem eine Kombination verschiedener Plattentechnologien verwendet, verwenden Sie die schnelleren Platten für die Datenbank und die aktive Protokolldatei. Trennen Sie die Serverdatenbank von den zugehörigen Protokollen und Speicherpools sowie von Daten für andere Anwendungen.</p>   | <p>Wenn das Plattensystem eine Kombination verschiedener Plattentechnologien verwendet, verwenden Sie die schnelleren Platten für die Datenbank und die aktive Protokolldatei. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die aktive Protokolldatei von der Serverdatenbank, den Archivprotokollen und den Speicherpools.</p>   | <p>Sie können eine Platte mit mittlerer Leistung oder eine Hochleistungsplatte für das Archivprotokoll und die Archivübernahmeprotokolle verwenden. Trennen Sie aus Gründen der Verfügbarkeit diese Protokolle von der Datenbank und der aktiven Protokolldatei.</p> | <p>Verwenden Sie eine Platte mit mittlerer Leistung oder eine Hochleistungsplatte für Speicherpools, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Daten werden häufig gelesen.</li> <li>• Daten werden häufig geschrieben.</li> </ul> <p>Trennen Sie aus Gründen der Leistung und Verfügbarkeit die Speicherpooldaten von der Serverdatenbank und den Protokollen sowie von Daten für andere Anwendungen.</p> |

| Speichertechnologietyp                      | Datenbank   | Aktive Protokolldatei  | Archivprotokoll und Archivübernahmeprotokoll  | Speicherpools  |
|---|---|--|---|--|
| <b>SATA, Network-attached Storage (NAS)</b> | Verwenden Sie diesen Speicher nicht für die Datenbank. Stellen Sie die Datenbank nicht auf XIV-Speichersysteme. | Verwenden Sie diesen Speicher nicht für die aktive Protokolldatei. | Die Verwendung dieser langsameren Speichertechnologie ist akzeptabel, da diese Protokolle einmal geschrieben und nur selten gelesen werden. | Verwenden Sie diese langsamere Speichertechnologie, wenn die folgenden Bedingungen erfüllt sind: <ul style="list-style-type: none"> <li>• Daten werden selten geschrieben, beispielsweise einmal.</li> <li>• Daten werden selten gelesen.</li> </ul> |
| <b>Bänder und virtuelle Bänder</b>          |   |  |   | Verwenden Sie diese Speichermedien für die langfristige Aufbewahrung oder wenn Daten nur selten verwendet werden.  |

## AIX: Bewährte Verfahren bei der Serverinstallation anwenden

Normalerweise hat die Konfiguration und Auswahl der Hardware die deutlichsten Auswirkungen auf die Leistung einer IBM Spectrum Protect-Lösung. Weitere Faktoren, die sich auf die Leistung auswirken, sind die Auswahl und Konfiguration des Betriebssystems sowie die Konfiguration von IBM Spectrum Protect.

### Vorgehensweise

- Nachfolgend sind die wichtigsten bewährten Verfahren für die Erzielung der optimalen Leistung und die Vermeidung von Problemen aufgeführt.
- Bestimmen Sie anhand der Tabelle die bewährten Verfahren, die für Ihre Umgebung gelten.

| Bewährtes Verfahren  | Weitere Informationen  |
|--|--|
| Verwenden Sie schnelle Platten für die Serverdatenbank. Enterprise-Solid-State-Laufwerke mit Fibre Channel- oder SAS-Schnittstellen bieten die beste Leistung. | Verwenden Sie schnelle Platten mit kurzer Latenzzeit für die Datenbank. Die Verwendung von Solid-State-Laufwerken ist von entscheidender Bedeutung, wenn Sie die Datenduplizierung und Knotenreplikation verwenden. Vermeiden Sie die Verwendung von SATA-Laufwerken (SATA = Serial Advanced Technology Attachment) und PATA-Laufwerken (PATA = Parallel Advanced Technology Attachment). Ausführliche Informationen und weitere Tipps finden Sie in: <ul style="list-style-type: none"> <li>◦ "Planung für Platten für die Serverdatenbank"</li> <li>◦ "Planung für die Auswahl des korrekten Speichertechnologietyps"</li> </ul> |
| Stellen Sie sicher, dass das Serversystem über genügend Speicher verfügt.  | Überprüfen Sie die Betriebssystemvoraussetzungen in Technote 1243309. Höhere Arbeitslasten erfordern mehr als die Mindestvoraussetzungen. Erweiterte Funktionen wie beispielsweise Datenduplizierung und Knotenreplikation können mehr Speicher als den Mindestspeicher erfordern, der im Dokument mit den Systemvoraussetzungen angegeben ist. <p>Wenn Sie die Ausführung mehrerer Instanzen planen, ist für jede Instanz der für einen einzelnen Server aufgelistete Speicher erforderlich. Multiplizieren Sie den für einen einzelnen Server erforderlichen Speicher mit der Anzahl der für das System geplanten Instanzen.</p> |

| Bewährtes Verfahren   | Weitere Informationen  |
|---|--|
| Trennen Sie die Serverdatenbank, die aktive Protokolldatei, das Archivprotokoll und die Plattenspeicherpools voneinander.   | <p>Stellen Sie alle IBM Spectrum Protect-Speicherressourcen auf unterschiedliche Platten. Trennen Sie Speicherpoolplatten von den Platten für die Serverdatenbank und die Protokolle.</p> <p>Speicherpooloperationen können Datenbankoperationen beeinträchtigen, wenn sich die Speicherpools und die Datenbank auf denselben Platten befinden. Im Idealfall werden auch die Serverdatenbank und die Protokolle voneinander getrennt.</p> <p>Ausführliche Informationen und weitere Tipps finden Sie in:</p> <ul style="list-style-type: none"> <li>○ "Planung für Platten für die Serverdatenbank"</li> <li>○ "Planung für Platten für das Serverwiederherstellungsprotokoll"</li> <li>○ "Planung für Speicherpools auf DISK- oder FILE-Einheiten"</li> </ul> |
| Verwenden Sie mindestens vier Verzeichnisse für die Serverdatenbank. Verwenden Sie für größere Server oder Server, die erweiterte Funktionen verwenden, acht Verzeichnisse.   | <p>Stellen Sie jedes Verzeichnis auf eine LUN, die von anderen LUNs und von anderen Anwendungen getrennt ist.</p> <p>Ein Server wird als großer Server betrachtet, wenn seine Datenbank größer als 2 TB ist oder wahrscheinlich diese Größe erreichen wird. Verwenden Sie für derartige Server acht Verzeichnisse.</p> <p>Siehe "Planung für Platten für die Serverdatenbank".</p>   |
| Wenn Sie die Datendeduplizierung und/oder die Knotenreplikation verwenden, beachten Sie die Richtlinien für die Datenbankkonfiguration und andere Elemente.   | <p>Konfigurieren Sie den Server gemäß den Richtlinien, da die Datenbank in Bezug darauf, wie gut die Ausführung des Servers bei Verwendung dieser Funktionen ist, extrem wichtig ist. Ausführliche Informationen und weitere Tipps finden Sie in:</p> <ul style="list-style-type: none"> <li>○ Prüfliste für Datendeduplizierung</li> <li>○ Prüfliste für Knotenreplikation</li> </ul>   |
| Beachten Sie bei Speicherpools, die Einheitenklassen des Typs FILE verwenden, die Richtlinien für die Größe von Speicherpooldatenträgern. In der Regel sind Datenträger mit einer Größe von 50 GB am besten geeignet. | <p>Lesen Sie die Informationen in Optimale Anzahl und Größe von Datenträgern für Speicherpools, die Platten verwenden zur Bestimmung der Datenträgergröße.</p> <p>Konfigurieren Sie Speicherpools und Dateisysteme auf der Basis der Anforderungen in Bezug auf den Durchsatz und nicht nur auf der Basis der Kapazitätsanforderungen.</p> <p>Trennen Sie die Speichereinheiten, die von IBM Spectrum Protect verwendet werden, von anderen Anwendungen mit hoher Ein-/Ausgabe und stellen Sie sicher, dass der Durchsatz für diesen Speicher ausreichend ist.</p> <p>Weitere Informationen finden Sie in Prüfliste für Speicherpools auf FILE- oder DISK-Einheiten.</p>   |
| Planen Sie IBM Spectrum Protect-Clientoperationen und -Serververwaltungsaktivitäten, um eine Überschneidung von Operationen zu verhindern oder auf ein Mindestmaß zu reduzieren.                                      | <p>Weitere ausführliche Informationen liefern die folgenden Themen:</p> <ul style="list-style-type: none"> <li>○ Zeitplan für tägliche Operationen optimieren</li> <li>○ Prüfliste für Serverkonfiguration</li> </ul>  |
| Überwachen Sie Operationen kontinuierlich.  | <p>Die Überwachung ermöglicht es Ihnen, Probleme frühzeitig erkennen und Ursachen leichter ermitteln zu können. Bewahren Sie Aufzeichnungen von Überwachungsberichten bis zu einem Jahr lang auf, um Trends schneller erkennen und Wachstum besser planen zu können. Siehe Umgebung im Hinblick auf die Leistung überwachen und verwalten.</p>   |

## AIX: Systemmindestvoraussetzungen für AIX-Systeme

Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem AIX-Betriebssystem ohne Datendeduplizierung installieren.



## Hardware- und Softwarevoraussetzungen für die IBM Spectrum Protect-Serverinstallation

Die folgenden Tabellen enthalten die Mindesthardware- und -softwarevoraussetzungen für die Installation eines IBM Spectrum Protect-Servers. Verwenden Sie diese Voraussetzungen als Ausgangspunkt für Systeme ohne Datendeduplizierung. Die optimale IBM Spectrum Protect-Umgebung ist mit Datendeduplizierung mithilfe der IBM Spectrum Protect Blueprints konfiguriert. Die neuesten Informationen zu den Systemvoraussetzungen finden Sie unter Technote 1243309.

### Hardwarevoraussetzungen

In Tabelle 1 sind die Hardwaremindestvoraussetzungen für den Server beschrieben. Wenn der Server die Mindestvoraussetzungen nicht erfüllt, schlägt die Installation fehl. Weitere Informationen zur Planung des Plattenspeicherplatzes finden Sie in AIX: Kapazitätsplanung.

Tabelle 1. Hardwarevoraussetzungen


| Hardwaretyp     | Hardwarevoraussetzungen  |
|-----------------|--|
| Hardware        | Ein ordnungsgemäß konfigurierter Computer mit POWER5-System oder höher (64-Bit)  |
| Plattenspeicher | <p>Folgende Mindestwerte für den Plattenspeicher:</p> <ul style="list-style-type: none"> <li>• 5 GB für das Installationsverzeichnis</li> <li>• 512 MB für das Verzeichnis /var</li> <li>• 2 GB für das Verzeichnis /tmp</li> <li>• 128 MB im Ausgangsverzeichnis des Rootbenutzers</li> <li>• 2 GB für den Bereich der gemeinsam genutzten Ressourcen</li> </ul> <p>Für den Fall, dass ein Problem auftritt und eine Diagnose erforderlich ist, wird empfohlen, temporären oder anderen Speicherbereich für ein FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) oder für andere temporäre Verwendungszwecke (z. B. für die Erfassung von Traceprotokollen) auf dem System verfügbar zu haben.</p> <p>Sehr viel zusätzlicher Plattenspeicherplatz ist für Datenbank- und Protokolldateien erforderlich. Die Größe der Datenbank ist von der Anzahl der zu speichernden Clientdateien und von der Methode abhängig, mit der sie vom Server verwaltet werden. Der Standardspeicherbereich der aktiven Protokolldatei beträgt 16 GB, das für die meisten Arbeitslasten und Konfigurationen benötigte Minimum. Wenn Sie die aktive Protokolldatei erstellen, benötigen Sie mindestens 64 GB für die Replikation. Wird sowohl Replikation als auch Datendeduplizierung verwendet, erstellen Sie eine aktive Protokolldatei mit einer Größe von 128 GB. Ordnen Sie mindestens die dreifache Größe des Standardspeicherbereichs der aktiven Protokolldatei für das Archivprotokoll zu (48 GB). Stellen Sie sicher, dass Sie über ausreichende Ressourcen verfügen, wenn Sie die Datendeduplizierung verwenden oder eine hohe Clientauslastung erwarten.</p> <p>Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN.</p> <p>Lesen Sie den Abschnitt zur AIX: Kapazitätsplanung, um weitere Informationen zum Plattenspeicherplatz zu erhalten.</p> |
| Hauptspeicher   | <p>Die folgenden Werte geben den Mindestsystemspeicherbedarf für Server mit Datenbanken bis zu 500 GB und einer Aufnahme von maximal 200 GB pro Tag an:</p> <ul style="list-style-type: none"> <li>• 16 GB für Standardserverbetrieb ohne Datendeduplizierung und Knotenreplikation</li> <li>• 24 GB für Datendeduplizierung oder Knotenreplikation</li> <li>• 32 GB für Knotenreplikation mit Datendeduplizierung</li> </ul> <p>Speziellere Angaben zum Speicherbedarf für große Datenbanken und höhere Aufnahmefähigkeit finden Sie in der Tabelle für die Serverspeicheroptimierung von IBM Spectrum Protect.</p> <p>Ausführliche Informationen zum Speicherbedarf bei Verwendung der Datendeduplizierung finden Sie unter IBM Spectrum Protect Blueprint für Ihr Betriebssystem.</p>   |


### Softwarevoraussetzungen

In Tabelle 2 sind die für einen Server auf einem AIX-System erforderlichen Softwaremindestvoraussetzungen beschrieben.

Tabelle 2. Softwarevoraussetzungen

| Softwaretyp | Softwaremindestvoraussetzungen |
|-------------|--------------------------------|
|-------------|--------------------------------|

| Softwaretyp           | Softwaremindestvoraussetzungen   |
|-----------------------|--|
| Betriebssystem        | <p>AIX 6.1 in einer 64-Bit-Kernel-Umgebung mit folgenden zusätzlichen Voraussetzungen:</p> <ul style="list-style-type: none"> <li>• AIX 6.1 TL 7 und SP6.</li> <li>• C++-Mindestlaufzeitversion mit den Dateigruppen xLC.rte 12.1.0.1 oder höher. Die Dateigruppe wird automatisch aktualisiert, wenn die Version älter als 12.1.0.1 ist. Die Dateigruppe ist im Fixpackpaket für IBM® C++ Runtime Environment Components for AIX vom Juni 2008 enthalten.</li> </ul> <p>AIX 7.1 in einer 64-Bit-Kernel-Umgebung.</p> <ul style="list-style-type: none"> <li>• AIX 7.1 TL 4 und SP2.</li> <li>• C++-Mindestlaufzeitversion mit den Dateigruppen xLC.rte 12.1.0.1 oder höher. Die Dateigruppe wird automatisch aktualisiert, wenn die Version älter als 12.1.0.1 ist. Die Dateigruppe ist im Fixpackpaket für IBM C++ Runtime Environment Components for AIX vom Juni 2008 enthalten.</li> </ul> <p>AIX 7.2 in einer 64-Bit-Kernel-Umgebung.</p> <ul style="list-style-type: none"> <li>• AIX 7.2 TL 0 und SP2.</li> <li>• C++-Mindestlaufzeitversion mit den Dateigruppen xLC.rte 13.1.3.1 oder höher. Die Dateigruppe wird automatisch aktualisiert, wenn die Version älter als 13.1.3.1 ist.</li> </ul> <p>Aktuelle Empfehlungen für AIX-Programmfices finden Sie unter Technote 21165448</p> <p>Damit die Funktion NPIV (N_Port ID Virtualization) genutzt werden kann, müssen die folgenden Mindestvoraussetzungen erfüllt sein:</p> <ul style="list-style-type: none"> <li>• Virtual I/O Server 2.1.2 oder höher</li> <li>• AIX 7.1 oder höher</li> <li>• Ein vom entsprechenden AIX-Server und Virtual I/O Server unterstützter HBA-Adapter</li> </ul> |
| Übertragungsprotokoll | Eine konfigurierte Übertragungsmethode.  |
| Verarbeitung          | Asynchrone Ein-/Ausgabe muss aktiviert sein.   |
| Einheitentreiber      | <p>Der IBM Spectrum Protect-Einheitentreiber ist für Laufwerke und Bandarchive eines anderen Herstellers erforderlich. Das IBM Spectrum Protect-Einheitentreiberpaket enthält Einheitentreibertools und ACSLS-Dämonen.</p> <p>Für die Bandarchive bzw. Bandlaufwerke IBM 3590, 3592 oder Ultrium sind die IBM Einheitentreiber erforderlich. Installieren Sie die aktuellen Einheitentreiber. IBM-Treiberpakete finden Sie bei Fix Central.</p> <p>Konfigurieren Sie die Einheitentreiber, bevor Sie den Server für Bandeinheiten verwenden.</p>   |
| Dienstprogramm gunzip | Das Dienstprogramm gunzip muss auf Ihrem System verfügbar sein, bevor Sie den Server installieren oder aktualisieren. Stellen Sie sicher, dass das Dienstprogramm gunzip installiert ist und dass der entsprechende Pfad in der Umgebungsvariablen PATH definiert ist.   |
| Sonstige Software     | <p>Korn-Shell (ksh) ist erforderlich.</p> <p> AIX-Betriebssysteme Konfigurieren Sie die I/O Completion Ports (IOCP) auf dem Betriebssystem.</p> <p>Um IBM Spectrum Protect-Benutzer mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol) zu authentifizieren, müssen Sie einen der folgenden Verzeichnisserver verwenden:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server Version 6.3</li> <li>• IBM Security Directory Server Version 6.4</li> </ul>  |

 AIX-Betriebssysteme

## AIX: Kompatibilität des IBM Spectrum Protect-Servers mit anderen DB2-Produkten auf dem System

Sie können andere Produkte, die DB2-Produkte auf demselben System wie der IBM Spectrum Protect-Server der Version 8.1.3 implementieren und verwenden, mit einigen Einschränkungen installieren.

Damit andere Produkte, die ein DB2-Produkt auf demselben System wie der IBM Spectrum Protect-Server verwenden, installiert und verwendet werden können, müssen die folgenden Bedingungen erfüllt sein:

Tabelle 1. Kompatibilität des IBM Spectrum Protect-Servers mit anderen DB2-Produkten auf dem System

| Bedingung                      | Anweisungen   |
|--------------------------------|---|
| Versionsschnittstelle          | Die anderen Produkte, die ein DB2-Produkt verwenden, müssen DB2 Version 9 oder höher verwenden. DB2-Produkte verfügen ab Version 9 über die Unterstützung für Produktkapselung und -trennung. Ab dieser Version können Sie mehrere Kopien von DB2-Produkten mit unterschiedlichen Codeversionen auf demselben System ausführen. Ausführliche Informationen finden Sie in dem Abschnitt über mehrere DB2-Kopien in der Produktinformation zu DB2.  |
| Benutzer-IDs und Verzeichnisse | Stellen Sie sicher, dass die Benutzer-IDs, die IDs der abgeschirmten Benutzer, die Installationsposition, andere Verzeichnisse und zugehörige Informationen nicht von mehreren DB2-Installationen gemeinsam genutzt werden. Ihre Angaben müssen sich von den IDs und Positionen unterscheiden, die Sie für die Installation und Konfiguration des IBM Spectrum Protect-Servers verwendet haben. Wenn Sie den Assistenten dsmicfgx für die Konfiguration des Servers verwendet haben, haben Sie diese Werte während der Ausführung des Assistenten eingegeben. Wenn Sie eine manuelle Konfiguration durchgeführt haben, überprüfen Sie im Bedarfsfall die verwendeten Prozeduren, um sich die für den Server verwendeten Werte in Erinnerung zu rufen.   |
| Ressourcenanzuordnung          | <p>Sie müssen die Ressourcen und das Leistungsspektrum des Systems gegen die Anforderungen für den IBM Spectrum Protect-Server und die anderen Anwendungen, die das DB2-Produkt verwenden, abwägen. Damit den anderen DB2-Anwendungen genügend Ressourcen zur Verfügung stehen, müssen Sie unter Umständen die Einstellungen des IBM Spectrum Protect-Servers ändern, so dass der Server weniger Systemspeicher und -ressourcen verwendet. Wenn die Verarbeitungsprozesse für die anderen DB2-Anwendungen und der IBM Spectrum Protect-Server um Prozessor- und Speicherressourcen konkurrieren, kann die Leistung des Servers in Bezug auf die Verarbeitung der erwarteten Clientauslastung oder anderer Serveroperationen beeinträchtigt werden.</p> <p>Um die Ressourcen zu trennen und die Möglichkeit zur Optimierung und Zuordnung von Prozessor-, Speicher- und anderen Systemressourcen für mehrere Anwendungen zu verbessern, sollten Sie Unterstützung für logische Partitionen (LPAR), Auslastungspartitionierung (WPAR) oder andere Unterstützung für virtuelle Workstations einsetzen. Führen Sie eine DB2-Anwendung beispielsweise auf einem eigenen virtuellen System aus.</p> |

## AIX: IBM Installation Manager

IBM Spectrum Protect verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositorys installiert oder aktualisiert werden können.

Wenn die erforderliche Version von IBM Installation Manager noch nicht installiert ist, wird sie automatisch installiert oder aktualisiert, wenn Sie IBM Spectrum Protect installieren. Die Software muss auf dem System installiert bleiben, damit IBM Spectrum Protect später nach Bedarf aktualisiert oder deinstalliert werden kann.

Die folgende Liste enthält Erläuterungen einiger Begriffe, die in IBM Installation Manager verwendet werden:

### Angebot

Eine installierbare Einheit eines Softwareprodukts.

Das Angebot 'IBM Spectrum Protect' enthält alle Datenträger, die IBM Installation Manager für die Installation von IBM Spectrum Protect benötigt.

### Paket

Die Gruppe der Softwarekomponenten, die für die Installation eines Angebots benötigt werden.

Das IBM Spectrum Protect-Paket enthält folgende Komponenten:

- Installationsprogramm IBM Installation Manager
- Das Angebot 'IBM Spectrum Protect'

### Paketgruppe

Eine Gruppe von Paketen mit demselben übergeordneten Verzeichnis.

Die Standardpaketgruppe für das IBM Spectrum Protect-Paket ist `IBM Installation Manager`.

### Repository

Ein ferner oder lokaler Speicherbereich für Daten und andere Anwendungsressourcen.

Das IBM Spectrum Protect-Paket wird in einem Repository in IBM Fix Central gespeichert.

Verzeichnis für gemeinsam genutzte Ressourcen

Ein Verzeichnis, das Softwaredateien oder Plug-ins enthält, die von Paketen gemeinsam genutzt werden.

In dem Verzeichnis für gemeinsam genutzte Ressourcen speichert IBM Installation Manager installationsbezogene Dateien, darunter Dateien, die für das Rollback zu einer vorherigen Version von IBM Spectrum Protect verwendet werden.

## AIX: Arbeitsblätter für Planungsdetails für den Server

Sie können die Arbeitsblätter für die Planung der Größe und der Position des für den IBM Spectrum Protect-Server benötigten Speichers verwenden. Sie können darauf auch Namen und Benutzer-IDs aufzeichnen.

| Element  | Erforderlicher Speicherbereich | Anzahl der Verzeichnisse | Position der Verzeichnisse |
|--|--------------------------------|--------------------------|----------------------------|
| Die Datenbank  |                                |                          |                            |
| Aktive Protokolldatei  |                                |                          |                            |
| Archivprotokoll  |                                |                          |                            |
| Optional: Protokollspiegel für die aktive Protokolldatei                         |                                |                          |                            |
| Optional: Sekundäres Archivprotokoll (Übernahmeverzeichnis für Archivprotokolle) |                                |                          |                            |

| Element   | Namen und Benutzer-IDs | Position |
|---|------------------------|----------|
| Die <i>Instanzbenutzer-ID</i> für den Server. Mit dieser ID starten Sie den IBM Spectrum Protect-Server und führen ihn aus.   |                        |          |
| Das <i>Ausgangsverzeichnis</i> des Servers. In diesem Verzeichnis befindet sich die Instanzbenutzer-ID.   |                        |          |
| Der Datenbankinstanzname  |                        |          |
| Das <i>Instanzverzeichnis</i> für den Server. Dieses Verzeichnis enthält spezielle Dateien für diese Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien). |                        |          |
| Der Servername; verwenden Sie einen eindeutigen Namen für jeden Server.   |                        |          |

## AIX: Kapazitätsplanung

Zur Kapazitätsplanung für IBM Spectrum Protect gehört die Verwaltung von Ressourcen wie z. B. die Datenbank, das Wiederherstellungsprotokoll und der Bereich für gemeinsam genutzte Ressourcen. Sie müssen den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll schätzen, um die Ressourcen als Teil der Kapazitätsplanung zu maximieren. Der verfügbare Speicherplatz für den Bereich für gemeinsam genutzte Ressourcen muss für jede Installation bzw. jedes Upgrade ausreichen.

- AIX: Speicherbedarf für die Datenbank schätzen  
Sie können den Speicherbedarf für die Datenbank auf der Basis der maximalen Anzahl Dateien schätzen, die sich gleichzeitig im Serverspeicher befinden können, oder auf der Basis der Speicherpoolkapazität.
- AIX: Speicherplatzbedarf für das Wiederherstellungsprotokoll  
In IBM Spectrum Protect beinhaltet der Begriff *Wiederherstellungsprotokoll* die aktive Protokolldatei, das Archivprotokoll, den Spiegel der aktiven Protokolldatei und das Archivübernahmeprotokoll. Der für das Wiederherstellungsprotokoll erforderliche Speicherbereich ist von verschiedenen Faktoren, wie z. B. dem Umfang der Clientaktivität mit dem Server, abhängig.
- AIX: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen  
Um den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei zu bestimmen, geben Sie den Befehl QUERY LOG

ein. Um die Speicherauslastung in der Datenbank und den Wiederherstellungsprotokollen zu überwachen, können Sie auch das Aktivitätenprotokoll auf Nachrichten überprüfen.

- AIX: Rollbackdateien der Installation löschen  
Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, löschen, um Speicherplatz im Verzeichnis für gemeinsam genutzte Ressourcen freizugeben. Zu den Dateitypen, die Sie löschen können, gehören z. B. Dateien, die für eine Rollbackoperation benötigt wurden.

## AIX: Speicherbedarf für die Datenbank schätzen

---

Sie können den Speicherbedarf für die Datenbank auf der Basis der maximalen Anzahl Dateien schätzen, die sich gleichzeitig im Serverspeicher befinden können, oder auf der Basis der Speicherpoolkapazität.

### Informationen zu diesem Vorgang

---

Anfänglich sollte mindestens 25 GB Speicherplatz in der Datenbank verwendet werden. Stellen Sie entsprechend Speicherplatz im Dateisystem bereit. Eine Datenbankgröße von 25 GB ist für eine Testumgebung oder eine Umgebung, die nur einen Speicherarchivmanager umfasst, ausreichend. Für einen Produktionsserver, der Clientlasten unterstützt, sollte die Datenbank größer sein. Wenn Sie Plattenspeicherpools (DISK) mit wahlfreiem Zugriff verwenden, ist mehr Datenbank- und Protokollspeicherbereich erforderlich als für Speicherpools mit sequenziellem Zugriff.

Die maximale Größe der IBM Spectrum Protect-Datenbank beträgt 6 TB.

Informationen zur Festlegung der Größe einer Datenbank in einer Produktionsumgebung, die auf der Anzahl Dateien und der Speicherpoolgröße basiert, enthalten die folgenden Abschnitte.

- AIX: Speicherbedarf für die Datenbank auf der Basis der Anzahl Dateien schätzen  
Wenn die maximale Anzahl Dateien, die sich zu einem bestimmten Zeitpunkt im Serverspeicher befinden, geschätzt werden kann, können Sie diese Zahl verwenden, um den Speicherbedarf für die Datenbank zu schätzen.
- AIX: Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität schätzen  
Um den Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität zu schätzen, verwenden Sie ein Verhältnis von 1-5 %. Sind beispielsweise 200 TB Speicherpoolkapazität erforderlich, sollte die Größe der Datenbank erwartungsgemäß zwischen 2 und 10 TB betragen. Als allgemeine Regel gilt: Wählen Sie die Größe ihrer Datenbank so groß wie möglich, um zu verhindern, dass der Speicherplatz knapp wird. Wenn der Speicherplatz knapp wird, können Serveroperationen und Clientspeicheroperationen fehlschlagen.
- AIX: Datenbankmanager und temporärer Speicherbereich  
Der Datenbankmanager des IBM Spectrum Protect-Servers verwaltet Systempeicher und Plattenspeicher für die Datenbank und ordnet diesen Speicher zu. Der benötigte Datenbankspeicherbereich ist von der Größe des verfügbaren Systemspeichers und von der Serverauslastung abhängig.

## AIX: Speicherbedarf für die Datenbank auf der Basis der Anzahl Dateien schätzen

---

Wenn die maximale Anzahl Dateien, die sich zu einem bestimmten Zeitpunkt im Serverspeicher befinden, geschätzt werden kann, können Sie diese Zahl verwenden, um den Speicherbedarf für die Datenbank zu schätzen.

### Informationen zu diesem Vorgang

---

Um den Speicherbedarf auf der Basis der maximalen Anzahl Dateien im Serverspeicher zu schätzen, verwenden Sie die folgenden Richtlinien:

- 600-1000 Byte für jede gespeicherte Version einer Datei einschließlich der Imagesicherungen.  
Einschränkung: Diese Richtlinie umfasst nicht den Speicherplatz, der während der Dateneduplizierung verwendet wird.
- 100-200 Byte für jede Datei im Cache, jede Kopierspeicherpooldatei, jede Datei im Pool für aktive Daten und jede deduplizierte Datei.
- Zusätzlicher Speicherbereich ist für die Datenbankoptimierung erforderlich, um variable Datenzugriffsmuster und die Server-Back-End-Verarbeitung von Daten zu unterstützen. Die Größe des zusätzlichen Speicherplatzes entspricht 50 % der Schätzung für die Gesamtanzahl Byte für Dateiobjekte.

In dem folgenden Beispiel für einen einzelnen Client basieren bei Berechnungen auf den Maximalwerten in den vorhergehenden Richtlinien. Bei den Beispielen wird die mögliche Verwendung der Dateiaggregation nicht berücksichtigt. Im Allgemeinen wird durch das Aggregieren kleiner Dateien der erforderliche Speicherplatz in der Datenbank reduziert. Die Dateiaggregation betrifft keine speicherwarteten Dateien.

## Vorgehensweise

---

1. Berechnen Sie die Anzahl Dateiversionen. Addieren Sie alle folgenden Werte, um die Anzahl Dateiversionen zu erhalten:
  - a. Berechnen Sie die Anzahl gesicherter Dateien. Beispiel: Möglicherweise werden bis zu 500.000 Clientdateien gleichzeitig gesichert. In diesem Beispiel sind die Speichermaßnahmen so definiert, dass maximal drei Kopien gesicherter Dateien aufbewahrt werden:  
$$500.000 \text{ Dateien} * 3 \text{ Kopien} = 1.500.000 \text{ Dateien}$$
  - b. Berechnen Sie die Anzahl Archivierungsdateien. Beispiel: Bis zu 100.000 Clientdateien können archivierte Kopien sein.
  - c. Berechnen Sie die Anzahl speicherwarteter Dateien. Beispiel: Bis zu 200.000 Clientdateien können von Client-Workstations umgelagert werden.Bei Verwendung von 1000 Byte pro Datei beträgt der Gesamtspeicherplatz in der Datenbank, der für die zu dem Client gehörigen Dateien erforderlich ist, 1,8 GB:

$$(1.500.000 + 100.000 + 200.000) * 1000 = 1,8 \text{ GB}$$

2. Berechnen Sie die Anzahl Dateien im Cache, Kopierspeicherpooldateien, Dateien im Pool für aktive Daten und deduplizierter Dateien:
  - a. Berechnen Sie die Anzahl der Cachekopien. Beispiel: In einem Plattenspeicherpool mit 5 GB Kapazität ist Caching aktiviert. Die obere Umlagerungsschwelle des Pools ist 90 % und die untere Umlagerungsschwelle ist 70 %. Das heißt 20 % des Plattenpools (oder 1 GB) wird von Cachedateien belegt. Wenn die durchschnittliche Dateigröße ungefähr 10 KB beträgt, enthält der Cache zu jedem beliebigen Zeitpunkt etwa 100.000 Dateien:  
$$100.000 \text{ Dateien} * 200 \text{ Byte} = 19 \text{ MB}$$
  - b. Berechnen Sie die Anzahl Kopierspeicherpooldateien. Alle primären Speicherpools werden im Kopierspeicherpool gesichert:  
$$(1.500.000 + 100.000 + 200.000) * 200 \text{ Byte} = 343 \text{ MB}$$
  - c. Berechnen Sie die Anzahl Dateien im Speicherpool für aktive Daten. Alle aktiven Clientsicherungsdaten in primären Speicherpools werden in den Speicherpool für aktive Daten kopiert. Angenommen, es sind 500.000 Versionen der 1.500.000 Sicherungsdateien im primären Speicherpool aktiv:  
$$500.000 * 200 \text{ Byte} = 95 \text{ MB}$$
  - d. Berechnen Sie die Anzahl deduplizierter Dateien. Angenommen, ein deduplizierter Speicherpool enthält 50.000 Dateien:  
$$50.000 * 200 \text{ Byte} = 10 \text{ MB}$$

Auf der Basis der vorhergehenden Berechnungen sind etwa 0,5 GB zusätzlicher Speicherplatz in der Datenbank für die Cachedateien, die Kopierspeicherpooldateien, die Dateien im Pool für aktive Daten und die deduplizierten Dateien des Clients erforderlich.

3. Berechnen Sie den zusätzlichen Speicherplatz, der für die Datenbankoptimierung benötigt wird. Um optimalen Datenzugriff und optimale Verwaltung durch den Server bereitzustellen, ist zusätzlicher Speicherplatz in der Datenbank erforderlich. Die Größe des zusätzlichen Speicherplatzes in der Datenbank beträgt 50 % des Gesamtspeicherbedarfs für Dateiobjekte.  
$$(1,8 + 0,5) * 50 \% = 1,2 \text{ GB}$$
4. Die Gesamtgröße des für den Client erforderlichen Datenbankspeicherbereichs berechnen. Die Gesamtgröße beträgt ca. 3,5 GB:  
$$1,8 + 0,5 + 1,2 = 3,5 \text{ GB}$$
5. Berechnen Sie den Gesamtspeicherplatz in der Datenbank, der für alle Clients erforderlich ist. Wenn der Client, der in den vorhergehenden Berechnungen verwendet wurde, ein typischer Client ist und Sie beispielsweise über 500 Clients verfügen, können Sie den Gesamtspeicherplatz in der Datenbank, der für alle Clients erforderlich ist, mithilfe der folgenden Berechnung schätzen:  
$$500 * 3,5 = 1,7 \text{ TB}$$

## Ergebnisse

---

Tipp: In den Beispielen oben handelt es sich bei den Ergebnissen um Schätzungen. Die tatsächliche Größe der Datenbank kann aufgrund von Faktoren wie beispielsweise der Anzahl Verzeichnisse und der Länge der Pfad- und Dateinamen von der geschätzten Größe abweichen. Sie sollten die Datenbank regelmäßig überwachen und die Größe wie erforderlich anpassen.

## Nächste Schritte

---

Während des normalen Betriebs erfordert der IBM Spectrum Protect-Server möglicherweise temporären Speicherplatz in der Datenbank. Dieser Speicherplatz wird aus den folgenden Gründen benötigt:

- Zum Speichern der Ergebnisse der Sortierung oder Änderung der Reihenfolge, die noch nicht in der Datenbank aufbewahrt und in der Datenbank nicht unmittelbar optimiert werden. Die Ergebnisse werden vorübergehend in der Datenbank zur Verarbeitung gespeichert.
- Zum Erteilen des Verwaltungszugriffs auf die Datenbank über eine der folgenden Methoden:
  - Ein DB2-ODBC-Client (ODBC = Open Database Connectivity)
  - Ein Oracle-JDBC-Client (JDBC = Java™ Database Connectivity)
  - SQL (Structured Query Language) für den Server über die Befehlszeile eines Verwaltungsclients

Erwägen Sie die Verwendung von zusätzlichen 50 GB an temporärem Speicherplatz pro 500 GB Speicherbereich für Dateiobjekte und Optimierung. Siehe die Richtlinien in der folgenden Tabelle. In dem Beispiel, das im vorhergehenden Schritt verwendet wurde, sind insgesamt 1,7 TB Speicherplatz in der Datenbank für Dateiobjekte und die Optimierung für 500 Clients erforderlich. Auf der Basis dieser Berechnung sind 200 GB für temporären Speicherplatz erforderlich. Der erforderliche Gesamtspeicherplatz in der Datenbank beträgt 1,9 TB.

| Datenbankgröße      | Mindestens erforderlicher temporärer Speicherplatz |
|---------------------|--|
| < 500 GB            | 50 GB  |
| ≥ 500 GB und < 1 TB | 100 GB   |
| ≥ 1 TB und < 1,5 TB | 150 GB   |
| ≥ 1,5 und < 2 TB    | 200 GB   |
| ≥ 2 und < 3 TB      | 250-300 GB   |
| ≥ 3 und < 4 TB      | 350-400 GB   |

## AIX: Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität schätzen

---

Um den Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität zu schätzen, verwenden Sie ein Verhältnis von 1-5 %. Sind beispielsweise 200 TB Speicherpoolkapazität erforderlich, sollte die Größe der Datenbank erwartungsgemäß zwischen 2 und 10 TB betragen. Als allgemeine Regel gilt: Wählen Sie die Größe ihrer Datenbank so groß wie möglich, um zu verhindern, dass der Speicherplatz knapp wird. Wenn der Speicherplatz knapp wird, können Serveroperationen und Clientspeicheroperationen fehlschlagen.

## AIX: Datenbankmanager und temporärer Speicherbereich

---

Der Datenbankmanager des IBM Spectrum Protect-Servers verwaltet System Speicher und Plattenspeicher für die Datenbank und ordnet diesen Speicher zu. Der benötigte Datenbankspeicherbereich ist von der Größe des verfügbaren System Speichers und von der Serverauslastung abhängig.

Der Datenbankmanager sortiert Daten in einer bestimmten Reihenfolge, gemäß der SQL-Anweisung, mit der Sie die Daten anfordern. Je nach Auslastung des Servers und wenn es mehr Daten gibt, als der Datenbankmanager verwalten kann, werden die (der Reihenfolge nach sortierten) Daten temporärem Plattenspeicher zugeordnet. Daten werden temporärem Plattenspeicher zugeordnet, wenn die Ergebnismenge sehr umfangreich ist. Der Datenbankmanager verwaltet den verwendeten Speicher dynamisch, wenn Daten temporärem Plattenspeicher zugeordnet werden.

Bei der Verfallsverarbeitung kann beispielsweise eine umfangreiche Ergebnismenge generiert werden. Wenn der System Speicher in der Datenbank zur Speicherung der Ergebnismenge nicht ausreicht, wird ein Teil der Daten temporärem Plattenspeicher zugeordnet. Wenn während der Verfallsverarbeitung ein Knoten oder ein Dateibereich ausgewählt wird, der für die Verarbeitung zu groß ist, kann der Datenbankmanager die Daten im Speicher nicht sortieren. Der Datenbankmanager muss temporären Speicherbereich zum Sortieren der Daten verwenden.

Bei der Ausführung von Datenbankoperationen sollten Sie in den folgenden Szenarios eine Erweiterung des Speicherplatzes in der Datenbank vornehmen:

- Der Speicherbereich der Datenbank ist klein und die Serveroperation, die temporären Speicherbereich benötigt, belegt den verbleibenden freien Speicherbereich.
- Die Dateibereiche sind groß oder den Dateibereichen ist eine Maßnahme zugeordnet, durch die viele Dateiversionen erstellt werden.
- Der IBM Spectrum Protect-Server muss mit begrenztem Speicher ausgeführt werden. Die Datenbank verwendet den Hauptspeicher des IBM Spectrum Protect-Servers für Datenbankoperationen. Ist der verfügbare Speicher jedoch nicht ausreichend, ordnet der IBM Spectrum Protect-Server der Datenbank temporären Speicherbereich auf Platte zu. Wenn

beispielsweise 10G Speicher zur Verfügung stehen und Datenbankoperationen 12G Speicher benötigen, verwendet die Datenbank temporären Speicherbereich.

- Bei der Implementierung eines IBM Spectrum Protect-Servers wird ein Fehler aufgrund fehlenden Datenbankspeicherbereichs (out of database space) angezeigt. Überwachen Sie das Serveraktivitätenprotokoll auf Nachrichten, die sich auf den Datenbankspeicherbereich beziehen.

Wichtig: Sie dürfen die DB2-Software, die mit IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht verändern. Führen Sie keine Installation bzw. kein Upgrade auf eine andere Version, ein anderes Release oder ein anderes Fixpack der DB2-Software durch, um eine Beschädigung der Datenbank zu vermeiden.

## AIX: Speicherplatzbedarf für das Wiederherstellungsprotokoll

---

In IBM Spectrum Protect beinhaltet der Begriff *Wiederherstellungsprotokoll* die aktive Protokolldatei, das Archivprotokoll, den Spiegel der aktiven Protokolldatei und das Archivübernahmeprotokoll. Der für das Wiederherstellungsprotokoll erforderliche Speicherbereich ist von verschiedenen Faktoren, wie z. B. dem Umfang der Clientaktivität mit dem Server, abhängig.

- AIX: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll  
Wenn Sie den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll schätzen, müssen Sie einigen zusätzlichen Speicherbereich für gelegentlich auftretende hohe Lasten und Übernahmesituationen einkalkulieren.
- AIX: Speicherbereich des Spiegels für aktive Protokolldateien  
Die aktive Protokolldatei kann gespiegelt werden, sodass die gespiegelte Kopie verwendet werden kann, falls die aktiven Protokolldateien nicht gelesen werden können. Es kann nur ein einziger Spiegel der aktiven Protokolldatei vorhanden sein.
- AIX: Speicherbereich des Übernahmeverzeichnisses für Archivprotokolle  
Das Übernahmeverzeichnis für Archivprotokolle wird vom Server verwendet, wenn der Speicherbereich des Verzeichnisses für Archivprotokolle nicht mehr ausreicht.

## AIX: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll

---

Wenn Sie den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll schätzen, müssen Sie einigen zusätzlichen Speicherbereich für gelegentlich auftretende hohe Lasten und Übernahmesituationen einkalkulieren.

In IBM Spectrum Protect-Servern der Version 7.1 und höher kann die aktive Protokolldatei eine maximale Größe von 512 GB haben. Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist.

Berücksichtigen Sie bei der Schätzung der Größe der aktiven Protokolldatei die folgenden allgemeinen Richtlinien:

- Die empfohlene Anfangsgröße für die aktive Protokolldatei ist 16 GB.
- Stellen Sie sicher, dass die aktive Protokolldatei mindestens groß genug ist, um die gleichzeitig ablaufende Aktivität handhaben zu können, die der Server in der Regel handhabt. Versuchen Sie als Vorsichtsmaßnahme das größte Arbeitsvolumen zu schätzen, das der Server jeweils handhabt. Stellen Sie für die aktive Protokolldatei zusätzlichen Speicherbereich bereit, der, falls erforderlich, verwendet werden kann. Ziehen Sie 20 % zusätzlichen Speicherbereich in Betracht.
- Überwachen Sie den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei. Passen Sie die Größe der aktiven Protokolldatei wie erforderlich abhängig von Faktoren wie Clientaktivität und Ebene der Serveroperationen an.
- Stellen Sie sicher, dass das Verzeichnis, das die aktive Protokolldatei enthält, mindestens genauso groß wie die aktive Protokolldatei ist. Ein Verzeichnis, das größer als die aktive Protokolldatei ist, kann Übernahmesituationen handhaben, sollten diese auftreten.
- Stellen Sie sicher, dass das Dateisystem, das das Verzeichnis für aktive Protokolldateien enthält, über mindestens 8 GB freien Speicherbereich für Anforderungen zum Versetzen temporärer Protokolle verfügt.

Die vorgeschlagene Anfangsgröße für das Archivprotokoll beträgt 48 GB.

Das Archivprotokollverzeichnis muss groß genug sein, um die Protokolldateien aufnehmen zu können, die seit der vorherigen Gesamtsicherung generiert wurden. Wenn Sie beispielsweise täglich eine Gesamtsicherung der Datenbank ausführen, muss das Archivprotokollverzeichnis groß genug sein, um die Protokolldateien für die gesamte Clientaktivität aufnehmen zu können, die während 24 Stunden stattfindet. Um Speicherbereich wiederherzustellen, löscht der Server veraltete Archivprotokolldateien nach einer Gesamtsicherung der Datenbank. Wenn das Archivprotokollverzeichnis voll wird und kein Verzeichnis für Archivübernahmeprotokolle vorhanden ist, verbleiben Protokolldateien im Verzeichnis für aktive Protokolldateien. Diese Bedingung kann zur Folge haben, dass das Verzeichnis für aktive Protokolldateien vollständig gefüllt und der Server gestoppt wird. Bei einem Serverneustart wird ein Teil des vorhandenen Speicherbereichs für die aktive Protokolldatei freigegeben wird.

Nach der Installation des Servers können Sie die Archivprotokollauslastung und den Speicherbereich im Archivprotokollverzeichnis überwachen. Wenn sich der Speicherbereich im Archivprotokollverzeichnis füllt, können die folgenden Probleme auftreten:

- Der Server kann keine Datenbankgesamtsicherungen ausführen. Untersuchen und beheben Sie dieses Problem.
- Andere Anwendungen schreiben in das Archivprotokollverzeichnis und belegen den für das Archivprotokoll erforderlichen Speicherbereich. Nutzen Sie den Speicherbereich für das Archivprotokoll nicht gemeinsam mit anderen Anwendungen,



einschließlich anderer IBM Spectrum Protect-Server. Stellen Sie sicher, dass jeder Server über eine separate Speicherposition verfügt, dessen Eigner dieser spezifische Server ist und der von diesem spezifischen Server verwaltet wird.

- AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen schätzen  
Grundlegende Clientspeicheroperationen umfassen Sicherung, Archivierung und Speicherbereichsverwaltung. Der Protokollspeicherbereich muss groß genug sein, um alle Speichertransaktionen handhaben zu können, die gleichzeitig aktiv sind.
- AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, schätzen  
Wenn Sie Clientoption RESOURCEUTILIZATION auf einen größeren Wert als den Standardwert gesetzt ist, erhöht sich die gleichzeitige Last für den Server.
- AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Operationen für gleichzeitiges Schreiben schätzen  
Wenn Clientsicherungsoperationen Speicherpools verwenden, die für gleichzeitiges Schreiben konfiguriert sind, erhöht sich der Protokollspeicherbedarf, der für jede Datei erforderlich ist.
- AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen und Serveroperationen schätzen  
Die Umlagerung von Daten in Serverspeicher, Identifikationsprozesse für die Dateneduplizierung, Wiederherstellung und Verfallsverarbeitung werden möglicherweise gleichzeitig mit Clientspeicheroperationen ausgeführt. Verwaltungstasks wie Verwaltungsbefehle oder SQL-Abfragen von Verwaltungsclients können ebenfalls gleichzeitig mit Clientspeicheroperationen ausgeführt werden. Serveroperationen und Verwaltungstasks, die gleichzeitig ausgeführt werden, können den erforderlichen Speicherbereich für die aktive Protokolldatei erhöhen.
- AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls unter Bedingungen mit extremen Abweichungen schätzen  
Probleme in Bezug auf knapp werdenden Speicherbereich für die aktive Protokolldatei können auftreten, wenn viele Transaktionen, die sehr schnell ausgeführt werden, zusammen mit einigen Transaktionen vorhanden sind, deren Ausführung sehr viel länger dauern kann. Ein typischer Fall sind viele aktive Workstation- oder Dateiserversicherungssitzungen und wenige aktive Serversicherungssitzungen für sehr große Datenbanken. Trifft diese Situation für Ihre Umgebung zu, müssen Sie möglicherweise die Größe der aktiven Protokolldatei erhöhen, damit die Arbeit erfolgreich ausgeführt werden kann.
- AIX: Beispiel: Größe des Archivprotokolls bei Datenbankgesamticherungen schätzen  
Der IBM Spectrum Protect-Server löscht nicht benötigte Dateien nur dann aus dem Archivprotokoll, wenn eine Datenbankgesamticherung ausgeführt wird. Demzufolge müssen Sie beim Schätzen des für das Archivprotokoll erforderlichen Speicherbereichs auch die Häufigkeit, mit der Datenbankgesamticherungen ausgeführt werden, berücksichtigen.
- AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Dateneduplizierungsoperationen schätzen  
Wenn Sie Daten deduplizieren, müssen Sie die Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll berücksichtigen.

## AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen schätzen

Grundlegende Clientspeicheroperationen umfassen Sicherung, Archivierung und Speicherbereichsverwaltung. Der Protokollspeicherbereich muss groß genug sein, um alle Speichertransaktionen handhaben zu können, die gleichzeitig aktiv sind.

Um die Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen zu bestimmen, führen Sie die folgende Berechnung aus:

Anzahl Clients x In jeder Transaktion gespeicherte Dateien  
x Für jede Datei benötigter Protokollspeicherbereich

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Grundlegende Clientspeicheroperationen

| Element   | Beispielwerte | Beschreibung  |
|---|---------------|---|
| Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern | 300           | Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern. |
| Anzahl während jeder Transaktion gespeicherter Dateien  | 4096          | Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.                         |

| Element  | Beispielwerte        | Beschreibung   |
|--|----------------------|--|
| Für jede Datei erforderlicher Protokollspeicherbereich   | 3053 Byte            | Der Wert von 3053 Byte für jede Datei in einer Transaktion gibt die Protokollbyte an, die erforderlich sind, wenn Dateien von einem Windows-Client gesichert werden, auf dem Dateinamen eine Länge von 12-120 Byte haben.<br><br>Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients für Sichern/Archivieren gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet. |
| Aktive Protokolldatei: vorgeschlagene Größe  | 19,5 GB <sup>1</sup> | Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.<br><br>(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 Byte = 3,5 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>3,5 + 16 = 19,5 GB  |
| Archivprotokoll: vorgeschlagene Größe  | 58,5 GB <sup>1</sup> | Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen.<br><br>3,5 x 3 = 10,5 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:<br><br>10,5 + 48 = 58,5 GB  |
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |                      |  |

## AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, schätzen

Wenn Sie Clientoption RESOURCEUTILIZATION auf einen größeren Wert als den Standardwert gesetzt ist, erhöht sich die gleichzeitige Last für den Server.

Um die Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, zu bestimmen, führen Sie die folgende Berechnung aus:

Anzahl Clients x Anzahl Sitzungen pro Client x Anzahl während jeder Transaktion gespeicherter Dateien x pro Datei erforderlicher Protokollspeicherbereich

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Mehrere Clientsitzungen

| Element | Beispielwerte | Beschreibung |
|---------|---------------|--------------|
|---------|---------------|--------------|

| Element   | Beispielwerte        |                     | Beschreibung   |
|---|----------------------|---------------------|--|
| Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern | 300                  | 1000                | Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.  |
| Mögliche Sitzungen für jeden Client   | 3                    | 3                   | Die Einstellung der Clientoption RESOURCEUTILIZATION ist größer als der Standardwert. Jede Clientsitzung führt maximal drei Sitzungen parallel aus.  |
| Anzahl während jeder Transaktion gespeicherter Dateien  | 4096                 | 4096                | Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.  |
| Für jede Datei erforderlicher Protokollspeicherbereich  | 3053                 | 3053                | Der Wert von 3053 Byte für jede Datei in einer Transaktion gibt die Protokollbyte an, die erforderlich sind, wenn Dateien von einem Windows-Client gesichert werden, auf dem Dateinamen eine Länge von 12-120 Byte haben.<br><br>Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet. |
| Aktive Protokolldatei: vorgeschlagene Größe   | 26,5 GB <sup>1</sup> | 51 GB <sup>1</sup>  | Die folgende Berechnung wurde für 300 Clients ausgeführt. 1 Gigabyte entspricht 1.073.741.824 Byte.<br><br>(300 Clients x 3 Sitzungen pro Client x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 = 10,5 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>10,5 + 16 = 26,5 GB<br><br>Die folgende Berechnung wurde für 1000 Clients ausgeführt. 1 Gigabyte entspricht 1.073.741.824 Byte.<br><br>(1000 Clients x 3 Sitzungen pro Client x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 = 35 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>35 + 16 = 51 GB                       |
| Archivprotokoll: vorgeschlagene Größe   | 79,5 GB <sup>1</sup> | 153 GB <sup>1</sup> | Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, wird die Schätzung für die aktive Protokolldatei mit 3 multipliziert:<br><br>10,5 x 3 = 31,5 GB<br><br>35 x 3 = 105 GB<br><br>Erhöhen Sie diese Werte um die vorgeschlagene Anfangsgröße von 48 GB:<br><br>31,5 + 48 = 79,5 GB<br><br>105 + 48 = 153 GB  |

| Element   | Beispielwerte | Beschreibung |
|---|---------------|--------------|
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre aktive Protokolldatei und passen Sie die Größe, falls erforderlich, an.</p> |               |              |

## AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Operationen für gleichzeitiges Schreiben schätzen

Wenn Clientsicherungsoperationen Speicherpools verwenden, die für gleichzeitiges Schreiben konfiguriert sind, erhöht sich der Protokollspeicherbedarf, der für jede Datei erforderlich ist.

Der Protokollspeicherbereich, der für jede Datei erforderlich ist, erhöht sich um ungefähr 200 Byte für jeden Kopienspeicherpool, der für eine Operation für gleichzeitiges Schreiben verwendet wird. In dem Beispiel in der folgenden Tabelle werden Daten in einem primären Speicherpool und darüber hinaus in zwei Kopienspeicherpools gespeichert. Die geschätzte Protokollgröße erhöht sich für jede Datei um 400 Byte. Wenn Sie den vorgeschlagenen Wert von 3053 Byte Protokollspeicherbereich pro Datei verwenden, sind insgesamt 3453 Byte erforderlich.

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Operationen für gleichzeitiges Schreiben

| Element   | Beispielwerte      | Beschreibung  |
|---|--------------------|---|
| Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern | 300                | Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.   |
| Anzahl während jeder Transaktion gespeicherter Dateien  | 4096               | Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.   |
| Für jede Datei erforderlicher Protokollspeicherbereich  | 3453 Byte          | <p>3053 Byte plus 200 Byte für jeden Kopienspeicherpool.</p> <p>Der Wert von 3053 Byte für jede Datei in einer Transaktion stellt die Anzahl der Protokollbyte dar, die bei der Sicherung von Dateien auf einem Windows-Client benötigt werden, wo die Dateinamen 12 - 120 Byte haben.</p> <p>Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients für Sichern/Archivieren gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.</p> |
| Aktive Protokolldatei: vorgeschlagene Größe   | 20 GB <sup>1</sup> | <p>Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.</p> <p><math>(300 \text{ Clients} \times 4096 \text{ während jeder Transaktion gespeicherte Dateien} \times 3453 \text{ Byte pro Datei}) \div 1.073.741.824 \text{ Byte} = 4,0 \text{ GB}</math></p> <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>   |

| Element  | Beispielwerte      | Beschreibung   |
|--|--------------------|--|
| Archivprotokoll: vorgeschlagene Größe  | 60 GB <sup>1</sup> | <p>Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Speicherbedarf für das Archivprotokoll zu schätzen:</p> $4 \text{ GB} \times 3 = 12 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $12 + 48 = 60 \text{ GB}$ |
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |                    |  |

## AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen und Serveroperationen schätzen

Die Umlagerung von Daten in Serverspeicher, Identifikationsprozesse für die Dateneduplizierung, Wiederherstellung und Verfallsverarbeitung werden möglicherweise gleichzeitig mit Clientspeicheroperationen ausgeführt. Verwaltungstasks wie Verwaltungsbefehle oder SQL-Abfragen von Verwaltungsclients können ebenfalls gleichzeitig mit Clientspeicheroperationen ausgeführt werden. Serveroperationen und Verwaltungstasks, die gleichzeitig ausgeführt werden, können den erforderlichen Speicherbereich für die aktive Protokolldatei erhöhen.

Beispielsweise wird bei der Umlagerung von Dateien aus dem Speicherpool mit wahlfreiem Zugriff (DISK) in einem Plattenspeicherpool mit sequenziellem Zugriff (FILE) für jede Datei, die umgelagert wird, ungefähr 110 Byte Protokollspeicherbereich verwendet. Beispiel: Angenommen, es sind 300 Clients für Sichern/Archivieren vorhanden, von denen jeder 100.000 Dateien jede Nacht sichert. Die Dateien sind anfänglich in einem DISK-Speicherpool gespeichert und werden dann in einen FILE-Speicherpool umgelagert. Um die Größe des Speicherbereichs für die aktive Protokolldatei zu schätzen, die für die Datenumlagerung erforderlich ist, verwenden Sie die folgende Berechnung. Die Anzahl Clients in der Berechnung stellt die maximale Anzahl zu einem beliebigen Zeitpunkt dar, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern.

$300 \text{ Clients} \times 100.000 \text{ Dateien pro Client} \times 110 \text{ Byte} = 3,1 \text{ GB}$

Addieren Sie diesen Wert zu der Schätzung für die Größe der aktiven Protokolldatei, die für grundlegende Clientspeicheroperationen berechnet wurde.

## AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls unter Bedingungen mit extremen Abweichungen schätzen

Probleme in Bezug auf knapp werdenden Speicherbereich für die aktive Protokolldatei können auftreten, wenn viele Transaktionen, die sehr schnell ausgeführt werden, zusammen mit einigen Transaktionen vorhanden sind, deren Ausführung sehr viel länger dauern kann. Ein typischer Fall sind viele aktive Workstation- oder Dateiserversicherungssitzungen und wenige aktive Serversicherungssitzungen für sehr große Datenbanken. Trifft diese Situation für Ihre Umgebung zu, müssen Sie möglicherweise die Größe der aktiven Protokolldatei erhöhen, damit die Arbeit erfolgreich ausgeführt werden kann.

## AIX: Beispiel: Größe des Archivprotokolls bei Datenbankgesamtsicherungen schätzen

Der IBM Spectrum Protect-Server löscht nicht benötigte Dateien nur dann aus dem Archivprotokoll, wenn eine Datenbankgesamtsicherung ausgeführt wird. Demzufolge müssen Sie beim Schätzen des für das Archivprotokoll erforderlichen Speicherbereichs auch die Häufigkeit, mit der Datenbankgesamtsicherungen ausgeführt werden, berücksichtigen.

Wenn beispielsweise einmal pro Woche eine Datenbankgesamtsicherung ausgeführt wird, muss der Speicherbereich für das Archivprotokoll groß genug sein, um die Informationen einer vollständigen Woche im Archivprotokoll aufnehmen zu können.

Die unterschiedliche Größe des Archivprotokolls für täglich ausgeführte Datenbankgesamtsicherungen wird in dem Beispiel in der folgenden Tabelle gezeigt.

Tabelle 1. Datenbankgesamtsicherungen

| Element   | Beispielwerte       | Beschreibung  |
|---|---------------------|---|
| Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern | 300                 | Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.   |
| Anzahl während jeder Transaktion gespeicherter Dateien  | 4096                | Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.   |
| Für jede Datei erforderlicher Protokollspeicherbereich  | 3453 Byte           | 3053 Byte für jede Datei plus 200 Byte für jeden Kopienspeicherpool.<br><br>Der Wert von 3053 Byte für jede Datei in einer Transaktion stellt die Anzahl der Protokollbyte dar, die bei der Sicherung von Dateien auf einem Windows-Client benötigt werden, wo die Dateinamen 12 - 120 Byte haben.<br><br>Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet. |
| Aktive Protokolldatei: vorgeschlagene Größe   | 20 GB <sup>1</sup>  | Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.<br><br>(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3453 Byte pro Datei) ÷ 1.073.741.824 Byte = 4,0 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>4 + 16 = 20 GB   |
| Archivprotokoll: vorgeschlagene Größe bei einer Datenbankgesamtsicherung pro Tag  | 60 GB <sup>1</sup>  | Aufgrund der Voraussetzung, dass Archivprotokolle über drei Sicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen:<br><br>4 GB x 3 = 12 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:<br><br>12 + 48 = 60 GB   |
| Archivprotokoll: vorgeschlagene Größe bei einer Datenbankgesamtsicherung pro Woche                                      | 132 GB <sup>1</sup> | Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen. Multiplizieren Sie das Ergebnis mit der Anzahl Tage, die zwischen Datenbankgesamtsicherungen liegen.<br><br>(4 GB x 3 ) x 7 = 84 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:<br><br>84 + 48 = 132 GB   |

| Element  | Beispielwerte | Beschreibung |
|--|---------------|--------------|
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Anfangsgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |               |              |

## AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Dateneduplizierungsoperationen schätzen

Wenn Sie Daten deduplizieren, müssen Sie die Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll berücksichtigen.

Die folgenden Faktoren haben Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll:

### Volumen der deduplizierten Daten

Welche Auswirkungen die Dateneduplizierung auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll hat, ist von dem Prozentsatz an Daten abhängig, der für die Deduplizierung auswählbar ist. Ist der Prozentsatz an Daten, die dedupliziert werden können, relativ hoch, ist mehr Protokollspeicherbereich erforderlich.

### Größe und Anzahl Speicherbereiche

Für jeden Speicherbereich, der durch einen Prozess zum Identifizieren doppelter Daten identifiziert wird, sind ungefähr 1.500 Byte Speicherbereich für die aktive Protokolldatei erforderlich. Werden beispielsweise 250.000 Speicherbereiche durch einen erkennen identifiziert, beträgt die geschätzte Größe der aktiven Protokolldatei 358 MB:

```
250.000 während jedes Prozesses ermittelte Speicherbereiche x 1.500 Byte
für jeden Speicherbereich = 358 MB
```

Betrachten Sie das folgende Szenario. 300 Clients für Sichern/Archivieren sichern jede Nacht bis zu 100.000 Dateien. Diese Aktivität hat eine Last von 30.000.000 Dateien zur Folge. Die durchschnittliche Anzahl Speicherbereiche für jede Datei ist 2. Demzufolge beträgt die Gesamtzahl Speicherbereiche 60.000.000 und der Speicherbedarf für das Archivprotokoll 84 GB:

```
60.000.000 Speicherbereiche x 1.500 Byte pro Speicherbereich = 84 GB
```

Ein Prozess zum Identifizieren doppelter Daten wird für Aggregate von Dateien ausgeführt. Ein Aggregat besteht aus Dateien, die in einer bestimmten Transaktion gespeichert sind, wie durch die Serveroption TXNGROUPMAX angegeben. Angenommen, die Serveroption TXNGROUPMAX ist auf den Standardwert 4096 gesetzt. Wenn die durchschnittliche Anzahl Speicherbereiche für jede Datei 2 beträgt, ist die Gesamtzahl Speicherbereiche in jedem Aggregat 8192 und der für die aktive Protokolldatei erforderliche Speicherbedarf 12 MB:

```
8192 Speicherbereiche in jedem Aggregat x 1500 Byte pro Speicherbereich =
12 MB
```

### Timing und Anzahl der Prozesse zum Identifizieren doppelter Daten

Das Timing und die Anzahl Prozesse zum Identifizieren doppelter Daten haben ebenfalls Auswirkungen auf die Größe der aktiven Protokolldatei. Bei Verwendung der in dem vorhergehenden Beispiel berechneten Größe der aktiven Protokolldatei von 12 MB beträgt die gleichzeitige Last für die aktive Protokolldatei 120 MB, wenn 10 Prozesse zum Identifizieren doppelter Daten parallel ausgeführt werden:

```
12 MB pro Prozess x 10 Prozesse = 120 MB
```

### Dateigröße

Große Dateien, die für die Identifizierung doppelter Daten verarbeitet werden, können ebenfalls Auswirkungen auf die Größe der aktiven Protokolldatei haben. Beispiel: Angenommen, ein Client für Sichern/Archivieren sichert ein Dateisystemimage mit einer Größe von 80 GB. Die Anzahl doppelter Speicherbereiche für dieses Objekt kann groß sein, wenn beispielsweise die in das Dateisystemimage eingeschlossenen Dateien mit Teilsicherungen gesichert wurden. Beispiel: Angenommen, ein Dateisystemimage hat 1,2 Millionen doppelte Speicherbereiche. Die 1,2 Millionen Speicherbereiche in dieser großen Datei stellen eine einzige Transaktion für einen Prozess zum Identifizieren doppelter Daten dar. Der Gesamtspeicherbereich in der aktiven Protokolldatei, der für dieses einzelne Objekt erforderlich ist, beträgt 1,7 GB:

```
1.200.000 Speicherbereich x 1.500 Byte pro Speicherbereich = 1,7 GB
```

Wenn andere, kleinere Prozesse zum Identifizieren doppelter Daten zu demselben Zeitpunkt ausgeführt werden wie der Prozess zum Identifizieren doppelter Daten für ein einzelnes großes Objekt, ist in der aktiven Protokolldatei möglicherweise nicht

genügend Speicherbereich verfügbar. Beispiel: Angenommen, ein Speicherpool ist für die Deduplizierung aktiviert. Der Speicherpool enthält gemischte Daten, einschließlich vieler relativ kleiner Dateien mit einer Größe von 10 KB bis zu mehreren hundert KB. Der Speicherpool enthält außerdem einige wenige große Objekte mit einem hohen Prozentsatz an doppelten Speicherbereichen.

Um nicht nur den Speicherbedarf zu berücksichtigen, sondern auch das Timing und die Dauer gleichzeitig ablaufender Transaktionen, erhöhen Sie die geschätzte Größe der aktiven Protokolldatei um den Faktor 2. Beispiel: Angenommen, das Ergebnis Ihrer Berechnungen für den Speicherbedarf lautet 25 GB (23,3 GB + 1,7 GB für die Deduplizierung eines großen Objekts). Wenn Deduplizierungsverarbeitung gleichzeitig ausgeführt werden, beträgt die vorgeschlagene Größe der aktiven Protokolldatei 50 GB. Die vorgeschlagene Größe des Archivprotokolls ist 150 GB.

Die Beispiele in den folgenden Tabellen zeigen Berechnungen für aktive Protokolldateien und Archivprotokolle. In dem Beispiel in der ersten Tabelle wird eine durchschnittliche Größe von 700 KB für Speicherbereiche verwendet. In dem Beispiel in der zweiten Tabelle wird eine durchschnittliche Größe von 256 KB verwendet. Wie den Beispielen zu entnehmen ist, zeigt die durchschnittliche Größe doppelter Speicherbereiche von 256 KB eine größere geschätzte Größe für die aktive Protokolldatei an. Um betriebsbezogene Probleme für den Server auf ein Mindestmaß zu reduzieren oder zu verhindern, verwenden Sie 256 KB für die Schätzung der Größe der aktiven Protokolldatei in Ihrer Produktionsumgebung.

Tabelle 1. Durchschnittliche Größe doppelter Speicherbereiche von 700 KB

| Element  | Beispielwerte |               | Beschreibung   |
|--|---------------|---------------|--|
| Größe des größten zu deduplizierenden Objekts  | 800 GB        | 4 TB          | Die Granularität der Verarbeitung für die Deduplizierung bezieht sich auf die Dateiebene. Demzufolge stellt die größte einzelne zu deduplizierende Datei die umfangreichste Transaktion und eine entsprechend hohe Last für die aktive Protokolldatei und das Archivprotokoll dar.   |
| Durchschnittliche Größe der Speicherbereiche   | 700 KB        | 700 KB        | Die Deduplizierungsalgorithmen verwenden eine variable Blockmethode. Nicht alle deduplizierten Speicherbereiche für eine bestimmte Datei haben dieselbe Größe, daher wird bei dieser Berechnung eine durchschnittliche Speicherbereichsgröße vorausgesetzt.  |
| Speicherbereiche für eine bestimmte Datei  | 1.198.372 Bit | 6.135.667 Bit | Bei Verwendung der durchschnittlichen Speicherbereichsgröße (700 KB), geben diese Berechnungen die Gesamtzahl Speicherbereiche für ein bestimmtes Objekt an.<br><br>Die folgende Berechnung wurde für ein Objekt mit einer Größe von 800 GB ausgeführt: $(800 \text{ GB} \div 700 \text{ KB}) = 1.198.372 \text{ Bit}$<br><br>Die folgende Berechnung wurde für ein Objekt mit einer Größe von 4 TB ausgeführt: $(4 \text{ TB} \div 700 \text{ KB}) = 6.135.667 \text{ Bit}$ |
| Aktive Protokolldatei: vorgeschlagene Größe, die für die Deduplizierung eines einzelnen großen Objekts während eines einzelnen Prozesses zum Identifizieren doppelter Daten erforderlich ist | 1,7 GB        | 8,6 GB        | Der geschätzte Speicherbereich für die aktive Protokolldatei, der für diese Transaktion benötigt wird.   |



| Element  | Beispielwerte       |                       | Beschreibung  |
|--|---------------------|-----------------------|---|
| Aktive Protokolldatei:<br>vorgeschlagene<br>Gesamtgröße  | 66 GB <sup>1</sup>  | 79,8 GB <sup>1</sup>  | <p>Multiplizieren Sie, nachdem zusätzlich zur Deduplizierung andere Aspekte der Last auf dem Server berücksichtigt wurden, die vorhandene Schätzung mit dem Faktor 2. In diesen Beispielen wird der zum Deduplizieren eines einzelnen großen Objekts erforderliche Speicherbereich für die aktive Protokolldatei im Zusammenhang mit den vorherigen Schätzungen für die erforderliche Größe der aktiven Protokolldatei betrachtet.</p> <p>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:</p> $(23,3 \text{ GB} + 1,7 \text{ GB}) \times 2 = 50 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:</p> $50 + 16 = 66 \text{ GB}$ <p>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:</p> $(23,3 \text{ GB} + 8,6 \text{ GB}) \times 2 = 63,8 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:</p> $63,8 + 16 = 79,8 \text{ GB}$ |
| Archivprotokoll:<br>vorgeschlagene<br>Größe  | 198 GB <sup>1</sup> | 239,4 GB <sup>1</sup> | <p>Multiplizieren Sie die geschätzte Größe der aktiven Protokolldatei mit dem Faktor 3.</p> <p>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:</p> $50 \text{ GB} \times 3 = 150 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $150 + 48 = 198 \text{ GB}$ <p>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:</p> $63,8 \text{ GB} \times 3 = 191,4 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $191,4 + 48 = 239,4 \text{ GB}$  |
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die die Deduplizierung verwendet, ist 32 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die die Deduplizierung verwendet, ist 96 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 32 GB bzw. 96 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |                     |                       |   |

Tabelle 2. Durchschnittliche Größe doppelter Speicherbereiche von 256 KB

| Element   | Beispielwerte |      | Beschreibung  |
|---|---------------|------|---|
| Größe des größten zu<br>deduplizierenden<br>Objekts | 800 GB        | 4 TB | <p>Die Granularität der Verarbeitung für die Deduplizierung bezieht sich auf die Dateiebene. Demzufolge stellt die größte einzelne zu deduplizierende Datei die umfangreichste Transaktion und eine entsprechend hohe Last für die aktive Protokolldatei und das Archivprotokoll dar.</p> |

| Element  | Beispielwerte        |                       | Beschreibung   |
|--|----------------------|-----------------------|--|
| Durchschnittliche Größe der Speicherbereiche   | 256 KB               | 256 KB                | Die Deduplizierungsalgorithmen verwenden eine variable Blockmethode. Nicht alle deduplizierten Speicherbereiche für eine bestimmte Datei haben dieselbe Größe, daher wird bei dieser Berechnung eine durchschnittliche Speicherbereichsgröße vorausgesetzt.  |
| Speicherbereiche für eine bestimmte Datei  | 3.276.800 Bit        | 16.777.216 Bit        | Bei Verwendung der durchschnittlichen Speicherbereichsgröße, geben diese Berechnungen die Gesamtzahl Speicherbereiche für ein bestimmtes Objekt an.<br><br>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:<br><br>$(800 \text{ GB} \div 256 \text{ KB}) = 3.276.800 \text{ Bit}$<br><br>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:<br><br>$(4 \text{ TB} \div 256 \text{ KB}) = 16.777.216 \text{ Bit}$  |
| Aktive Protokolldatei: vorgeschlagene Größe, die für die Deduplizierung eines einzelnen großen Objekts während eines einzelnen Prozesses zum Identifizieren doppelter Daten erforderlich ist | 4,5 GB               | 23,4 GB               | Die geschätzte Größe des Speicherbereichs für die aktive Protokolldatei, die für diese Transaktion erforderlich ist.   |
| Aktive Protokolldatei: vorgeschlagene Gesamtgröße  | 71,6 GB <sup>1</sup> | 109,4 GB <sup>1</sup> | Nachdem Sie neben der Deduplizierung andere Aspekte der Serverauslastung mit berücksichtigt haben, multiplizieren Sie die vorhandene Schätzung mit dem Faktor 2. In diesen Beispielen wird der zum Deduplizieren eines einzelnen großen Objekts erforderliche Speicherbereich für die aktive Protokolldatei im Zusammenhang mit den vorherigen Schätzungen für die erforderliche Größe der aktiven Protokolldatei betrachtet.<br><br>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:<br><br>$(23,3 \text{ GB} + 4,5 \text{ GB}) \times 2 = 55,6 \text{ GB}$<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>$55,6 + 16 = 71,6 \text{ GB}$<br><br>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:<br><br>$(23,3 \text{ GB} + 23,4 \text{ GB}) \times 2 = 93,4 \text{ GB}$<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>$93,4 + 16 = 109,4 \text{ GB}$ |

| Element  | Beispielwerte         |                       | Beschreibung   |
|--|-----------------------|-----------------------|--|
| Archivprotokoll:<br>vorgeschlagene<br>Größe  | 214,8 GB <sup>1</sup> | 328,2 GB <sup>1</sup> | <p>Die geschätzte Größe der aktiven Protokolldatei multipliziert mit dem Faktor 3.</p> <p>Die folgende Berechnung wurde für ein Objekt mit einer Größe von 800 GB ausgeführt:</p> $55,6 \text{ GB} \times 3 = 166,8 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $166,8 + 48 = 214,8 \text{ GB}$ <p>Die folgende Berechnung wurde für ein Objekt mit einer Größe von 4 TB ausgeführt:</p> $93,4 \text{ GB} \times 3 = 280,2 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $280,2 + 48 = 328,2 \text{ GB}$ |
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die die Deduplizierung verwendet, ist 32 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die die Deduplizierung verwendet, ist 96 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 32 GB bzw. 96 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |                       |                       |  |

## AIX: Speicherbereich des Spiegels für aktive Protokolldateien

Die aktive Protokolldatei kann gespiegelt werden, sodass die gespiegelte Kopie verwendet werden kann, falls die aktiven Protokolldateien nicht gelesen werden können. Es kann nur ein einziger Spiegel der aktiven Protokolldatei vorhanden sein.

Die Erstellung einer Protokollspiegel ist eine vorgeschlagene Option. Wenn Sie die aktive Protokolldatei vergrößern, wird der Protokollspiegel automatisch vergrößert. Die Spiegelung des Protokolls kann sich negativ auf die Leistung auswirken, da die doppelte E/A-Aktivität erforderlich ist, um den Spiegel zu verwalten. Der zusätzliche Speicherbereich, den der Protokollspiegel benötigt, ist ein weiterer Faktor, der bei der Entscheidung über die Erstellung eines Protokollspiegels berücksichtigt werden muss.

Wenn das Spiegelprotokollverzeichnis voll wird, gibt der Server Fehlernachrichten in das Aktivitätenprotokoll und in die Datei db2diag.log aus. Die Serveraktivität wird fortgesetzt.

## AIX: Speicherbereich des Übernahmeverzeichnis für Archivprotokolle

Das Übernahmeverzeichnis für Archivprotokolle wird vom Server verwendet, wenn der Speicherbereich des Verzeichnisses für Archivprotokolle nicht mehr ausreicht.

Durch Angabe eines Übernahmezeichnisses für Archivprotokolle können Probleme verhindert werden, die auftreten, wenn der Speicherbereich der Archivprotokolldatei nicht mehr ausreicht. Wenn sowohl das Verzeichnis für Archivprotokolle als auch das Laufwerk oder das Dateisystem, in dem sich das Übernahmeverzeichnis für Archivprotokolle befindet, voll wird, bleiben die Daten im Verzeichnis für aktive Protokolldateien. Dadurch kann die aktive Protokolldatei vollständig ausgefüllt werden, was einen Serverhalt verursacht.

## AIX: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen

Um den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei zu bestimmen, geben Sie den Befehl QUERY LOG ein. Um die Speicherauslastung in der Datenbank und den Wiederherstellungsprotokollen zu überwachen, können Sie auch das Aktivitätenprotokoll auf Nachrichten überprüfen.

### Aktive Protokolldatei

Wenn der verfügbare Speicherbereich für die aktive Protokolldatei zu gering ist, werden die folgenden Nachrichten im Aktivitätenprotokoll angezeigt:

**ANR4531I: IC\_AUTOBACKUP\_LOG\_USED\_SINCE\_LAST\_BACKUP\_TRIGGER**

Diese Nachricht wird angezeigt, wenn der Speicherbereich für die aktive Protokolldatei die angegebene maximale Größe überschreitet. Der IBM Spectrum Protect-Server startet eine Datenbankgesamticherung.

Um die maximale Protokollgröße zu ändern, stoppen Sie den Server. Öffnen Sie die Datei dmserv.opt und geben Sie für die Option ACTIVELOGSIZE einen neuen Wert an. Starten Sie anschließend den Server erneut.

**ANR0297I: IC\_BACKUP\_NEEDED\_LOG\_USED\_SINCE\_LAST\_BACKUP**

Diese Nachricht wird angezeigt, wenn der Speicherbereich für die aktive Protokolldatei die angegebene maximale Größe überschreitet. Sie müssen die Datenbank manuell sichern.

Um die maximale Protokollgröße zu ändern, stoppen Sie den Server. Öffnen Sie die Datei dmserv.opt und geben Sie für die Option ACTIVELOGSIZE einen neuen Wert an. Starten Sie anschließend den Server erneut.

**ANR4529I: IC\_AUTOBACKUP\_LOG\_UTILIZATION\_TRIGGER**

Das Verhältnis des belegten Speicherbereichs für die aktive Protokolldatei zum verfügbaren Speicherbereich für die aktive Protokolldatei überschreitet den Schwellenwert für die Protokollauslastung. Wenn mindestens eine einzige Datenbankgesamticherung ausgeführt wurde, startet der IBM Spectrum Protect-Server eine Teilsicherung der Datenbank. Andernfalls startet der Server eine Datenbankgesamticherung.

**ANR0295I: IC\_BACKUP\_NEEDED\_LOG\_UTILIZATION**

Das Verhältnis des belegten Speicherbereichs für die aktive Protokolldatei zum verfügbaren Speicherbereich für die aktive Protokolldatei überschreitet den Schwellenwert für die Protokollauslastung. Sie müssen die Datenbank manuell sichern.

## Archivprotokoll

---

Wenn der verfügbare Speicherbereich für das Archivprotokoll zu gering ist, wird die folgende Nachricht im Aktivitätenprotokoll angezeigt:

**ANR0299I: IC\_BACKUP\_NEEDED\_ARCHLOG\_USED**

Das Verhältnis des belegten Speicherbereichs für das Archivprotokoll zum verfügbaren Speicherbereich für das Archivprotokoll überschreitet den Schwellenwert für die Protokollauslastung. Der IBM Spectrum Protect-Server startet eine automatische Datenbankgesamticherung.

## Datenbank

---

Wenn der verfügbare Speicherbereich für Datenbankaktivitäten zu gering ist, wird die folgende Nachricht im Aktivitätenprotokoll angezeigt:

**ANR2992W: IC\_LOG\_FILE\_SYSTEM\_UTILIZATION\_WARNING\_2**

Der belegte Speicherplatz in der Datenbank überschreitet den Schwellenwert für die Belegung des Speicherplatzes in der Datenbank. Um den Speicherplatz für die Datenbank zu vergrößern, verwenden Sie den Befehl EXTEND DBSPACE oder das Dienstprogramm DSMSERV FORMAT mit dem Parameter DBDIR.

**ANR1546W: FILESYSTEM\_DBPATH\_LESS\_1GB**

Der verfügbare Speicherbereich in dem Verzeichnis, in dem sich die Serverdatenbankdateien befinden, beträgt weniger als 1 GB.

Wenn ein IBM Spectrum Protect-Server mit dem Dienstprogramm DSMSERV FORMAT oder dem Konfigurationsassistenten erstellt wird, werden auch eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien erstellt, in denen Datenbankinformationen gespeichert werden sollen, die vom Datenbankmanager verwendet werden. Der in dieser Nachricht angegebene Pfad gibt die Speicherposition der Datenbankinformationen an, die vom Datenbankmanager verwendet werden. Ist in dem Pfad kein Speicherbereich verfügbar, ist der Server nicht mehr funktionsfähig.

Sie müssen dem Dateisystem Speicherbereich hinzufügen oder in dem Dateisystem oder auf der Platte Speicherbereich freigeben.

## AIX: Rollbackdateien der Installation löschen

---

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, löschen, um Speicherplatz im Verzeichnis für gemeinsam genutzte Ressourcen freizugeben. Zu den Dateitypen, die Sie löschen können, gehören z. B. Dateien, die für eine Rollbackoperation benötigt wurden.

## Informationen zu diesem Vorgang

---

Zum Löschen der nicht mehr benötigten Dateien verwenden Sie den grafisch orientierten Installationsassistenten oder die Befehlszeile im Konsolenmodus.

- AIX: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen  
Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der IBM® Installation Manager-Benutzerschnittstelle löschen.
- AIX: Rollbackdateien für die Installation mit der Befehlszeile löschen  
Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der Befehlszeile löschen.

## AIX: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen

---

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der IBM® Installation Manager-Benutzerschnittstelle löschen.

### Vorgehensweise

---

1. Öffnen Sie IBM Installation Manager.  
 In dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das Unterverzeichnis eclipse (z. B. /opt/IBM/InstallationManager/eclipse) und geben Sie folgenden Befehl aus, um IBM Installation Manager zu starten:  

```
./IBMIM
```
2. Klicken Sie auf Datei > Benutzervorgaben.
3. Wählen Sie Dateien für Rollback aus.
4. Klicken Sie auf Gespeicherte Dateien löschen und dann auf OK.

## AIX: Rollbackdateien für die Installation mit der Befehlszeile löschen

---

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der Befehlszeile löschen.

### Vorgehensweise

---

1. In dem Verzeichnis, in dem IBM® Installation Manager installiert ist, wechseln Sie in das folgende Unterverzeichnis:
  -  AIX-Betriebssysteme/eclipse/tools
 Beispiel:
  -  AIX-Betriebssysteme/opt/IBM/InstallationManager/eclipse/tools
2. Geben Sie im Verzeichnis tools den folgenden Befehl aus, um eine IBM Installation Manager-Befehlszeile zu starten:
  -  AIX-Betriebssysteme./imcl -c
3. Geben Sie P ein, um Benutzervorgaben auszuwählen.
4. Geben Sie 3 ein, um Dateien für Rollback auszuwählen.
5. Geben Sie D ein, um die Dateien für Rollback zu löschen.
6. Geben Sie A ein, um die Änderungen anzuwenden und zum Benutzervorgabenmenü zurückzukehren.
7. Geben Sie C ein, um das Benutzervorgabenmenü zu verlassen.
8. Geben Sie X ein, um Installation Manager zu beenden.

## AIX: Empfehlungen für die Serverbenennung

---

Verwenden Sie diese Beschreibungen als Referenz bei der Installation oder beim Upgrade eines IBM Spectrum Protect-Servers.

### Instanzenbenutzer-ID

---

Die Instanzbenutzer-ID wird als Basis für andere Namen verwendet, die sich auf die Serverinstanz beziehen. Die Instanzbenutzer-ID wird auch als Instanzeigner bezeichnet.

Zum Beispiel: tsminst1

Die Instanzbenutzer-ID ist die Benutzer-ID, die über das Eigentumsrecht oder über Schreib-/Lesezugriffsberechtigung für alle Verzeichnisse verfügen muss, die Sie für die Datenbank und das Wiederherstellungsprotokoll erstellen. Der Server wird standardmäßig mit der Instanzbenutzer-ID ausgeführt. Diese Benutzer-ID benötigt außerdem Schreib-/Lesezugriff für die Verzeichnisse, die für die Einheitenklasse FILE verwendet werden.

## Ausgangsverzeichnis für die Instanzbenutzer-ID

---

Das Ausgangsverzeichnis kann während der Erstellung der Instanzbenutzer-ID erstellt werden. Hierfür wird die Option für die Erstellung eines Ausgangsverzeichnisses (-m) verwendet, falls es noch nicht vorhanden ist. Abhängig von den lokalen Einstellungen kann das Verzeichnis folgendes Format haben: `/home/Instanzbenutzer-ID`

Zum Beispiel: `/home/tsminst1`

Das Ausgangsverzeichnis dient hauptsächlich zur Aufbewahrung des Profils für die Benutzer-ID und für Sicherheitseinstellungen.

## Datenbankinstanzname

---

Der Datenbankinstanzname muss mit der Instanzbenutzer-ID identisch sein, mit der Sie die Serverinstanz ausführen.

Zum Beispiel: `tsminst1`

## Instanzverzeichnis

---

Das Instanzverzeichnis enthält spezielle Dateien für eine Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien). Es kann einen beliebigen Namen haben. Um die Identifizierung zu erleichtern, sollten Sie einen Namen verwenden, der das Verzeichnis mit dem Instanznamen verknüpft.

Sie können das Instanzverzeichnis als Unterverzeichnis des Ausgangsverzeichnisses für die Instanzbenutzer-ID erstellen. Zum Beispiel: `/home/Instanzbenutzer-ID/Instanzbenutzer-ID`

Im folgenden Beispiel befindet sich das Instanzverzeichnis im Ausgangsverzeichnis der Benutzer-ID `tsminst1`:  
`/home/tsminst1/tsminst1`

Sie können das Verzeichnis auch an einer anderen Position erstellen, zum Beispiel: `/tsmserver/tsminst1`

Im Instanzverzeichnis sind folgende Dateien für die Serverinstanz gespeichert:

- Serveroptionsdatei `dsmserv.opt`
- Die Serverschlüsseldatenbankdatei `cert.kdb` und die `.arm`-Dateien (werden von Clients und anderen Servern zum Importieren der Secure Sockets Layer-Zertifikate des Servers verwendet)
- Einheitenkonfigurationsdatei, wenn die Serveroption `DEVCONFIG` keinen vollständig qualifizierten Namen angibt
- Protokolldatei für Datenträger, wenn die Serveroption `VOLUMEHISTORY` keinen vollständig qualifizierten Namen angibt
- Datenträger für Speicherpools mit dem Typ `DEVTYPE=FILE`, wenn das Verzeichnis für die Einheitenklasse nicht vollständig angegeben oder nicht vollständig qualifiziert ist
- Benutzerexits
- Traceausgabe (wenn nicht vollständig qualifiziert)

## Datenbankname


---

Der Datenbankname lautet für jede Serverinstanz immer `TSMDB1`. Dieser Name kann nicht geändert werden.

## Servername


---

Der Servername ist ein interner Name für IBM Spectrum Protect und wird für Operationen verwendet, bei denen eine Datenübertragung zwischen mehreren IBM Spectrum Protect-Servern auftritt. Zum Beispiel bei der Kommunikation zwischen Servern und bei der gemeinsamen Nutzung von Speicherarchiven.

 Der Servername wird auch verwendet, wenn Sie den Server dem Operations Center hinzufügen, so dass er mit dieser Schnittstelle verwaltet werden kann. Verwenden Sie einen eindeutigen Namen für jeden Server. Verwenden Sie einen Namen, der die Position oder den Zweck des Servers angibt, um die Identifikation im Operations Center (oder mit einem Befehl `QUERY SERVER`) zu erleichtern. Nachdem ein IBM Spectrum Protect-Server als Hub- oder Peripherieserver konfiguriert wurde, dürfen Sie seinen Namen nicht mehr ändern.

Wenn Sie den Assistenten verwenden, wird als Standardname der Hostname des von Ihnen verwendeten Systems vorgeschlagen. Sie können einen anderen, für Ihre Umgebung aussagekräftigen Namen verwenden. Befinden sich mehrere Server auf dem System, können

Sie bei Verwendung des Assistenten den Standardnamen nur für einen der Server angeben. Sie müssen einen eindeutigen Namen für jeden Server eingeben.

 AIX-Betriebssysteme Zum Beispiel:

- LOHNBUCHHALTUNG
- VERTRIEB

## Verzeichnisse für Datenbankbereich und Wiederherstellungsprotokoll

---

Die Verzeichnisse können gemäß den lokalen Vorgaben benannt werden. Sie sollten Namen verwenden, die die Verzeichnisse mit der Serverinstanz verknüpfen, um die Identifikation zu erleichtern.

Beispiel für das Archivprotokoll:

-  AIX-Betriebssysteme/tsminst1\_archlog

## AIX: Installationsverzeichnisse

---

Zu den Installationsverzeichnissen für den IBM Spectrum Protect-Server gehören die Verzeichnisse für den Server, DB2, die Einheiten, die Sprache und andere Verzeichnisse. Jedes Verzeichnis enthält mehrere zusätzliche Verzeichnisse.

Das Verzeichnis `/opt/tivoli/tsm/server/bin` ist das Standardverzeichnis, das den Servercode und die Lizenzierung enthält.

Das während der Installation des IBM Spectrum Protect-Servers installierte DB2-Produkt hat die in den DB2-Informationsquellen dokumentierte Verzeichnisstruktur. Schützen Sie diese Verzeichnisse und Dateien wie die Serververzeichnisse. Das Standardverzeichnis heißt `/opt/tivoli/tsm/db2`.

Sie können folgende Sprachen verwenden: Englisch (US), Deutsch, Französisch, Italienisch, Spanisch, Portugiesisch (Brasilien), Koreanisch, Japanisch, traditionelles Chinesisch, vereinfachtes Chinesisch, Chinesisch GBK, Chinesisch Big5 und Russisch.

## AIX: Serverkomponenten installieren

---

Für die Installation der Serverkomponenten der Version 8.1.3 können Sie den Installationsassistenten, die Befehlszeile im Konsolenmodus oder den unbeaufsichtigten Modus verwenden.

### Informationen zu diesem Vorgang

---

Mithilfe der IBM Spectrum Protect-Installationssoftware können Sie die folgenden Komponenten installieren:

- Server  
Tipp: Die Datenbank (DB2), Global Security Kit (GSKit) und IBM® Java™ Runtime Environment (JRE) werden automatisch installiert, wenn Sie die Serverkomponente auswählen.
- Sprachen des Servers
- Lizenz
- Einheiten
- IBM Spectrum Protect for SAN
- Operations Center

 AIX-Betriebssysteme Für die Installation eines Servers der Version 8.1.3 anhand dieses Leitfadens müssen Sie 30 - 45 Minuten einplanen.

- AIX: Installationspaket abrufen  
Das Installationspaket für IBM Spectrum Protect kann von einer IBM Download-Site heruntergeladen werden, z. B. von Passport Advantage oder IBM Fix Central.
- AIX: IBM Spectrum Protect mit dem Installationsassistenten installieren  
Sie können den Server mit dem grafisch orientierten Assistenten von IBM Installation Manager installieren.
- AIX: IBM Spectrum Protect im Konsolenmodus installieren  
Sie können IBM Spectrum Protect mithilfe der Befehlszeile im Konsolenmodus installieren.
- AIX: IBM Spectrum Protect im unbeaufsichtigten Modus installieren  
Sie können den Server im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlernachrichten in Protokolldateien gespeichert.
- AIX: Serversprachenpakete installieren  
Übersetzungen für den Server ermöglichen das Anzeigen von Nachrichten und Hilfetext auf dem Server in verschiedenen

Sprachen. Die Übersetzungen gestatten auch die Verwendung länderspezifischer Einstellungen für das Datums-, Uhrzeit- und Zahlenformat.

## AIX: Installationspaket abrufen

---

Das Installationspaket für IBM Spectrum Protect kann von einer IBM® Download-Site heruntergeladen werden, z. B. von Passport Advantage oder IBM Fix Central.

 AIX-Betriebssysteme

### Vorbereitende Schritte

---

Wenn Sie die Dateien herunterladen wollen, legen Sie als Systembenutzergrenzwert für die maximale Dateigröße 'unlimited' (unbegrenzt) fest, um sicherzustellen, dass die Dateien ordnungsgemäß heruntergeladen werden können:

1. Geben Sie den folgenden Befehl aus, um den Wert für die maximale Dateigröße abzufragen:

```
ulimit -Hf
```

2. Wenn als Systembenutzergrenzwert für die maximale Dateigröße nicht 'unlimited' (unbegrenzt) angegeben ist, geben Sie 'unlimited' gemäß den Anweisungen in der Dokumentation Ihres Betriebssystems an.

### Vorgehensweise

---

1. Laden Sie die entsprechende Paketdatei von einer der folgenden Websites herunter:
  - Laden Sie das Serverpaket aus Passport Advantage oder Fix Central herunter.
  - Die neuesten Informationen, Aktualisierungen und Fixes finden Sie im IBM Support Portal.
2. Gehen Sie wie folgt vor, wenn Sie das Paket von einer IBM Download-Site heruntergeladen haben:
  - a. Überprüfen Sie, ob genug Speicherbereich zum Speichern der Installationsdateien nach dem Extrahieren aus dem Produktpaket vorhanden ist. Informationen zum Speicherplatzbedarf finden Sie im Downloaddokument:
    - IBM Spectrum Protect Technote 4042944
    - IBM Spectrum Protect Extended Edition Technote 4042945
    - IBM Spectrum Protect for Data Retention Technote 4042946
  - b. Laden Sie die Paketdatei in ein beliebiges Verzeichnis herunter. Der Pfad darf maximal 128 Zeichen enthalten. Sie müssen die Installationsdateien in ein leeres Verzeichnis extrahieren. Verwenden Sie kein Verzeichnis, das bereits extrahierte Dateien oder andere Dateien enthält.
  - c. Stellen Sie sicher, dass die Berechtigung zur Ausführung für das Paket definiert ist. Bei Bedarf können Sie die Dateiberechtigungen mit dem folgenden Befehl ändern:

```
chmod a+x Paketname.bin
```

- d. Geben Sie den folgenden Befehl aus, um das Paket zu extrahieren:

```
./Paketname.bin
```

*Paketname* ist der Name der heruntergeladenen Datei. Zum Beispiel:

 AIX-Betriebssysteme

```
8.1.x.000-IBM-SPSRV-AIX.bin
```

3.  AIX-Betriebssysteme Stellen Sie sicher, dass der folgende Befehl aktiviert ist, damit die IBM Spectrum Protect-Assistenten ordnungsgemäß funktionieren:
  -  AIX-Betriebssysteme `lsuser`Der Befehl ist standardmäßig aktiviert.
4. Wählen Sie eine der folgenden Methoden für die Installation von IBM Spectrum Protect aus:
  - AIX: IBM Spectrum Protect mit dem Installationsassistenten installieren
  - AIX: IBM Spectrum Protect im Konsolenmodus installieren
  - AIX: IBM Spectrum Protect im unbeaufsichtigten Modus installieren
5. Nachdem Sie IBM Spectrum Protect installiert haben und bevor Sie IBM Spectrum Protect für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Support and downloads und legen Sie alle gültigen Fixes an.

## AIX: IBM Spectrum Protect mit dem Installationsassistenten installieren


---

Sie können den Server mit dem grafisch orientierten Assistenten von IBM® Installation Manager installieren.




## Vorbereitende Schritte

Führen Sie vor dem Start der Installation die folgenden Schritte aus:

-  Wenn die folgenden RPM-Dateien in Ihrem System nicht installiert sind, müssen Sie sie installieren. Anweisungen finden Sie in RPM-Dateien für den grafisch orientierten Assistenten installieren.
  - atk-1.12.3-2.aix5.2.ppc.rpm
  - cairo-1.8.8-1.aix5.2.ppc.rpm
  - expat-2.0.1-1.aix5.2.ppc.rpm
  - fontconfig-2.4.2-1.aix5.2.ppc.rpm
  - freetype2-2.3.9-1.aix5.2.ppc.rpm
  - gettext-0.10.40-6.aix5.1.ppc.rpm
  - glib2-2.12.4-2.aix5.2.ppc.rpm
  - gtk2-2.10.6-4.aix5.2.ppc.rpm
  - libjpeg-6b-6.aix5.1.ppc.rpm
  - libpng-1.2.32-2.aix5.2.ppc.rpm
  - libtiff-3.8.2-1.aix5.2.ppc.rpm
  - pango-1.14.5-4.aix5.2.ppc.rpm
  - pixman-0.12.0-3.aix5.2.ppc.rpm
  - xcursor-1.1.7-3.aix5.2.ppc.rpm
  - xft-2.1.6-5.aix5.1.ppc.rpm
  - xrender-0.9.1-3.aix5.2.ppc.rpm
  - zlib-1.2.3-3.aix5.1.ppc.rpm
- Überprüfen Sie, ob für das Betriebssystem die erforderliche Sprache definiert ist. Die Sprache des Betriebssystems ist standardmäßig die Sprache des Installationsassistenten.



## Vorgehensweise

Installieren Sie IBM Spectrum Protect mit dem folgenden Verfahren:

| Option  | Bezeichnung  |
|---|--|
| <b>Installation der Software mithilfe eines heruntergeladenen Pakets:</b> | <p>a. Wechseln Sie in das Verzeichnis, in das Sie das Paket heruntergeladen haben.</p> <p>b. Geben Sie den folgenden Befehl aus, um den Installationsassistenten zu starten:  AIX-Betriebssysteme</p> <pre>./install.sh</pre> |

## Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM Installation Manager-Verzeichnis logs gespeichert werden.

Installationsprotokolldateien können Sie anzeigen, indem Sie in Installation Manager auf Datei > Protokoll anzeigen klicken. Um diese Protokolldateien zu erfassen, klicken Sie in Installation Manager auf Hilfe > Daten zur Fehleranalyse exportieren.
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.
-  Nachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.
-  AIX: Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren  
Bevor Sie IBM Spectrum Protect mithilfe des grafisch orientierten Assistenten von IBM Installation Manager installieren können, müssen Sie sicherstellen, dass die erforderlichen RPM-Dateien installiert sind.

## AIX: IBM Spectrum Protect im Konsolenmodus installieren

Sie können IBM Spectrum Protect mithilfe der Befehlszeile im Konsolenmodus installieren.


## Vorbereitende Schritte

Führen Sie vor dem Start der Installation die folgenden Schritte aus:



- Überprüfen Sie, ob für das Betriebssystem die erforderliche Sprache definiert ist. Die Sprache des Betriebssystems ist standardmäßig die Sprache des Installationsassistenten.

## Vorgehensweise

Installieren Sie IBM Spectrum Protect mit dem folgenden Verfahren:

| Option  | Bezeichnung   |
|---|---|
| <b>Installation der Software mithilfe eines heruntergeladenen Pakets:</b> | <p>a. Wechseln Sie in das Verzeichnis, in das Sie das Paket heruntergeladen haben.</p> <p>b. Geben Sie den folgenden Befehl aus, um den Installationsassistenten im Konsolenmodus zu starten:  AIX-Betriebssysteme</p> <pre>./install.sh -c</pre> <p>Optional : Generieren Sie während einer Installation im Konsolenmodus eine Antwortdatei. Geben Sie die Optionen für die Installation im Konsolenmodus und in der Anzeige Zusammenfassung <b>G</b> an, um die Antworten zu generieren.</p> |

## Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM® Installation Manager-Verzeichnis logs gespeichert werden. Zum Beispiel:
  -  AIX-Betriebssysteme/var/ibm/InstallationManager/logs
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.
-  AIX-Betriebssysteme Nachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.

## AIX: IBM Spectrum Protect im unbeaufsichtigten Modus installieren

Sie können den Server im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlernachrichten in Protokolldateien gespeichert.

### Vorbereitende Schritte

Für die Dateneingabe bei Verwendung der unbeaufsichtigten Installation können Sie eine Antwortdatei verwenden. Die folgenden Musterantwortdateien stehen im Verzeichnis input zur Verfügung, in dem das Installationspaket extrahiert wird:

install\_response\_sample.xml

Verwenden Sie diese Datei für die Installation der IBM Spectrum Protect-Komponenten.

update\_response\_sample.xml

Verwenden Sie diese Datei für das Upgrade der IBM Spectrum Protect-Komponenten.

Diese Dateien enthalten Standardwerte, die dazu beitragen können, unnötige Warnungen zu vermeiden. Befolgen Sie die in den Dateien enthaltenen Anweisungen zur Verwendung dieser Dateien.

Wenn Sie eine Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.


## Vorgehensweise

1. Erstellen Sie eine Antwortdatei. Sie können die Musterantwortdatei ändern oder eine eigene Datei erstellen.
2. Wenn Sie den Server und das Operations Center im unbeaufsichtigten Modus installieren, erstellen Sie in der Antwortdatei ein Kennwort für den Truststore des Operations Center.  
Wenn Sie die Datei install\_response\_sample.xml verwenden, fügen Sie das Kennwort in die folgende Zeile der Datei ein. Hierbei ist *mein\_Kennwort* das Kennwort:

```
<variable name='ssl.password' value='mein_Kennwort' />
```



Weitere Informationen zu diesem Kennwort finden Sie in Prüfliste für die Installation.

Tipp: Das Truststore-Kennwort ist nicht erforderlich, wenn Sie das Operations Center mit der Datei update\_response\_sample.xml aktualisieren.

3. Geben Sie den folgenden Befehl in dem Verzeichnis, in dem das Installationspaket extrahiert wurde, aus, um die unbeaufsichtigte Installation zu starten. Der Wert *Antwortdatei* gibt den Pfad und den Namen der Antwortdatei an.
  -  AIX-Betriebssysteme

```
./install.sh -s -input Antwortdatei -acceptLicense
```

## Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM® Installation Manager-Verzeichnis logs gespeichert werden. Zum Beispiel:
  -  AIX-Betriebssysteme/var/ibm/InstallationManager/logs
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.
-  AIX-Betriebssysteme Nachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.

 AIX-Betriebssysteme

## AIX: Serversprachenpakete installieren

Übersetzungen für den Server ermöglichen das Anzeigen von Nachrichten und Hilfetext auf dem Server in verschiedenen Sprachen. Die Übersetzungen gestatten auch die Verwendung länderspezifischer Einstellungen für das Datums-, Uhrzeit- und Zahlenformat.


## Vorbereitende Schritte

Anweisungen zur Installation von von Sprachenpaketen für Speicheragenten finden Sie unter Language pack configuration for Storage Agent.

- AIX: Spracheinstellungen für den Server  
Verwenden Sie zum Anzeigen von Servernachrichten und Hilfetext entweder das Standardsprachenpaket oder wählen Sie ein anderes Sprachenpaket aus.
- AIX: Sprachenpaket konfigurieren  
Nach der Konfiguration eines Sprachenpakets werden Nachrichten und Hilfetext auf dem Server in der Sprache dieses Sprachenpakets und nicht in Englisch (US) angezeigt. Installationspakete werden mit IBM Spectrum Protect zur Verfügung gestellt.
- AIX: Sprachenpaket aktualisieren  
Sie können ein Sprachenpaket mithilfe von IBM® Installation Manager ändern oder aktualisieren.

## AIX: Spracheinstellungen für den Server

Verwenden Sie zum Anzeigen von Servernachrichten und Hilfetext entweder das Standardsprachenpaket oder wählen Sie ein anderes Sprachenpaket aus.

 AIX-Betriebssysteme Dieses Sprachenpaket wird automatisch für die folgende Standardsprachenoption für IBM Spectrum Protect-Servernachrichten und -Hilfetext installiert:

-  AIX-Betriebssysteme LANGUAGE en\_US

Für vom Standard abweichende Sprachen oder Ländereinstellungen installieren Sie das für Ihre Installation erforderliche Sprachenpaket.

Sie können die aufgeführten Sprachen verwenden:



 AIX-Betriebssysteme

Tabelle 1. Serversprachen für AIX

| Sprache                           | Wert der Option LANGUAGE |
|-----------------------------------|--------------------------|
| Chinesisch, vereinfacht           | zh_CN                    |
| Chinesisch, vereinfacht (UTF-8)   | ZH_CN                    |
| Chinesisch, traditionell (Big5)   | Zh_TW                    |
| Chinesisch, traditionell (UTF-8)  | ZH_TW                    |
| Chinesisch, traditionell (euc_tw) | zh_TW                    |
| Englisch                          | en_US                    |
| Englisch (UTF-8)                  | EN_US                    |
| Französisch                       | fr_FR                    |
| Französisch (UTF-8)               | FR_FR                    |

| Sprache                                | Wert der Option LANGUAGE |
|--|--------------------------|
| Deutsch                                | de_DE                    |
| Deutsch (UTF-8)                        | DE_DE                    |
| Italienisch                            | it_IT                    |
| Italienisch (UTF-8)                    | IT_IT                    |
| Japanisch, EUC                         | ja_JP                    |
| Japanisch, PC                          | Ja_JP                    |
| Japanisch, UTF8                        | JA_JP                    |
| Koreanisch                             | ko_KR                    |
| Koreanisch (UTF-8)                     | KO_KR                    |
| Portugiesisch, Brasilianisches         | pt_BR                    |
| Portugiesisch, Brasilianisches (UTF-8) | PT_BR                    |
| Russisch                               | ru_RU                    |
| Russisch (UTF-8)                       | RU_RU                    |
| Spanisch                               | es_ES                    |
| Spanisch (UTF-8)                       | ES_ES                    |

 **Einschränkung:** Bei Verwendung des Operations Center werden einige Zeichen möglicherweise nicht ordnungsgemäß angezeigt, wenn der Web-Browsers und der Server nicht dieselbe Sprache verwenden. Wenn dieses Problem auftritt, geben Sie im Browser dieselbe Sprache wie im Server an.


## AIX: Sprachenpaket konfigurieren



---

Nach der Konfiguration eines Sprachenpakets werden Nachrichten und Hilfetext auf dem Server in der Sprache dieses Sprachenpakets und nicht in Englisch (US) angezeigt. Installationspakete werden mit IBM Spectrum Protect zur Verfügung gestellt.

### Informationen zu diesem Vorgang

---

 Führen Sie eine der folgenden Tasks aus, um die Unterstützung für eine bestimmte Ländereinstellung zu aktivieren:

- Geben Sie in der Option LANGUAGE in der Serveroptionsdatei den Namen der Ländereinstellung an, die verwendet werden soll.  
Beispiel:
  -  Soll die Ländereinstellung `it_IT` verwendet werden, setzen Sie die Option LANGUAGE auf `it_IT`.  
Siehe AIX: Spracheinstellungen für den Server.
-  Wenn Sie den Server im Vordergrund starten, definieren Sie die Umgebungsvariable `LC_ALL` gemäß dem in der Serveroptionsdatei definierten Wert. Soll beispielsweise die Umgebungsvariable für Italienisch definiert werden, geben Sie folgenden Wert ein:

```
export LC_ALL=it_IT
```

Wenn die Ländereinstellung erfolgreich initialisiert wird, steuert sie die Datums-, Uhrzeit- und Zahlenformatierung für den Server. Wenn die Ländereinstellung nicht erfolgreich initialisiert wird, verwendet der Server die englischen (US) Nachrichtendateien und das Datums-, Uhrzeit- und Zahlenformat der englischen (US) Ländereinstellung.

## AIX: Sprachenpaket aktualisieren

---

Sie können ein Sprachenpaket mithilfe von IBM® Installation Manager ändern oder aktualisieren.

### Informationen zu diesem Vorgang

---

Sie können ein anderes Sprachenpaket in derselben IBM Spectrum Protect-Instanz installieren.




- Verwenden Sie die Funktion Ändern von IBM Installation Manager, um ein anderes Sprachenpaket zu installieren.
- Verwenden Sie die Funktion Aktualisieren von IBM Installation Manager, um eine Aktualisierung auf neuere Versionen der Sprachenpakete durchzuführen.

Tipp: In IBM Installation Manager bedeutet *aktualisieren* das Erkennen und Installieren von Aktualisierungen und Fixes für installierte Softwarepakete. In diesem Kontext sind *Aktualisierung* und *Upgrade* gleichbedeutend.

## AIX: Die ersten Schritte nach der Installation von IBM Spectrum Protect

Nach der Installation von Version 8.1.3 bereiten Sie die Konfiguration vor. Bevorzugte Methode für die Konfiguration der IBM Spectrum Protect-Instanz ist die Verwendung des Konfigurationsassistenten.

### Informationen zu diesem Vorgang

1. Erstellen Sie die Verzeichnisse und die Benutzer-ID für die Serverinstanz. Siehe AIX: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen.
  2. Konfigurieren Sie eine Serverinstanz. Wählen Sie eine der folgenden Optionen aus:
    - Verwenden Sie den Konfigurationsassistenten (die bevorzugte Methode). Siehe AIX: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren.
    - Konfigurieren Sie die neue Instanz manuell. Siehe AIX: Serverinstanz manuell konfigurieren. Führen Sie während einer manuellen Konfiguration die folgenden Schritte aus:
      - a. Definieren Sie Ihre Verzeichnisse und erstellen Sie die IBM Spectrum Protect-Instanz. Siehe AIX: Serverinstanz erstellen.
      - b. Erstellen Sie eine neue Serveroptionsdatei, indem Sie die Musterdatei kopieren, um die Datenübertragung zwischen dem Server und den Clients zu definieren. Siehe  AIX-Betriebssysteme AIX: Server- und Clientübertragung konfigurieren.
      - c. Geben Sie den Befehl DSMSERV FORMAT aus, um die Datenbank zu formatieren. Siehe AIX: Datenbank und Protokoll formatieren.
      - d. Konfigurieren Sie Ihr System für die Datenbanksicherung. Siehe AIX: Datenbankmanager für die Datenbanksicherung vorbereiten.
  3. Konfigurieren Sie Optionen, die die Ausführung der Datenbankreorganisation steuern. Siehe AIX: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren.
  4. Starten Sie die Serverinstanz, falls noch nicht gestartet.
    -  AIX-Betriebssysteme Siehe AIX: Serverinstanz starten.
  5. Registrieren Sie Ihre Lizenz. Siehe AIX: Lizenzregistrierung.
  6. Bereiten Sie Ihr System auf Datenbanksicherungen vor. Siehe AIX: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben.
  7. Überwachen Sie den Server. Siehe AIX: Server überwachen.
- AIX: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen  
Erstellen Sie die Benutzer-ID für die IBM Spectrum Protect-Serverinstanz und die Verzeichnisse, die die Serverinstanz für Datenbank- und Wiederherstellungsprotokolle benötigt.
  - AIX: IBM Spectrum Protect-Server konfigurieren  
Nachdem Sie den Server installiert und für die Konfiguration vorbereitet haben, konfigurieren Sie die Serverinstanz.
  - AIX: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren  
Um Probleme bezüglich des Datenbankwachstums und der Serverleistung zu vermeiden, überwacht der Server automatisch seine Datenbanktabellen und reorganisiert diese Tabellen, wenn dies erforderlich ist. Bevor der Server für den Produktionseinsatz gestartet wird, definieren Sie Serveroptionen, mit denen gesteuert wird, wann die Reorganisation ausgeführt wird. Ist die Verwendung der Datendeduplizierung geplant, stellen Sie sicher, dass die Option für die Ausführung der Indexreorganisation aktiviert ist.
  -  AIX-Betriebssysteme AIX: Serverinstanz starten  
Sie können den Server mit der Instanzbenutzer-ID (bevorzugte Methode) oder mit der Rootbenutzer-ID starten.
  - AIX: Server stoppen  
Sie können den Server bei Bedarf stoppen, um die Steuerung an das Betriebssystem zurückzugeben. Um den Verlust von Verwaltungs- und Clientknotenverbindungen zu vermeiden, stoppen Sie den Server erst nach Beendigung oder Abbruch laufender Sitzungen.
  - AIX: Lizenzregistrierung  
Registrieren Sie alle lizenzierten IBM Spectrum Protect-Funktionen, die Sie beziehen, sofort, damit Sie nach dem Starten der Serveroperationen (z. B. Datensicherung) keine Daten verlieren.
  - AIX: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben  
Sie müssen die zu verwendende Einheitenklasse angeben, um das System für automatische oder manuelle Datenbanksicherungen vorzubereiten.
  - AIX: Mehrere Serverinstanzen auf einem System ausführen  
Sie können mehrere Serverinstanzen auf Ihrem System erstellen. Jede Serverinstanz verfügt über ein eigenes Instanzverzeichnis sowie über Datenbank- und Protokollverzeichnisse.
  - AIX: Server überwachen  
Wenn Sie den Server im Produktionsbetrieb einsetzen, überwachen Sie den von ihm verwendeten Speicherbereich, um sicherzustellen, dass die Größe des Speicherbereichs angemessen ist. Ändern Sie den Speicherbereich, falls erforderlich.

# AIX: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen

Erstellen Sie die Benutzer-ID für die IBM Spectrum Protect-Serverinstanz und die Verzeichnisse, die die Serverinstanz für Datenbank- und Wiederherstellungsprotokolle benötigt.


## Vorbereitende Schritte

Lesen Sie die Informationen zur Planung des Speicherbereichs für den Server, bevor Sie diese Task ausführen. Siehe AIX: Arbeitsblätter für Planungsdetails für den Server.

## Vorgehensweise

1. Erstellen Sie die Benutzer-ID, die Eigner der Serverinstanz sein soll. Diese Benutzer-ID verwenden Sie später bei der Erstellung der Serverinstanz.

### AIX-Betriebssysteme

 AIX-Betriebssysteme Erstellen Sie eine Benutzer-ID und eine Gruppe, die Eigner der Serverinstanz sein sollen.

- a. Die folgenden Befehle können mit einer Verwaltungsbenutzer-ID ausgeführt werden, die den Benutzer und die Gruppe definieren soll. Erstellen Sie die Benutzer-ID und Gruppe im Ausgangsverzeichnis des Benutzers.  
Einschränkung: In der Benutzer-ID dürfen nur Kleinbuchstaben (a-z), Ziffern (0-9) und das Unterstrichungszeichen ( \_ ) verwendet werden. Die Benutzer-ID und der Gruppenname müssen die folgenden Regeln einhalten:
  - Die maximale Länge beträgt 8 Zeichen.
  - Die Benutzer-ID und der Gruppenname dürfen nicht mit *ibm*, *sql*, *sys* oder mit einer Ziffer beginnen.
  - Als Benutzer-ID und Gruppenname dürfen nicht *user*, *admin*, *guest*, *public*, *local* und kein reserviertes SQL-Wort verwendet werden.

Erstellen Sie beispielsweise die Benutzer-ID `tsminst1` in der Gruppe `tsmsrvrs`. Die folgenden Beispiele zeigen, wie diese Benutzer-ID und diese Gruppe mit Betriebssystembefehlen erstellt werden.


### AIX-Betriebssysteme

```
mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

Einschränkung: DB2 unterstützt nicht die direkte Authentifizierung von Betriebssystembenutzern durch LDAP.

- b. Melden Sie sich ab und dann bei Ihrem System an. Wechseln Sie zu dem gerade erstellten Benutzerkonto.  
Verwenden Sie ein interaktives Anmeldeprogramm, z. B. Telnet, damit Sie zur Eingabe des Kennworts aufgefordert werden und es ggf. ändern können.

2. Erstellen Sie die vom Server benötigten Verzeichnisse.

 AIX-Betriebssysteme Erstellen Sie leere Verzeichnisse für jeden Tabelleneintrag und stellen Sie sicher, dass die neue Benutzer-ID, die Sie gerade erstellt haben, Eigner der Verzeichnisse ist. Hängen Sie den zugeordneten Speicher in jedem der Verzeichnisse für aktive Protokolldateien, für Archivprotokolle und Datenbanken an.

| Element   | Beispielbefehle für die Verzeichniserstellung  | Ihre Verzeichnisse |
|---|--|--------------------|
| Das <i>Instanzverzeichnis</i> für den Server. Dieses Verzeichnis enthält spezielle Dateien für diese Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien). | <code>mkdir /tsminst1</code>   |                    |
| Die Datenbankverzeichnisse  | <code>mkdir /tsmdb001</code><br><code>mkdir /tsmdb002</code><br><code>mkdir /tsmdb003</code><br><code>mkdir /tsmdb004</code> |                    |
| Verzeichnis für aktive Protokolldateien   | <code>mkdir /tsmlog</code>   |                    |
| Verzeichnis für Archivprotokolle  | <code>mkdir /tsmarchlog</code>   |                    |
| Optional: Verzeichnis für den Protokollspiegel für die aktive Protokolldatei  | <code>mkdir /tsmlogmirror</code>   |                    |

| Element   | Beispielbefehle für die Verzeichniserstellung | Ihre Verzeichnisse |
|---|---|--------------------|
| Optional: Sekundäres Verzeichnis für Archivprotokolle (Übernahmeverzeichnis für Archivprotokolle) | <code>mkdir /tsmarchlogfailover</code>        |                    |

Wenn ein Server anfänglich mit dem Dienstprogramm DSMSERV FORMAT oder mit dem Konfigurationsassistenten erstellt wird, werden eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien zum Speichern von Datenbankinformationen erstellt, die vom Datenbankmanager verwendet werden.

3. Melden Sie die neue Benutzer-ID ab.

## AIX: IBM Spectrum Protect-Server konfigurieren

Nachdem Sie den Server installiert und für die Konfiguration vorbereitet haben, konfigurieren Sie die Serverinstanz.

### Informationen zu diesem Vorgang

Wählen Sie eine der folgenden Optionen aus, um eine IBM Spectrum Protect-Serverinstanz zu konfigurieren:

- AIX: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren  
Der Assistent stellt eine Möglichkeit zur Konfiguration eines Servers mit Anleitung dar. Wenn Sie die grafische Benutzerschnittstelle (GUI) verwenden, können Sie einige komplexe Konfigurationsschritte der manuellen Ausführung vermeiden. Starten Sie den Assistenten auf dem System, auf dem Sie das IBM Spectrum Protect-Serverprogramm installiert haben.
- AIX: Serverinstanz manuell konfigurieren  
Nach der Installation von IBM Spectrum Protect Version 8.1.3 können Sie IBM Spectrum Protect auch manuell und nicht mit dem Konfigurationsassistenten konfigurieren.



## AIX: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren

Der Assistent stellt eine Möglichkeit zur Konfiguration eines Servers mit Anleitung dar. Wenn Sie die grafische Benutzerschnittstelle (GUI) verwenden, können Sie einige komplexe Konfigurationsschritte der manuellen Ausführung vermeiden. Starten Sie den Assistenten auf dem System, auf dem Sie das IBM Spectrum Protect-Serverprogramm installiert haben.

### Vorbereitende Schritte

Bevor Sie den Konfigurationsassistenten starten, müssen Sie alle vorhergehenden Schritte zur Vorbereitung der Konfiguration ausführen. Zu diesen Schritten gehören die Installation von IBM Spectrum Protect, die Erstellung der Datenbank- und Protokollverzeichnisse und die Erstellung der Verzeichnisse und der Benutzer-ID für die Serverinstanz.


### Vorgehensweise

1. Stellen Sie sicher, dass folgende Anforderungen erfüllt sind:  AIX-Betriebssysteme
  - Das System, auf dem Sie IBM Spectrum Protect installiert haben, muss über den X Window System-Client verfügen. Außerdem müssen Sie einen X Window System-Server auf Ihrem Desktop ausführen.
  - Im System muss das SSH-Protokoll (Secure Shell) aktiviert sein. Stellen Sie sicher, dass für den Port der Standardwert 22 definiert ist und dass der Port nicht durch eine Firewall blockiert wird. Sie müssen die Kennwortauthentifizierung in der Datei `sshd_config` im Verzeichnis `/etc/ssh/` aktivieren. Stellen Sie außerdem sicher, dass der SSH-Dämons-service über Zugriffsberechtigungen zum Herstellen einer Verbindung zum System mithilfe des Werts `localhost` verfügt.
  - Sie müssen sich mit der Benutzer-ID, die Sie für die Serverinstanz erstellt haben, mit dem SSH-Protokoll bei IBM Spectrum Protect anmelden können. Bei Verwendung des Assistenten müssen Sie diese Benutzer-ID und dieses Kennwort für den Zugriff auf dieses System angeben.
  - Starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.
2. Starten Sie die lokale Version des Assistenten:
  -  AIX-Betriebssysteme Öffnen Sie das Programm `dsmsicfgx` im Verzeichnis `/opt/tivoli/tsm/server/bin`. Dieser Assistent kann nur als Root ausgeführt werden.

Befolgen Sie die Anweisungen zur Ausführung der Konfiguration. Der Assistent kann gestoppt und erneut gestartet werden. Der Server ist jedoch erst betriebsbereit, wenn der gesamte Konfigurationsprozess abgeschlossen ist.

## AIX: Serverinstanz manuell konfigurieren

Nach der Installation von IBM Spectrum Protect Version 8.1.3 können Sie IBM Spectrum Protect auch manuell und nicht mit dem Konfigurationsassistenten konfigurieren.

- AIX: Serverinstanz erstellen  
Erstellen Sie eine IBM Spectrum Protect-Instanz mit dem Befehl db2icrt.
-  AIX: Server- und Clientübertragung konfigurieren  
Eine standardmäßige Beispielserveroptionsdatei mit dem Namen dsm serv.opt.smp wird während der IBM Spectrum Protect-Installation im Verzeichnis /opt/tivoli/tsm/server/bin erstellt. Sie müssen die Datenübertragung zwischen dem Server und den Clients definieren, indem Sie eine neue Serveroptionsdatei erstellen. Hierfür kopieren Sie die Musterdatei in das Verzeichnis für die Serverinstanz.
- AIX: Datenbank und Protokoll formatieren  
Mit dem Dienstprogramm DSM SERV FORMAT können Sie eine Serverinstanz initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls ist keine andere Serveraktivität zulässig.
- AIX: Datenbankmanager für die Datenbanksicherung vorbereiten  
Um die Daten in der Datenbank in IBM Spectrum Protect zu sichern, müssen Sie den Datenbankmanager aktivieren und die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) konfigurieren.

## AIX: Serverinstanz erstellen


---

Erstellen Sie eine IBM Spectrum Protect-Instanz mit dem Befehl db2icrt.

### Informationen zu diesem Vorgang

---

Auf einer Workstation kann mindestens eine Serverinstanz vorhanden sein.


 **Wichtig:** Stellen Sie Folgendes sicher, bevor der Befehl db2icrt ausgeführt wird:

- Das Ausgangsverzeichnis für den Benutzer (/home/tsminst1) ist vorhanden. Ist kein Ausgangsverzeichnis vorhanden, müssen Sie es erstellen.


Im Instanzverzeichnis sind folgende Kerndateien gespeichert, die vom IBM Spectrum Protect-Server generiert werden:

- Serveroptionsdatei dsm serv.opt
  - Die Serverschlüsseldatenbankdatei cert.kdb und die .arm-Dateien (werden von Clients und anderen Servern zum Importieren der Secure Sockets Layer-Zertifikate des Servers verwendet)
  - Einheitenkonfigurationsdatei, wenn die Serveroption DEVCONFIG keinen vollständig qualifizierten Namen angibt
  - Protokolldatei für Datenträger, wenn die Serveroption VOLUMEHISTORY keinen vollständig qualifizierten Namen angibt
  - Datenträger für Speicherpools mit dem Typ DEVTYPE=FILE, wenn das Verzeichnis für die Einheitenklasse nicht vollständig angegeben oder nicht vollständig qualifiziert ist
  - Benutzerexits
  - Traceausgabe (wenn nicht vollständig qualifiziert)
- Eine Shellkonfigurationsdatei (z. B. .profile) ist im Ausgangsverzeichnis vorhanden. Die Rootbenutzer- und Instanzbenutzer-ID müssen über Schreibberechtigung für diese Datei verfügen. Weitere Informationen finden Sie in Produktinformation zu DB2. Suchen Sie dort nach den Einstellungen für Linux- und UNIX-Umgebungsvariablen.

#### AIX-Betriebssysteme

1. Melden Sie sich mit der Root-ID an und erstellen Sie eine IBM Spectrum Protect-Instanz. Der Name der Instanz muss mit dem Namen des Benutzers identisch sein, der Eigner der Instanz ist. Verwenden Sie den Befehl db2icrt und geben Sie den Befehl in eine Zeile ein: 

```
/opt/tivoli/tsm/db2/instance/db2icrt -a server -u  
Instanzname Instanzname
```

Lautet Ihre Benutzer-ID für diese Instanz z. B. tsminst1, verwenden Sie den folgenden Befehl, um die Instanz zu erstellen. Geben Sie den Befehl in eine einzelne Zeile ein. 

```
/opt/tivoli/tsm/db2/instance/db2icrt -a server -u  
tsminst1 tsminst1
```

Hinweis: Verwenden Sie ab diesem Punkt diese neue Benutzer-ID für die Konfiguration Ihres IBM Spectrum Protect-Servers. Melden Sie sich mit der Root-ID ab und mit der neuen Instanzbenutzer-ID an.

2. Geben Sie als Standardverzeichnis für die Datenbank das Instanzverzeichnis für den Server an. Sind mehrere Server vorhanden, melden Sie sich mit der Instanz-ID des jeweiligen Servers an. Geben Sie den folgenden Befehl aus:


```
db2 update dbm cfg using dftdbpath Instanzverzeichnis
```

Lautet das Instanzverzeichnis für den Server z. B. 'tsminst1', ändern Sie mit dem folgenden Befehl das Standardverzeichnis für die Datenbank in 'tsminst1':

```
db2 update dbm cfg using dftdbpath /tsminst1
```



3. Ändern Sie den Bibliothekspfad, so dass die Version von IBM Global Security Kit (GSKit) verwendet wird, die mit dem Server installiert wird. In den folgenden Beispielen ist *server\_bin\_directory* ein Unterverzeichnis des Serverinstallationsverzeichnisses. Zum Beispiel */opt/tivoli/tsm/server/bin*.

-  AIX-Betriebssysteme Geben Sie den folgenden Befehl in einer Zeile ein:

```
export LIBPATH=server_bin_directory/dbbkapi:  
/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```


- Sie müssen die folgenden Dateien aktualisieren, um den Bibliothekspfad zu definieren, wenn DB2 oder der Server gestartet wird:

Bash- oder Korn-Shell-Beispiel:

```
Instanzbenutzer-Ausgangsverzeichnis/sqlllib/userprofile
```


C-Shell-Beispiel:

```
Instanzbenutzer-Ausgangsverzeichnis/sqlllib/usercshrc
```

- Fügen Sie den folgenden Eintrag zur Datei *Instanzbenutzer-Ausgangsverzeichnis/sqlllib/userprofile* (Bash- oder Korn-Shell) in einer einzigen Zeile hinzu:  AIX-Betriebssysteme

```
export LIBPATH=server_bin_directory/  
dbbkapi:/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```

Hinweis: Der Bibliothekspfad muss folgende Einträge enthalten:

- */usr/local/ibm/gsk8\_64/lib64*
  - */opt/ibm/lib*
  - */opt/ibm/lib64*
  - */usr/lib64*
- Fügen Sie den folgenden Eintrag zur Datei *Instanzbenutzer-Ausgangsverzeichnis/sqlllib/usercshrc* (C-Shell) in einer einzigen Zeile hinzu:  AIX-Betriebssysteme

```
setenv LIBPATH server_bin_directory/dbbkapi:  
/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```

4. Erstellen Sie eine neue Serveroptionsdatei. Siehe AIX: Server- und Clientübertragung konfigurieren.

 AIX-Betriebssysteme

## AIX: Server- und Clientübertragung konfigurieren

---

Eine standardmäßige Beispielserveroptionsdatei mit dem Namen *dsm serv.opt.smp* wird während der IBM Spectrum Protect-Installation im Verzeichnis */opt/tivoli/tsm/server/bin* erstellt. Sie müssen die Datenübertragung zwischen dem Server und den Clients definieren, indem Sie eine neue Serveroptionsdatei erstellen. Hierfür kopieren Sie die Musterdatei in das Verzeichnis für die Serverinstanz.

### Informationen zu diesem Vorgang

---

Stellen Sie sicher, dass ein Serverinstanzverzeichnis, z. B. */tsminst1*, vorhanden ist und kopieren Sie die Musterdatei in dieses Verzeichnis. Nennen Sie die neue Datei *dsm serv.opt* und editieren Sie die Optionen. Führen Sie diese Konfiguration vor der Initialisierung der Serverdatenbank aus. Jedes Beispiel bzw. jeder Standardeintrag in der Beispieloptionsdatei ist ein Kommentar in einer Zeile, die mit einem Stern (\*) beginnt. Bei Optionen muss die Groß-/Kleinschreibung nicht beachtet werden, und zwischen Schlüsselwörtern und Werten dürfen sich ein oder mehrere Leerzeichen befinden.

Für das Editieren der Optionsdatei gelten folgende Richtlinien:




- Entfernen Sie den Stern am Anfang der Zeile, um eine Option zu aktivieren.
- Beginnen Sie mit der Eingabe der Optionen in einer beliebigen Spalte.
- Geben Sie nur eine Option pro Zeile ein. Die Option muss auf einer Zeile stehen.
- Werden mehrere Einträge für ein Schlüsselwort vorgenommen, verwendet der IBM Spectrum Protect-Server den letzten Eintrag.

Wenn Sie die Serveroptionsdatei ändern, müssen Sie den Server erneut starten, damit die Änderungen wirksam werden.

Sie können mindestens eine der folgenden Übertragungsmethoden angeben:

- TCP/IP Version 4 oder Version 6
- Shared Memory
- Secure Sockets Layer (SSL)

Tipp: Sie können Kennwörter im LDAP-Verzeichnisserver oder im IBM Spectrum Protect-Server authentifizieren. Im LDAP-Verzeichnisserver authentifizierte Kennwörter können erweiterte Systemsicherheit zur Verfügung stellen.

-  AIX-BetriebssystemeAIX: TCP/IP-Optionen definieren  
Wählen Sie aus dem Bereich von TCP/IP-Optionen eine Option für den IBM Spectrum Protect-Server aus oder verwenden Sie den Standardwert.
-  AIX-BetriebssystemeAIX: Shared Memory-Optionen definieren  
Sie können die Shared Memory-Übertragung zwischen Clients und Servern auf demselben System verwenden. Für die Verwendung von Shared Memory muss TCP/IP Version 4 auf dem System installiert sein.
-  AIX-BetriebssystemeAIX: Secure Sockets Layer-Optionen definieren  
Mithilfe von Secure Sockets Layer (SSL) können Sie Ihre Daten und Kennwörter besser schützen.

## AIX: TCP/IP-Optionen definieren

---

Wählen Sie aus dem Bereich von TCP/IP-Optionen eine Option für den IBM Spectrum Protect-Server aus oder verwenden Sie den Standardwert.

### Informationen zu diesem Vorgang

---

Das folgende Beispiel zeigt eine Liste der TCP/IP-Optionen, mit denen Sie Ihr System definieren können.


```
commmethod      tcpip
tcpport         1500
tcpwindowsize   0
tcpnodelay      yes
```

Tipp: Sie können TCP/IP Version 4 und/oder Version 6 verwenden.

#### TCPPORT

Die Adresse des Server-Ports für TCP/IP- und SSL-Kommunikation. Der Standardwert ist 1500.

#### AIX-BetriebssystemeTCPWINDOWSIZE

 AIX-BetriebssystemeGibt die Größe des TCP/IP-Puffers an, der beim Senden oder Empfangen von Daten verwendet wird. Die in einer Sitzung verwendete Fenstergröße ist der kleinere Wert der Server- und Clientfenstergröße. Größere Fenstergrößen benötigen zusätzlichen Speicher, können jedoch die Leistung verbessern.

Sie können eine ganze Zahl von 0 bis 2048 angeben. Soll die Standardfenstergröße für das Betriebssystem verwendet werden, geben Sie 0 an.

#### TCPNODELAY

Gibt an, ob der Server kleine Nachrichten sendet oder ob TCP/IP die Nachrichten puffern soll. Das Senden kleiner Nachrichten kann den Durchsatz verbessern, erhöht jedoch die Anzahl der im Netz gesendeten Pakete. Geben Sie YES an, wenn kleine Nachrichten gesendet werden sollen, oder NO, wenn sie TCP/IP puffern soll. Der Standardwert ist YES.

#### TCPADMINPORT

Gibt die Anschlussnummer an, an der der TCP/IP-DFV-Treiber des Servers auf TCP/IP- oder SSL-fähige Kommunikationsanforderungen warten soll, die keine Clientsitzungen sind. Der Standardwert ist der Wert von TCPPORT.

#### SSLTCPPOINT

(Nur SSL) Gibt die SSL-Anschlussnummer (SSL = Secure Sockets Layer) an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen für SSL-fähige Sitzungen des Befehlszeilenclients für Sichern/Archivieren und des Verwaltungsbefehlszeilenclients wartet.

#### SSLTCPADMINPORT

(Nur SSL) Gibt die Anschlussadresse an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen für SSL-fähige Sitzungen für den Verwaltungsbefehlszeilenclient wartet.

## AIX: Shared Memory-Optionen definieren

---

Sie können die Shared Memory-Übertragung zwischen Clients und Servern auf demselben System verwenden. Für die Verwendung von Shared Memory muss TCP/IP Version 4 auf dem System installiert sein.

### Informationen zu diesem Vorgang

---


Das folgende Beispiel zeigt eine Einstellung für Shared Memory:


```
commmethod      sharedmem
shmport         1510
```

In diesem Beispiel gibt SHMPORT die TCP/IP-Anschlussadresse eines Servers bei Verwendung von Shared Memory an. Verwenden Sie die Option SHMPORT, um einen anderen TCP/IP-Anschluss anzugeben. Die Standardanschlussadresse ist 1510.

COMMETHOD kann in der IBM Spectrum Protect-Serveroptionsdatei mehrfach mit einem jeweils anderen Wert verwendet werden. Die folgende Angabe ist beispielsweise möglich:

```
commmethod tcpip
commmethod sharedmem
```

 Die maximale Anzahl gleichzeitig ablaufender Shared Memory-Sitzungen basiert auf den verfügbaren Systemressourcen. Jede Shared Memory-Sitzung verwendet eine Shared Memory-Region mit maximal 4 MB und vier IPCS-Nachrichtenwarteschlangen, abhängig von der Version des IBM Spectrum Protect-Clients.

 Werden der Server und der Client nicht unter derselben Benutzer-ID ausgeführt, muss der Server der Root sein. Damit werden Shared Memory-Übertragungsfehler vermieden.

## AIX: Secure Sockets Layer-Optionen definieren

---

Mithilfe von Secure Sockets Layer (SSL) können Sie Ihre Daten und Kennwörter besser schützen.

### Vorbereitende Schritte

---

SSL ist die Standardtechnologie für die Erstellung verschlüsselter Sitzungen zwischen Servern und Clients. SSL stellt einen sicheren Kanal für die Server- und Clientkommunikation über offene Kommunikationspfade zur Verfügung. Bei SSL wird die Identität des Servers durch Verwendung digitaler Zertifikate überprüft.

Verwenden Sie SSL für Sitzungen nur im Bedarfsfall, um eine bessere Systemleistung sicherzustellen. Sie könnten die Prozessorressourcen auf dem IBM Spectrum Protect-Server erweitern, um den erhöhten Anforderungen gerecht zu werden.

## AIX: Datenbank und Protokoll formatieren

---

Mit dem Dienstprogramm DSMSEV FORMAT können Sie eine Serverinstanz initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls ist keine andere Serveraktivität zulässig.

Nach der Konfiguration der Serverübertragung können Sie die Datenbank initialisieren. Sie müssen sich mit der Instanzbenutzer-ID anmelden. Fügen Sie die Verzeichnisse nicht in Dateisysteme ein, deren Speicherplatz nicht ausreichen könnte. Wenn bestimmte Verzeichnisse (z. B. das Archivprotokoll) nicht verfügbar oder voll werden, stoppt der Server.


Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN.

### Exitlistenhandler definieren

---

Geben Sie für jede Serverinstanz ON für die Registry-Variablen DB2NOEXITLIST an. Melden Sie sich als Serverinstanzeigner beim System an und geben Sie den folgenden Befehl aus:


```
db2set -i Name_der_Serverinstanz DB2NOEXITLIST=ON
```

Beispiel: 

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```


### Serverinstanz initialisieren

---

Mit dem Dienstprogramm DSMSEV FORMAT können Sie eine Serverinstanz initialisieren. Wenn das Verzeichnis der Serverinstanz z. B. `/tsminst1` lautet, geben Sie die folgenden Befehle aus: 

```
cd /tsminst1
dsmsevr format dbdir=/tsmdb001 activelogsiz=32768
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Tip: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zu Grunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorabesezugriff und zur Verteilung der Datenbank verringert.

 Tip: Wenn DB2 nach Ausgabe des Befehls DSMSEV FORMAT nicht startet, müssen Sie möglicherweise die Mountoption NOSUID des Dateisystems inaktivieren. Wird diese Option in dem Dateisystem definiert, in dem sich das Verzeichnis des DB2-Instanzeigners befindet, oder in einem beliebigen Dateisystem, in dem sich die DB2-Datenbank, aktive Protokolldateien, Archivprotokolle, Übernahmeprotokolle oder Spiegelprotokolle befinden, muss die Option inaktiviert werden, um das System starten zu können.

Nach der Inaktivierung der Option NOSUID hängen Sie das Dateisystem erneut an. Dann starten Sie DB2 mit dem folgenden Befehl:


**Zugehörige Informationen:**

DSMSERV FORMAT (Datenbank und Protokoll formatieren)

## AIX: Datenbankmanager für die Datenbanksicherung vorbereiten


Um die Daten in der Datenbank in IBM Spectrum Protect zu sichern, müssen Sie den Datenbankmanager aktivieren und die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) konfigurieren.

### Informationen zu diesem Vorgang

 **AIX-Betriebssysteme** Ab IBM Spectrum Protect Version 7.1 ist es nicht mehr erforderlich, das API-Kennwort während einer manuellen Konfiguration des Servers zu definieren. Wenn Sie das API-Kennwort während des manuellen Konfigurationsprozesses definieren, können Datenbanksicherungsversuche fehlschlagen.

Wenn Sie den Konfigurationsassistenten verwenden, um eine IBM Spectrum Protect-Serverinstanz zu erstellen, müssen Sie diese Schritte nicht ausführen. Wenn Sie eine Instanz manuell konfigurieren, führen Sie die folgenden Schritte aus, bevor Sie den Befehl BACKUP DB oder RESTORE DB ausgeben.

**Achtung:** Wenn die Datenbank nicht verwendet werden kann, ist der gesamte IBM Spectrum Protect-Server nicht verfügbar. Wenn eine Datenbank verloren geht und nicht wiederhergestellt werden kann, kann die Wiederherstellung der von diesem Server verwalteten Daten schwierig oder unmöglich sein. Daher ist es unbedingt erforderlich, die Datenbank zu sichern.

 **AIX-Betriebssysteme** In den folgenden Befehlen müssen Sie die Beispielwerte durch Ihre tatsächlichen Werte ersetzen. In den Beispielen wird `tsminst1` für die Benutzer-ID der Serverinstanz, `/tsminst1` für das Verzeichnis der Serverinstanz und `/home/tsminst1` als Ausgangsverzeichnis der Serverinstanzbenutzer verwendet.

1. Definieren Sie die Umgebungsvariablenkonfiguration der IBM Spectrum Protect-API für die Datenbankinstanz:
  - a. Melden Sie sich mit der Benutzer-ID `tsminst1` an.
  - b. Wenn der Benutzer `tsminst1` angemeldet ist, stellen Sie sicher, dass die DB2-Umgebung ordnungsgemäß initialisiert wird. Die DB2-Umgebung wird durch Ausführung des Scripts `/home/tsminst1/sqllib/db2profile` initialisiert, das normalerweise automatisch über das Profil der Benutzer-ID ausgeführt wird. Stellen Sie sicher, dass die `.profile`-Datei im Ausgangsverzeichnis der Instanzbenutzer vorhanden ist, z. B. `/home/tsminst1/.profile`. Wenn `.profile` das Script `db2profile` nicht ausführt, fügen Sie folgende Zeilen hinzu:

```
if [ -f /home/tsminst1/sqllib/db2profile ]; then
    . /home/tsminst1/sqllib/db2profile
fi
```

- c. Fügen Sie in der Datei `Instanzverzeichnis/sqllib/userprofile` die folgenden Zeilen hinzu:

```
DSMI_CONFIG=Serverinstanzverzeichnis/tsmdbmgr.opt
DSMI_DIR=Serververzeichnis_bin/dbbkapi
DSMI_LOG=Serverinstanzverzeichnis
export DSMI_CONFIG DSMI_DIR DSMI_LOG
```

Hierbei gilt Folgendes:

- `Instanzverzeichnis` ist das Ausgangsverzeichnis des Serverinstanzbenutzers.
- `Serverinstanzverzeichnis` ist das Serverinstanzverzeichnis.
- `Serververzeichnis_bin` ist das Serververzeichnis 'bin'. Die Standardposition ist `/opt/tivoli/tsm/server/bin`.

Fügen Sie in der Datei `Instanzverzeichnis/sqllib/usercshrc` die folgenden Zeilen hinzu:

```
setenv DSMI_CONFIG=Serverinstanzverzeichnis/tsmdbmgr.opt
setenv DSMI_DIR=Serververzeichnis_bin/dbbkapi
setenv DSMI_LOG=Serverinstanzverzeichnis
```

2. Melden Sie sich ab und als `tsminst1` erneut an oder geben Sie den folgenden Befehl aus:

```
. ~/.profile
```

**Tipp:** Stellen Sie sicher, dass Sie ein Leerzeichen nach dem ersten Punkt (.) eingeben.

3. Erstellen Sie eine Datei mit dem Namen `tsmdbmgr.opt` im Verzeichnis `Serverinstanz`, das sich in diesem Beispiel im Verzeichnis `/tsminst1` befindet, und fügen Sie folgende Zeile hinzu:

```
SERVERNAME TSMDBMGR_TSMINST1
```

**Hinweis:** Der Wert für `SERVERNAME` muss in den Dateien `tsmdbmgr.opt` und `dsm.sys` konsistent sein.

4. Fügen Sie als Rootbenutzer die folgenden Zeilen zur Konfigurationsdatei `dsm.sys` der IBM Spectrum Protect-API hinzu. Die Konfigurationsdatei `dsm.sys` befindet sich standardmäßig in folgendem Standardverzeichnis:
  - `Serververzeichnis_bin/dbbkapi/dsm.sys`

```
servername TSMDBMGR_TSMINST1
commmethod tcpip
tcpserveraddr localhost
tcpport 1500
errorlogname /tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

#### Erläuterungen:

- *Servername* stimmt mit dem Wert für *servername* in der Datei *tsmdbmgr.opt* überein.
  - *Commmethod* gibt die Client-API an, mit der Kontakt zum Server wegen der Datenbanksicherung hergestellt wird. Gültige Werte sind *tcpip* und *sharedmem*. Weitere Informationen zu Shared Memory (gemeinsam genutzter Speicher) finden Sie in Schritt 5.
  - *Tcpserveraddr* gibt die Serveradresse an, mit der die Client-API Kontakt zum Server wegen der Datenbanksicherung herstellt. Um sicherzustellen, dass die Datenbank gesichert werden kann, muss dieser Wert *localhost* lauten.
  - *Tcpport* gibt die Anschlussnummer an, mit der die Client-API Kontakt zum Server wegen der Datenbanksicherung herstellt. Sie müssen denselben *tcpport*-Wert wie in der Serveroptionsdatei *dmserv.opt* angeben.
  - *Errorlogname* gibt das Fehlerprotokoll an, in dem die Client-API Fehler protokolliert, die während einer Datenbanksicherung auftreten. Dieses Protokoll befindet sich normalerweise im Serverinstanzverzeichnis. Dieses Protokoll kann sich jedoch an jeder beliebigen Position befinden, für die die Instanzbenutzer-ID Schreibberechtigung hat.
  - *Nodename* gibt den Knotennamen an, mit dem die Client-API während einer Datenbanksicherung eine Verbindung zum Server herstellt. Um sicherzustellen, dass die Datenbank gesichert werden kann, muss dieser Wert *\$\_TSMDBMGR\_\$\$* lauten.
5. Optional: Konfigurieren Sie den Server für die Datenbanksicherung mithilfe von Shared Memory. Auf diese Weise könnten Sie die Prozessorauslastung verringern und den Durchsatz verbessern. Führen Sie die folgenden Schritte aus:
- Überprüfen Sie die Datei *dmserv.opt*. Fügen Sie die folgenden Zeilen in die Datei ein, falls nicht vorhanden:

```
commmethod sharedmem
shmport Anschlussnummer
```

Hierbei steht *Anschlussnummer* für den Anschluss, der für Shared Memory verwendet werden soll.

- Suchen Sie in der Konfigurationsdatei *dsm.sys* die folgenden Zeilen:

```
commmethod tcpip
tcpserveraddr localhost
tcpport Anschlussnummer
```

Ersetzen Sie die angegebenen Zeilen durch die folgenden Zeilen:

```
commmethod sharedmem
shmport Anschlussnummer
```


Hierbei steht *Anschlussnummer* für den Anschluss, der für Shared Memory verwendet werden soll.

## AIX: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren

Um Probleme bezüglich des Datenbankwachstums und der Serverleistung zu vermeiden, überwacht der Server automatisch seine Datenbanktabellen und reorganisiert diese Tabellen, wenn dies erforderlich ist. Bevor der Server für den Produktionseinsatz gestartet wird, definieren Sie Serveroptionen, mit denen gesteuert wird, wann die Reorganisation ausgeführt wird. Ist die Verwendung der Datendeduplizierung geplant, stellen Sie sicher, dass die Option für die Ausführung der Indexreorganisation aktiviert ist.

### Informationen zu diesem Vorgang


Die Tabellen- und Indexreorganisation erfordert in hohem Umfang Prozessorressourcen, Speicherbereich für die aktive Protokolldatei und Speicherbereich für das Archivprotokoll. Da die Datenbanksicherung Vorrang vor der Reorganisation hat, wählen Sie den Zeitpunkt und die Dauer für die Reorganisation aus, um sicherzustellen, dass sich die Prozesse nicht überlappen und die Reorganisation ausgeführt werden kann.

 AIX-Betriebssysteme Sie können die Index- und Tabellenreorganisation für die Serverdatenbank optimieren. Auf diese Weise können Sie die Vermeidung von unerwartetem Datenbankwachstum und Leistungsproblemen verbessern. Anweisungen finden Sie in Technote 1683633.

Wenn Sie diese Serveroptionen aktualisieren, während der Server aktiv ist, müssen Sie den Server stoppen und erneut starten, damit die aktualisierten Werte wirksam werden.

### Vorgehensweise

1. Ändern Sie die Serveroptionen.

 AIX-Betriebssysteme Bearbeiten Sie die Serveroptionsdatei dmserv.opt im Serverinstanzverzeichnis. Beachten Sie bei der Bearbeitung der Serveroptionsdatei die folgenden Richtlinien:

- Entfernen Sie den Stern am Zeilenanfang, um eine Option zu aktivieren.
- Geben Sie eine Option in einer beliebigen Zeile ein.
- Geben Sie nur eine Option pro Zeile ein. Die vollständige Option mit ihrem Wert muss sich in einer Zeile befinden.
- Haben Sie mehrere Einträge für eine Option in der Datei, verwendet der Server den letzten Eintrag.

Die verfügbaren Serveroptionen können Sie mit der Musterdatei dmserv.opt.smp im Verzeichnis /opt/tivoli/tsm/server/bin anzeigen.

2. Ist die Verwendung der Datenduplizierung geplant, aktivieren Sie die Serveroption ALLOWREORGINDEX. Fügen Sie der Serveroptionsdatei die folgende Option und den folgenden Wert hinzu:

```
allowreorgindex yes
```

3. Definieren Sie die Serveroptionen REORGBEGINTIME und REORGDURATION, mit denen gesteuert wird, wann die Reorganisation gestartet und wie lange sie ausgeführt wird. Wählen Sie den Zeitpunkt und die Dauer so aus, dass die Reorganisation ausgeführt wird, wenn der Server voraussichtlich am wenigsten ausgelastet ist. Diese Serveroptionen steuern sowohl die Tabellen- als auch die Indexreorganisationsprozesse.

- a. Definieren Sie die Startzeit der Reorganisation mit der Serveroption REORGBEGINTIME. Geben Sie die Zeit im 24-Stunden-Format an. Um beispielsweise als Startzeit der Reorganisation 20:30 Uhr festzulegen, geben Sie die folgende Option und den folgenden Wert in der Serveroptionsdatei an:

```
reorgbegintime 20:30
```

- b. Definieren Sie das Intervall, in dem der Server die Reorganisation starten kann. Um beispielsweise anzugeben, dass der Server die Reorganisation innerhalb von 4 Stunden nach dem mit der Serveroption REORGBEGINTIME definierten Zeitpunkt starten kann, geben Sie die folgende Option und den folgenden Wert in der Serveroptionsdatei an:

```
reorgduration 4
```

4. War der Server aktiv, während Sie die Serveroptionsdatei aktualisiert haben, stoppen Sie den Server und starten Sie ihn erneut.

#### Zugehörige Informationen:

 ALLOWREORGINDEX

 ALLOWREORGTABLE

 REORGBEGINTIME

 REORGDURATION

 AIX-Betriebssysteme

## AIX: Serverinstanz starten

---

Sie können den Server mit der Instanzbenutzer-ID (bevorzugte Methode) oder mit der Rootbenutzer-ID starten.

### Vorbereitende Schritte

---


Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden.

 AIX-Betriebssysteme Anweisungen finden Sie in Zugriffsberechtigungen und Benutzergrenzwerte überprüfen.

### Informationen zu diesem Vorgang

---

Wenn Sie den Server unter Verwendung der Instanzbenutzer-ID starten, wird der Konfigurationsprozess vereinfacht und potenzielle Probleme werden vermieden. In einigen Fällen kann jedoch die Verwendung der Rootbenutzer-ID zum Starten des Servers erforderlich sein. Beispielsweise kann die Rootbenutzer-ID verwendet werden, um sicherzustellen, dass der Server auf bestimmte Einheiten zugreifen kann. Sie können den automatischen Serverstart mit der Instanzbenutzer-ID oder mit der Rootbenutzer-ID konfigurieren.


 AIX-Betriebssysteme Wenn Sie Verwaltungs- oder Rekonfigurationstasks ausführen müssen, starten Sie den Server im Verwaltungsmodus.

### Vorgehensweise

---




Führen Sie einen der folgenden Schritte aus, um den Server zu starten:

- Starten Sie den Server mithilfe der Instanzbenutzer-ID.

 AIX-Betriebssysteme Anweisungen finden Sie in Server mit der Instanzbenutzer-ID starten.

- Starten Sie den Server mithilfe der Rootbenutzer-ID.

Anweisungen zum Berechtigen von Rootbenutzer-IDs zum Starten des Servers finden Sie in Rootbenutzer-IDs zum Starten des Servers berechtigen (Version 7.1.1). Anweisungen zum Starten des Servers mit der Rootbenutzer-ID finden Sie in Server mit der Rootbenutzer-ID starten (Version 7.1.1).

-  AIX-Betriebssysteme Starten Sie den Server automatisch.
  -  AIX-Betriebssysteme Anweisungen siehe AIX: Server automatisch starten.
  -  AIX-Betriebssysteme Starten Sie den Server im Verwaltungsmodus.
- Anweisungen siehe AIX: Server im Verwaltungsmodus starten.

 AIX-Betriebssysteme

## AIX: Zugriffsberechtigungen und Benutzergrenzwerte überprüfen

Vor dem Start des Servers überprüfen Sie Zugriffsberechtigungen und Benutzergrenzwerte.

### Informationen zu diesem Vorgang

Wenn Sie die Benutzergrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, nicht überprüfen, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann. Die müssen auch den systemweiten Grenzwert für die maximale Anzahl offener Dateien überprüfen. Der systemweite Grenzwert muss größer-gleich dem Benutzergrenzwert sein.

### Vorgehensweise

1. Überprüfen Sie, ob die Benutzer-ID der Serverinstanz über Berechtigungen zum Starten des Servers verfügt.
2. Stellen Sie für die Serverinstanz, die Sie starten wollen, sicher, dass Sie über die Berechtigung zum Lesen und Schreiben von Dateien im Serverinstanzverzeichnis verfügen. Stellen Sie sicher, dass die Datei `dmserv.opt` im Serverinstanzverzeichnis vorhanden ist und dass die Datei Parameter für die Serverinstanz enthält.
3. Wenn der Server mit einem Bandlaufwerk, einem Datenträgerwechsler oder mit einer Einheit für austauschbare Datenträger verbunden ist und Sie den Server mit der Instanzbenutzer-ID starten wollen, erteilen Sie der Instanzbenutzer-ID Schreib-/Lesezugriff für diese Einheiten. Führen Sie einen der folgenden Schritte aus, um Berechtigungen festzulegen:
  - Bei einem für IBM Spectrum Protect dediziertem System, auf das nur der IBM Spectrum Protect-Administrator zugreifen kann, erteilen Sie globale Schreibberechtigung für die Gerätedateien der Einheiten. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

```
chmod +w /dev/rmtX
```

- Verfügt das System über mehrere Benutzer, können Sie den Zugriff einschränken, indem Sie die IBM Spectrum Protect-Instanzbenutzer-ID zum Eigner der Gerätedateien der Einheit machen. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

```
chmod u+w /dev/rmtX
```

- Sind mehrere Benutzerinstanzen auf einem System aktiv, ändern Sie den Gruppennamen (z. B. TAPEUSERS) und fügen Sie jede IBM Spectrum Protect-Instanzbenutzer-ID dieser Gruppe hinzu. Übertragen Sie dann das Eigentumsrecht der Gerätedateien der Einheiten an die Gruppe TAPEUSERS und erteilen Sie Schreibberechtigung für die Gruppe. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

```
chmod g+w /dev/rmtX
```

4. Überprüfen Sie die folgenden Benutzergrenzwerte anhand der Richtlinien in der Tabelle.

Tabelle 1. Benutzergrenzwerte (ulimit-Werte)

| Typ des Benutzergrenzwerts                           | Bevorzugter Wert | Befehl zum Abfragen des Werts |
|--|------------------|-------------------------------|
| Maximale Größe erstellter Kerndateien                | Unlimited        | <code>ulimit -Hc</code>       |
| Maximale Größe eines Datensegments für einen Prozess | Unlimited        | <code>ulimit -Hd</code>       |
| Maximale Dateigröße                                  | Unlimited        | <code>ulimit -Hf</code>       |
| Maximale Anzahl offener Dateien                      | 65536            | <code>ulimit -Hn</code>       |
| Maximale Prozessorzeit in Sekunden                   | Unlimited        | <code>ulimit -Ht</code>       |

Für die Änderung von Benutzergrenzwerten befolgen Sie die Anweisungen in der Dokumentation Ihres Betriebssystems.


Tipp: Wenn Sie den Server mithilfe eines Scripts automatisch starten wollen, können Sie die Benutzergrenzwerte in dem Script definieren.

5. Stellen Sie sicher, dass als Benutzergrenzwert für die maximale Anzahl Benutzerprozesse (`nproc`-Einstellung) der empfohlene Mindestwert 16384 festgelegt wird.

- a. Geben Sie den Befehl `ulimit -Hu` mithilfe der Instanzbenutzer-ID aus, um den aktuellen Benutzergrenzwert zu überprüfen. Zum Beispiel:

```
[user@Machine ~]$ ulimit -Hu
16384
```

- b. Lautet der Grenzwert für die maximale Anzahl Benutzerprozesse nicht 16384, geben Sie den Wert 16384 an.

 AIX-Betriebssysteme Fügen Sie der Datei `/etc/security/limits` die folgende Zeile hinzu:

```
Instanzbenutzer-ID          -      nproc          16384
```

Hierbei gibt `Instanzbenutzer-ID` die Benutzer-ID der Serverinstanz an.

 AIX-Betriebssysteme

## AIX: Server mit der Instanzbenutzer-ID starten

---

Um den Server mit der Instanzbenutzer-ID zu starten, melden Sie sich mit der Instanzbenutzer-ID an und geben Sie im Serverinstanzverzeichnis den entsprechenden Befehl ein.

### Vorbereitende Schritte

---

Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden. Anweisungen siehe AIX: Zugriffsberechtigungen und Benutzergrenzwerte überprüfen.

### Vorgehensweise

---

1. Melden Sie sich bei dem System, auf dem IBM Spectrum Protect installiert ist, unter Verwendung der Instanzbenutzer-ID für den Server an.
2. Wenn Sie über kein Benutzerprofil zur Ausführung des Scripts `db2profile` verfügen, geben Sie den folgenden Befehl ein:


```
. /home/tsminst1/sqlllib/db2profile
```

Tipp: Anweisungen zur Aktualisierung des Benutzer-ID-Anmeldescripts zur automatischen Ausführung des Scripts `db2profile` finden Sie in der DB2-Dokumentation.


3. Geben Sie den folgenden Befehl in einer Zeile im Verzeichnis der Serverinstanz aus, um den Server zu starten:

 AIX-Betriebssysteme

```
LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K
usr/bin/dsmserv
```

 AIX-Betriebssysteme Achten Sie darauf, ein Leerzeichen hinter `SHMPSIZE=64K` einzufügen. Wenn Sie den Server mit diesem Befehl starten, aktivieren Sie 64-KB-Speicherseiten für den Server. Diese Einstellung hilft Ihnen bei der Optimierung der Serverleistung.

Tipp: Der Befehl wird im Vordergrund ausgeführt, sodass Sie eine Administrator-ID definieren und der Serverinstanz zuordnen können.

 AIX-Betriebssysteme Hat beispielsweise die Serverinstanz den Namen `tsminst1` und das Serverinstanzverzeichnis den Namen `/tsminst1`, können Sie die Instanz starten, indem Sie die folgenden Befehle ausgeben:

```
cd /tsminst1
. ~/sqlllib/db2profile
LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K
usr/bin/dsmserv
```

 AIX-Betriebssysteme

## AIX: Server automatisch starten

---

Sie können den Server so konfigurieren, dass er beim Systemstart automatisch gestartet wird. Zu diesem Zweck wird das Script `rc.dsmserv` zur Verfügung gestellt.

### Vorbereitende Schritte

---




Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden.

 AIX-Betriebssysteme Anweisungen finden Sie in Zugriffsberechtigungen und Benutzergrenzwerte überprüfen.

## Informationen zu diesem Vorgang

---

Das Script `rc.dsmserv` befindet sich im Serverinstallationsverzeichnis, z. B. in `/opt/tivoli/tsm/server/bin`.

 AIX-Betriebssysteme Tipp: Wenn Sie den Konfigurationsassistenten verwendet hatten, hatten Sie möglicherweise die Auswahl getroffen, den Server beim Systemneustart automatisch zu starten. Wenn Sie diese Auswahl getroffen hatten, wurde der Datei `/etc/inittab` automatisch ein Eintrag zum Starten des Servers hinzugefügt.

## Vorgehensweise

---

Wenn Sie keinen Assistenten zur Konfiguration des Servers verwendet haben, fügen Sie der Datei `/etc/inittab` für jeden Server, der automatisch gestartet werden soll, einen Eintrag hinzu:

1. Setzen Sie die Ausführungsebene auf den Wert, der dem Mehrbenutzermodus mit aktiviertem Netzbetrieb entspricht. Normalerweise ist der zu verwendende Wert für die Ausführungsebene abhängig vom Betriebssystem und seiner Konfiguration 2, 3 oder 5. Stellen Sie sicher, dass die Ausführungsebene in der Datei `/etc/inittab` mit der Ausführungsebene des Betriebssystems übereinstimmt. Weitere Informationen zum Mehrbenutzermodus und zu Ausführungsebenen enthält die Dokumentation zu Ihrem Betriebssystem.
2. Geben Sie im Befehl `rc.dsmserv` in der Datei `/etc/inittab` die Instanzbenutzer-ID mit der Option `-u` und die Position des Serverinstallationsverzeichnisses mit der Option `-i` an. Wenn mehrere Serverinstanzen automatisch gestartet werden sollen, fügen Sie für jede Serverinstanz einen Eintrag hinzu. Informationen zur Überprüfung der Syntax finden Sie in der Dokumentation zu Ihrem Betriebssystem.  
Tipp: Um eine Serverinstanz automatisch mit der Rootbenutzer-ID zu starten, verwenden Sie die Option `-U`.

## Beispiel

---

Hat beispielsweise der Instanzeigner den Namen `tsminst1` und das Serverinstallationsverzeichnis den Namen `/home/tsminst1/tsminst1`, fügen Sie `/etc/inittab` in einer einzigen Zeile den folgenden Eintrag hinzu:

 AIX-Betriebssysteme

```
tsm1:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst1  
-i /home/tsminst1/tsminst1 -q >/dev/console 2>&1
```

In diesem Beispiel ist die Prozess-ID `tsm1` und die Ausführungsebene ist mit 2 definiert.


Wenn Sie mehrere Serverinstanzen ausführen möchten, fügen Sie für jede Serverinstanz einen Eintrag hinzu. Sind beispielsweise die Instanzeigner-IDs `tsminst1` und `tsminst2` und die Instanzverzeichnisse `/home/tsminst1/tsminst1` und `/home/tsminst2/tsminst2` definiert, fügen Sie `/etc/inittab` die folgenden Einträge hinzu. Jeder Eintrag befindet sich in jeweils einer Zeile.

 AIX-Betriebssysteme

```
tsm1:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst1  
-i /home/tsminst1/tsminst1 -q >/dev/console 2>&1  
tsm2:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst2  
-i /home/tsminst2/tsminst2 -q >/dev/console 2>&1
```

### Zugehörige Verweise:

 Serverstartscript: `rc.dsmserv`

 AIX-Betriebssysteme

## AIX: Server im Verwaltungsmodus starten

---

Sie können den Server im Verwaltungsmodus starten, um Unterbrechungen während Verwaltungs- oder Rekonfigurationstasks zu vermeiden.

## Informationen zu diesem Vorgang

---

Führen Sie das Dienstprogramm `DSMSERV` mit dem Parameter `MAINTENANCE` aus, um den Server im Verwaltungsmodus zu starten.

Die folgenden Operationen sind im Verwaltungsmodus inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne

- Wiederherstellung von Speicherbereich auf dem Server
- Bestandsverfall
- Umlagerung von Speicherpools

Außerdem wird verhindert, dass Clients Sitzungen mit dem Server starten.

Tipps:

- Sie müssen die Serveroptionsdatei `dsmserv.opt` nicht bearbeiten, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Prozesse für die Speicherbereichswiederherstellung, den Bestandsverfall und die Speicherpoolumlagerung manuell starten.

## Vorgehensweise

---

Geben Sie den folgenden Befehl aus, um den Server im Verwaltungsmodus zu starten:

```
dsmserv maintenance
```

Tipp: Ein Video zum Starten des Servers im Verwaltungsmodus kann unter [Server im Verwaltungsmodus starten](#) angezeigt werden.

## Nächste Schritte

---

Gehen Sie wie folgt vor, um den Serverbetrieb im Produktionsmodus fortzusetzen:

1. Geben Sie den Befehl `HALT` aus, um den Server herunterzufahren:

```
halt
```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden.

Die während des Verwaltungsmodus inaktivierten Operationen werden wieder aktiviert.

## AIX: Server stoppen

---


Sie können den Server bei Bedarf stoppen, um die Steuerung an das Betriebssystem zurückzugeben. Um den Verlust von Verwaltungs- und Clientknotenverbindungen zu vermeiden, stoppen Sie den Server erst nach Beendigung oder Abbruch laufender Sitzungen.

### Informationen zu diesem Vorgang

---

Geben Sie den folgenden Befehl in die IBM Spectrum Protect-Befehlszeile ein, um den Server zu stoppen:

```
halt
```

 Wenn Sie keine Verbindung zum Server mit einem Verwaltungsclient herstellen können und wenn der Server gestoppt werden soll, müssen Sie den Prozess mit dem Befehl `kill` mit der Prozess-ID (PID) abbrechen. Die PID wird bei der Initialisierung angezeigt.

Wichtig: Bevor der Befehl `kill` eingegeben wird, müssen Sie sicherstellen, dass die korrekte Prozess-ID für den IBM Spectrum Protect-Server bekannt ist.

Die Prozess-ID des mit dem Befehl `kill` abzubrechenden Prozesses kann mithilfe der Datei `dsmserv.v6lock` in dem Verzeichnis, in dem der Server ausgeführt wird, ermittelt werden. Geben Sie Folgendes ein, um die Datei anzuzeigen:

```
cat /instance_dir/dsmserv.v6lock
```

 Geben Sie den folgenden Befehl aus, um den Server zu stoppen:

```
kill -36 dsmserv_pid
```

Hierbei steht `dsmserv_pid` für die Prozess-ID.

## AIX: Lizenzregistrierung

---

Registrieren Sie alle lizenzierten IBM Spectrum Protect-Funktionen, die Sie beziehen, sofort, damit Sie nach dem Starten der Serveroperationen (z. B. Datensicherung) keine Daten verlieren.

### Informationen zu diesem Vorgang

---

Verwenden Sie hierfür den Befehl `REGISTER LICENSE`. Weitere Informationen siehe `REGISTER LICENSE`.

## Beispiel: Lizenz registrieren

---

Die IBM Spectrum Protect-Basislizenz registrieren.

```
register license file=tsmbasic.lic
```

## AIX: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben

---

Sie müssen die zu verwendende Einheitenklasse angeben, um das System für automatische oder manuelle Datenbanksicherungen vorzubereiten.

### Vorbereitende Schritte

---

Stellen Sie sicher, dass eine Bandeinheitenklasse oder eine Einheitenklasse FILE definiert wurde. Ausführliche Informationen finden Sie in DEFINE DEVCLASS oder suchen Sie nach 'Einheitenklasse definieren'.

### Informationen zu diesem Vorgang

---

Gehen Sie wie folgt vor, um Ihr System für Datenbanksicherungen zu konfigurieren.

### Vorgehensweise

---

1. Wenn Sie den Server nicht mit dem Konfigurationsassistenten (dsmicfgx) konfiguriert haben, müssen Sie sicherstellen, dass die Schritte zur manuellen Konfiguration des Systems für Datenbanksicherungen ausgeführt werden.
2. Wählen Sie die für Datenbanksicherungen zu verwendende Einheitenklasse aus. Geben Sie den folgenden Befehl über eine IBM Spectrum Protect-Verwaltungsbefehlszeile aus.

```
set dbrecovery Einheitenklassenname
```

Die angegebene Einheitenklasse wird vom Datenbankmanager für Datenbanksicherungen verwendet. Wenn Sie keine Einheitenklasse mit dem Befehl SET DBRECOVERY angeben, schlägt die Sicherung fehl.

### Beispiel

---

Geben Sie beispielsweise den folgenden Befehl aus, um anzugeben, dass die Einheitenklasse DBBACK verwendet werden soll:


```
set dbrecovery dbback
```

## AIX: Mehrere Serverinstanzen auf einem System ausführen

---

Sie können mehrere Serverinstanzen auf Ihrem System erstellen. Jede Serverinstanz verfügt über ein eigenes Instanzverzeichnis sowie über Datenbank- und Protokollverzeichnisse.

Multiplizieren Sie den Speicherbedarf und andere Systemvoraussetzungen für einen Server mit der geplanten Instanzzahl für das System.

 **AIX-Betriebssysteme** Die Gruppe der Dateien für eine Instanz des Servers wird getrennt von den Dateien gespeichert, die von einer anderen Serverinstanz auf demselben System verwendet werden. Gehen Sie wie in AIX: Serverinstanz erstellen beschrieben für jede neue Instanz vor, einschließlich der Erstellung des neuen Instanzbenutzers.

Zur Verwaltung des von jedem Server verwendeten Systemspeichers begrenzen Sie mit der Serveroption DBMEMPERCENT den Prozentsatz des Systemspeichers. Haben alle Server denselben Stellenwert, verwenden Sie für jeden Server denselben Wert. Ist ein Server ein Produktionsserver und andere Server sind Testserver, geben Sie für den Produktionsserver einen höheren Wert an als für die Testserver.

Von Version 7.1 auf Version 8.1 ist ein direktes Upgrade möglich. Weitere Informationen finden Sie im Abschnitt über das Upgrade (Upgrade auf Version 8.1 durchführen). Wenn Sie ein Upgrade durchführen und mehrere Server auf dem System haben, müssen Sie den Installationsassistenten nur einmal ausführen. Der Installationsassistent erfasst die Datenbank- und Variablendaten für alle ursprünglichen Serverinstanzen.

Wenn Sie ein Upgrade von IBM Spectrum Protect Version 6.3 auf Version 8.1.3 durchführen und sich mehrere Server auf Ihrem System befinden, werden alle in DB2 Version 9.7 vorhandenen Instanzen gelöscht und in DB2 Version 11.1 erneut erstellt. Der Assistent gibt den Befehl `db2 upgrade DB DB-Name` für jede Datenbank aus. Die Datenbankumgebungsvariablen für jede Instanz auf Ihrem System werden ebenfalls während des Upgradeprozesses neu konfiguriert.

**Zugehörige Tasks:**

## AIX: Server überwachen

---

Wenn Sie den Server im Produktionsbetrieb einsetzen, überwachen Sie den von ihm verwendeten Speicherbereich, um sicherzustellen, dass die Größe des Speicherbereichs angemessen ist. Ändern Sie den Speicherbereich, falls erforderlich.

### Vorgehensweise

---

1. Überwachen Sie die aktive Protokolldatei, um sicherzustellen, dass die Größe für die Auslastung der Serverinstanz korrekt ist.

Wenn die Serverauslastung ihren normalen erwarteten Stand erreicht hat, belegt der von der aktiven Protokolldatei verwendete Speicherbereich 80 bis 90 Prozent des Speicherbereichs, der für das Verzeichnis für aktive Protokolldateien zur Verfügung steht. An diesem Punkt müssen Sie den Speicherbereich möglicherweise vergrößern. Die Vergrößerung des Speicherbereichs ist von der Art der Transaktionen in der Serververarbeitung abhängig. Transaktionsmerkmale wirken sich auf die Belegung des Speicherbereichs der aktiven Protokolldateien aus.

Die folgenden Transaktionsmerkmale können sich auf die Speicherbereichsbelegung in der aktiven Protokolldatei auswirken:

- Die Anzahl und Größe der Dateien in Sicherungsoperationen
  - Clients, wie z. B. Dateiserver, die zahlreiche kleine Dateien sichern, können zahlreiche Transaktionen verursachen, die in kurzer Zeit ausgeführt werden. Die Transaktionen können sehr viel Speicherbereich in der aktiven Protokolldatei belegen, jedoch nur für kurze Zeit.
  - Clients, wie z. B. E-Mail-Server oder ein Datenbankserver, die große Datenvolumen in wenigen Transaktionen sichern, können wenige Transaktionen verursachen, deren Ausführung viel Zeit in Anspruch nimmt. Die Transaktionen können wenig Speicherbereich in der aktiven Protokolldatei belegen, jedoch für lange Zeit.
- Netzverbindungstypen
  - Mit schnellen Netzverbindungen ausgeführte Sicherungsoperationen verursachen Transaktionen, die schneller ausgeführt werden. Die Transaktionen belegen Speicherbereich in der aktiven Protokolldatei über einen kürzeren Zeitraum.
  - Mit langsameren Verbindungen ausgeführte Sicherungsoperationen verursachen Transaktionen, deren Ausführung länger dauert. Die Transaktionen belegen Speicherbereich in der aktiven Protokolldatei über einen längeren Zeitraum.

Wenn der Server Transaktionen mit sehr unterschiedlichen Merkmalen verarbeitet, kann der für die aktive Protokolldatei verwendete Speicherbereich im Lauf der Zeit sehr stark schwanken. Für einen solchen Server müssen Sie unter Umständen dafür sorgen, dass ein niedrigerer Prozentsatz des Speicherbereichs der aktiven Protokolldatei verwendet wird. Der zusätzliche Speicherbereich gestattet eine Vergrößerung der aktiven Protokolldatei für Transaktionen, die viel Zeit in Anspruch nehmen.

2. Überwachen Sie das Archivprotokoll, um sicherzustellen, dass immer Speicherbereich verfügbar ist.  
Hinweis: Wenn das Archivprotokoll und das Übernahmearchivprotokoll voll werden, kann die aktive Protokolldatei voll werden, so dass der Server stoppt. Für das Archivprotokoll muss so viel Speicherbereich zur Verfügung stehen, dass dieser niemals vollständig belegt wird.

Sie werden wahrscheinlich Folgendes feststellen:

- a. Am Anfang wird das Archivprotokoll schnell größer, wenn normale Clientsicherungsoperationen ausgeführt werden.
- b. Datenbanksicherungen werden regelmäßig ausgeführt, entweder mit einem Zeitplan oder manuell.
- c. Nach mindestens zwei Datenbankgesamtsicherungen wird das Abschneiden des Protokolls automatisch ausgeführt. Der vom Archivprotokoll belegte Speicherbereich verringert sich durch das Abschneiden.
- d. Normale Clientoperationen werden fortgesetzt und das Archivprotokoll wird wieder größer.
- e. Datenbanksicherungen finden regelmäßig statt und die Häufigkeit der Protokollbereinigung ist von der Häufigkeit der Datenbankgesamtsicherungen abhängig.

Nach diesem Muster nimmt die Größe des Archivprotokolls zunächst zu, verringert sich und nimmt dann eventuell wieder zu. Im Laufe der Zeit sollte der vom Archivprotokoll belegte Speicherbereich während der normalen Verarbeitung einen relativ konstanten Stand erreichen.

Wenn die Größe des Archivprotokolls weiter zunimmt, sollten Sie eine oder beide der folgenden Maßnahmen in Betracht ziehen:

- Ordnen Sie dem Archivprotokoll weiteren Speicherbereich zu. Sie müssen unter Umständen das Archivprotokoll in ein anderes Dateisystem versetzen.
  - Erhöhen Sie die Häufigkeit der Datenbankgesamtsicherungen, so dass die Protokollbereinigung häufiger stattfindet.
3. Wenn Sie ein Verzeichnis für das Übernahmearchivprotokoll definiert haben, überprüfen Sie, ob darin Protokolle während der normalen Verarbeitung gespeichert werden. Wenn der Speicherbereich des Übernahmeprotokolls verwendet wird, sollten Sie das Archivprotokoll vergrößern. Das Übernahmearchivprotokoll sollte nur unter außergewöhnlichen Bedingungen verwendet werden, nicht während der normalen Verarbeitung.

# AIX: IBM Spectrum Protect-Server-Fixpack installieren

---

IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe.

## Vorbereitende Schritte

---

Damit ein Fixpack oder ein vorläufiger Fix auf dem Server installiert werden kann, müssen Sie den Server mit der Stufe installieren, auf der er ausgeführt werden soll. Sie müssen die Serverinstallation nicht mit dem Basisrelease beginnen. Wenn momentan beispielsweise Version 8.1.1 installiert ist, können Sie das aktuelle Fixpack für Version 8.1 direkt verwenden. Sie müssen nicht mit der Installation von Version 8.1.0 beginnen, wenn eine Wartungsaktualisierung verfügbar ist.

Das IBM Spectrum Protect-Lizenzpaket muss installiert sein. Das Lizenzpaket wird beim Kauf eines Basisreleases bereitgestellt. Wenn Sie ein Fixpack oder einen vorläufigen Fix von Fix Central herunterladen, installieren Sie die Serverlizenz, die auf der Website von Passport Advantage zur Verfügung steht. Sollen Nachrichten und Hilfetext nicht in Englisch angezeigt werden, installieren Sie das gewünschte Sprachenpaket.

Wenn Sie ein Upgrade des Servers auf Version 8.1.3 oder höher durchführen und den Server dann auf einen Stand vor Version 8.1.3 zurücksetzen, müssen Sie die Datenbank auf einen Zeitpunkt vor dem Upgrade zurückschreiben. Führen Sie während des Upgrades die erforderlichen Schritte aus, mit denen sichergestellt wird, dass die Datenbank zurückgeschrieben werden kann: Sichern Sie die Datenbank, die Protokolldatei für Datenträger, die Einheitenkonfigurationsdatei und die Serveroptionsdatei. Weitere Informationen finden Sie in AIX: Von Version 8.1.3 auf eine vorherige Serverversion zurücksetzen.

Wenn Sie den Clientverwaltungsservice verwenden, müssen Sie ein Upgrade dieses Service auf dieselbe Version wie beim IBM Spectrum Protect-Server durchführen.

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease des installierten Servers aufbewahrt werden. Wenn Sie IBM Spectrum Protect über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, sind die Installationsmedien für das Basisrelease des Servers für die Neuinstallation der Lizenz erforderlich.

Rufen Sie das IBM® Support Portal auf. Hier finden Sie folgende Informationen:

- Eine Liste der neuesten Wartungs- und Download-Fixes. Klicken Sie auf **Download** und legen Sie alle gültigen Fixes an.
- Informationen zum Erwerb eines Basislizenzpakets. Suchen Sie nach **Downloads > Passport Advantage**.
- Unterstützte Plattformen und Systemvoraussetzungen. Suchen Sie nach **IBM Spectrum Protect supported operating systems**.

Sie müssen ein Upgrade des Servers durchführen, bevor Sie ein Upgrade der Clients für Sichern/Archivieren durchführen. Wenn Sie das Upgrade des Servers nicht zuerst durchführen, könnte die Kommunikation zwischen dem Server und den Clients unterbrochen werden.

Achtung: Sie dürfen die DB2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der DB2-Software und führen Sie kein Upgrade durch, da dies die Datenbank beschädigen kann.

## Vorgehensweise

---

Führen Sie die folgenden Schritte aus, um ein Fixpack oder einen vorläufigen Fix zu installieren:

1. Sichern Sie die Datenbank. Die bevorzugte Methode ist eine Momentaufnahmesicherung. Bei einer Momentaufnahmesicherung handelt es sich um eine Datenbankgesamticherung, bei der geplante Datenbanksicherungen nicht unterbrochen werden. Geben Sie beispielsweise den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Sichern Sie die Einheitenkonfigurationsdaten. Geben Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

```
backup devconfig filenames=Dateiname
```



*Dateiname* gibt den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.

3. Speichern Sie die Protokolldatei für Datenträger in einem anderen Verzeichnis oder benennen Sie die Datei um. Geben Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

```
backup volhistory filenames=Dateiname
```

*Dateiname* gibt den Namen der Datei an, in der Datenträgerhistory-Informationen (Datenträgerprotokolldaten) gespeichert werden sollen.

4. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dsmserv.opt heißt. Die Datei befindet sich im Serverinstanzverzeichnis.

5. Halten Sie den Server vor der Installation eines Fixpacks oder eines vorläufigen Fixes an. Verwenden Sie den Befehl HALT.
6. Stellen Sie sicher, dass im Installationsverzeichnis zusätzlicher Speicherplatz zur Verfügung steht. Für die Installation dieses Fixpacks kann zusätzlicher temporärer Plattenspeicherplatz im Installationsverzeichnis des Servers erforderlich sein. Die Größe des zusätzlichen Plattenspeicherplatzes kann der Größe entsprechen, die für die Installation einer neuen Datenbank während einer IBM Spectrum Protect-Installation benötigt wird. Der IBM Spectrum Protect-Installationsassistent zeigt an, wie viel Speicherplatz für die Installation des Fixpacks benötigt wird und wie viel Platz zur Verfügung steht. Wenn der erforderliche Speicherplatz größer ist als der verfügbare Speicherplatz, stoppt die Installation. Wenn die Installation stoppt, fügen Sie dem Dateisystem den erforderlichen Plattenspeicherplatz hinzu und starten Sie die Installation erneut.
7.  Melden Sie sich als Root an.
8. Laden Sie die Paketdatei für das Fixpack bzw. den vorläufigen Fix, das bzw. der installiert werden soll, über IBM Support Portal, Passport Advantage oder Fix Central herunter.
9.  Wechseln Sie in das Verzeichnis, in dem sich die ausführbare Datei befindet, und führen Sie die folgenden Schritte aus.

Tipp: Die Dateien werden in das aktuelle Verzeichnis extrahiert. Stellen Sie sicher, dass sich die ausführbare Datei in dem Verzeichnis befindet, in dem sich die extrahierten Dateien befinden sollen.

- a. Geben Sie den folgenden Befehl ein, um die Dateiberechtigungen zu ändern:

```
chmod a+x 8.x.x.x-IBM-SPSRV-Plattform.bin
```

Hierbei steht *Plattform* für die Architektur, in der IBM Spectrum Protect installiert werden soll.

- b. Geben Sie den folgenden Befehl aus, um die Installationsdateien zu extrahieren:

```
./8.x.x.x-IBM-SPSRV-Plattform.bin
```

10. Wählen Sie eine der folgenden Möglichkeiten für die Installation von IBM Spectrum Protect aus.

Wichtig: Nach der Installation eines Fixpacks muss die Konfiguration nicht wiederholt werden. Sie können nach Beendigung der Installation stoppen, alle Fehler beheben und dann Ihre Server erneut starten.

Installieren Sie die IBM Spectrum Protect-Software mit einer der folgenden Methoden:

#### Installationsassistent

Befolgen Sie die Anweisungen für Ihr Betriebssystem:

AIX: IBM Spectrum Protect mit dem Installationsassistenten installieren

Tipp: Klicken Sie nach dem Start des Assistenten im Fenster von IBM Installation Manager auf das Symbol Aktualisieren. Klicken Sie nicht auf das Symbol Installieren oder Ändern.

#### Befehlszeile im Konsolenmodus

Befolgen Sie die Anweisungen für Ihr Betriebssystem:

AIX: IBM Spectrum Protect im Konsolenmodus installieren

#### Unbeaufsichtigter Modus

Befolgen Sie die Anweisungen für Ihr Betriebssystem:

AIX: IBM Spectrum Protect im unbeaufsichtigten Modus installieren



Tipp: Befinden sich mehrere Serverinstanzen auf Ihrem System, führen Sie den Installationsassistenten nur einmal aus. Der Installationsassistent führt ein Upgrade aller Serverinstanzen durch.

## Ergebnisse

Beheben Sie alle Fehler, die während des Installationsprozesses festgestellt werden.

Wenn Sie den Server mithilfe des Installationsassistenten installiert haben, können Sie Installationsprotokolle mithilfe des Tools IBM Installation Manager anzeigen. Klicken Sie auf Datei > Protokoll anzeigen. Um Protokolldateien zu erfassen, klicken Sie in IBM Installation Manager auf Hilfe > Daten zur Fehleranalyse exportieren.

Wenn Sie den Server im Konsolenmodus oder im unbeaufsichtigten Modus installiert haben, können Sie Fehlerprotokolle im IBM Installation Manager-Protokollverzeichnis anzeigen. Zum Beispiel:

-  /var/ibm/InstallationManager/logs
-  AIX: Fixpack auf IBM Spectrum Protect Version 8.1.3 in einer Clusterumgebung unter AIX anwenden  
IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe. Es ist möglich, ein Fixpack auf eine Clusterumgebung für AIX anzuwenden.

## AIX: Von Version 8.1.3 auf eine vorherige Serverversion zurücksetzen

Wenn Sie nach einem Upgrade auf die vorherige Version des Servers zurücksetzen müssen, benötigen Sie eine Datenbankgesamtsicherung der ursprünglichen Version. Außerdem benötigen Sie die Serverinstallationsmedien für Ihre ursprüngliche

Version und Schlüsselkonfigurationsdateien. Führen Sie die Schritte zur Vorbereitung sorgfältig aus, bevor Sie das Upgrade des Servers durchführen. Dadurch könnte das Zurücksetzen auf die vorherige Version des IBM Spectrum Protect-Servers mit minimalem Datenverlust möglich sein.

## Vorbereitende Schritte

---

Sie benötigen die folgenden Elemente aus der früheren Version des Servers:

- Serverdatenbanksicherung
- Protokolldatei für Datenträger
- Einheitenkonfigurationsdatei
- Serveroptionsdatei

## Informationen zu diesem Vorgang

---

Die Anweisungen sind für das Zurücksetzen innerhalb eines Releases oder von einem Release auf ein vorheriges Release identisch, z. B. von 8.1.3 auf 8.1.2 oder von 8.1.3 auf 7.1.2. Die ältere Version muss mit der Version übereinstimmen, die Sie vor dem Upgrade auf Version 8.1 verwendet haben.

Achtung: Geben Sie den Parameter REUSEDELAY an, um den Verlust von Daten des Clients für Sichern/Archivieren verhindern zu helfen, wenn Sie den Server auf eine vorherige Version zurücksetzen.


## Vorgehensweise beim Zurücksetzen auf vorherige Serverversion


---

### Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte auf dem System aus, auf dem sich der Server der Version 8.1 befindet.

### Vorgehensweise

1. Stoppen Sie den Server, um alle Serveroperationen zu beenden. Verwenden Sie hierfür den Befehl HALT.
2. Entfernen Sie die Datenbank aus dem Datenbankmanager und löschen Sie anschließend die Datenbank- und Wiederherstellungsprotokollverzeichnisse.
  - a. Entfernen Sie die Datenbank manuell. Eine Möglichkeit zum Entfernen ist der folgende Befehl:  AIX-Betriebssysteme

```
dsmserv removedb tsmdbl
```
  - b. Wenn Sie den von den Datenbank- und Wiederherstellungsprotokollverzeichnissen belegten Speicherplatz wiederverwenden müssen, können Sie diese Verzeichnisse jetzt löschen.
3. Deinstallieren Sie den Server der Version 8.1 mit dem Deinstallationsprogramm. Bei der Deinstallation werden der Server und der Datenbankmanager mit den jeweiligen Verzeichnissen entfernt. Ausführliche Informationen siehe AIX: IBM Spectrum Protect deinstallieren.
4. Stoppen Sie den Clusterdienst. Installieren Sie die Version des Serverprogramms, die Sie vor dem Upgrade auf Version 8.1.3 verwendet haben, erneut. Diese Version muss mit der Version übereinstimmen, die auf Ihrem Server verwendet wurde, als Sie die Datenbanksicherung erstellt haben, die Sie zu einem späteren Zeitpunkt wiederherstellen wollen. Wenn der Server vor dem Upgrade z. B. die Version 7.1.7 hatte und wenn Sie die Datenbanksicherung verwenden wollen, die auf diesem Server verwendet wurde, müssen Sie das Fixpack V7.1.7 installieren, damit Sie die Datenbanksicherung zurückschreiben können.
5. Konfigurieren Sie die neue Serverdatenbank mithilfe des Konfigurationsassistenten. Geben Sie den folgenden Befehl aus, um den Assistenten zu starten:  AIX-Betriebssysteme

```
./dsmicfgx
```
6. Stellen Sie sicher, dass keine Server im Hintergrund ausgeführt werden.
7. Schreiben Sie die Datenbank zu einem Zeitpunkt vor dem Upgrade zurück.
8. Kopieren Sie die folgenden Dateien in das Instanzverzeichnis.
  - Einheitenkonfigurationsdatei
  - Protokolldatei für Datenträger
  - Serveroptionsdatei (normalerweise dsmserv.opt)
9. Wenn Sie die Datendeduplizierung für Speicherpools des Typs FILE, die vor dem Upgrade vorhanden waren, aktiviert haben oder wenn Sie während der Verwendung des Servers der Version 8.1.3 Daten, die vor dem Upgrade vorhanden waren, in neue Speicherpools verschoben haben, müssen Sie zusätzliche Schritte ausführen. Weitere Informationen finden Sie in Zusätzliche Wiederherstellungsschritte wegen der Erstellung neuer Speicherpools oder der Aktivierung der Datendeduplizierung.
10. Wenn die Einstellung des Parameters REUSEDELAY für Speicherpools das Alter der zurückgeschriebenen Datenbank unterschreitet, schreiben Sie Datenträger auf allen Speicherpools mit sequenziellem Zugriff, die nach dieser Datenbanksicherung wiederhergestellt wurden, zurück. Verwenden Sie den Befehl RESTORE VOLUME.

Wenn keine Sicherung eines Speicherpools vorliegt, prüfen Sie die wiederhergestellten Datenträger mit dem Befehl `AUDIT VOLUME` und dem Parameter `FIX=YES`, um Inkonsistenzen zu beheben. Beispiel:

```
audit volume Datenträgername fix=yes
```

11. Wurden mit dem Server der Version 8.1 Clientsicherungs- oder -archivierungsoperationen ausgeführt, prüfen Sie die Speicherpooldatenträger, auf denen die Daten gespeichert wurden.

## Zusätzliche Wiederherstellungsschritte wegen der Erstellung neuer Speicherpools oder der Aktivierung der Datendeduplizierung

---

Wenn Sie während der Ausführung des Servers mit Version 8.1.3 neue Speicherpools erstellt und/oder die Datendeduplizierung für Speicherpools des Typs FILE aktiviert haben, müssen Sie zusätzliche Schritte ausführen, um die vorherige Serverversion wiederherzustellen.

### Vorbereitende Schritte

Für diese Task benötigen Sie eine Gesamtsicherung des Speicherpools, die vor dem Upgrade auf Version 8.1.3 erstellt wurde.

### Informationen zu diesem Vorgang

Verwenden Sie diese Informationen, wenn Sie einen oder beide der folgenden Schritte ausgeführt haben, während Ihr Server mit Version 8.1.3 ausgeführt wurde:

- Sie haben die Datendeduplizierungsfunktion für beliebige Speicherpools aktiviert, die vor dem Upgrade auf Version 8.1.3 bereits vorhanden waren. Die Datendeduplizierung ist nur für Speicherpools gültig, die den Einheitentyp FILE verwenden.
- Sie haben neue primäre Speicherpools nach dem Upgrade erstellt *und* Daten, die in anderen Speicherpools gespeichert waren, in die neuen Speicherpools versetzt.

Führen Sie diese Schritte aus, nachdem der Server wieder auf Version 7 zurückgesetzt wurde.

### Vorgehensweise

- Schreiben Sie für jeden Speicherpool, für den Sie die Datendeduplizierungsfunktion aktiviert haben, den gesamten Speicherpool mit dem Befehl `RESTORE STGPOOL` zurück.
- Bestimmen Sie für Speicherpools, die Sie nach dem Upgrade erstellt haben, welche Maßnahme durchzuführen ist. Daten, die aus vorhandenen Speicherpools der Version 8 in die neuen Speicherpools versetzt wurden, gehen möglicherweise verloren, weil die neuen Speicherpools auf Ihrem auf Version 8 zurückgesetzten Server nicht mehr vorhanden sind. Die Wiederherstellungsmaßnahmen sind vom Typ des Speicherpools abhängig:
  - Wurden Daten aus Speicherpools des Typs DISK der Version 8 in einen neuen Speicherpool versetzt, wurde der von den versetzten Daten belegte Speicherplatz wahrscheinlich wiederverwendet. Daher müssen Sie die ursprünglichen Speicherpools der Version 8 mithilfe der Speicherpoolsicherungen zurückschreiben, die vor dem Upgrade auf Version 8.1.3 erstellt wurden.

Wurden *keine* Daten aus Speicherpools des Typs DISK der Version 8 in einen neuen Speicherpool versetzt, müssen Sie die Speicherpooldatenträger in diesen Speicherpools des Typs DISK prüfen.

- Wurden Daten aus Speicherpools mit sequenziellem Zugriff der Version 8 in einen neuen Speicherpool versetzt, sind diese Daten möglicherweise noch vorhanden und sie können eventuell auf Speicherpooldatenträgern auf dem wiederhergestellten Server der Version 8 verwendet werden. Die Daten können verwendbar sein, wenn für den Parameter `REUSEDDELAY` des Speicherpools ein Wert definiert wurde, der die Wiederherstellung verhindert hat, während der Server mit der Version 8.1.3 ausgeführt wurde. Wurden Datenträger wiederhergestellt, während der Server mit der Version 8.1.3 ausgeführt wurde, müssen Sie diese Datenträger aus Speicherpoolsicherungen zurückschreiben, die vor dem Upgrade auf Version 8.1.3 erstellt wurden.

## AIX: Referenz: DB2-Befehle für IBM Spectrum Protect-Serverdatenbanken

---

Verwenden Sie diese Liste als Referenz, wenn der IBM® Support Sie anweist, DB2-Befehle auszugeben.

### Zweck

---


Nach der Installation und Konfiguration von IBM Spectrum Protect mithilfe der Assistenten müssen Sie DB2-Befehle nur selten verwenden. Eine begrenzte Gruppe von DB2-Befehlen, die Sie verwenden bzw. zu deren Verwendung Sie aufgefordert werden könnten, ist in Tabelle 1 aufgelistet. Diese Liste ist nicht umfassend, es handelt sich lediglich um ergänzende Informationen. Es besteht keine



Implikation, dass ein IBM Spectrum Protect-Administrator sie täglich oder regelmäßig verwendet. Beispiele einiger Befehle sind angegeben. Ausgabedaten sind nicht enthalten.

Vollständige Erläuterungen zu den hier beschriebenen Befehlen und zu deren Syntax finden Sie in der Produktinformation zu DB2.

Tabelle 1. DB2-Befehle

| Befehl              | Beschreibung  | Beispiel  |
|---------------------|---|---|
| db2icrt             | <p>Erstellt DB2-Instanzen im Ausgangsverzeichnis des Instanzeigners.</p> <p>Tipp: Der IBM Spectrum Protect-Konfigurationsassistent erstellt die vom Server und von der Datenbank verwendete Instanz. Nach der Installation und Konfiguration eines Servers mithilfe des Konfigurationsassistenten wird der Befehl db2icrt in der Regel nicht verwendet.</p> <p> Dieses Dienstprogramm befindet sich im Verzeichnis DB2DIR/instance. Hierbei steht DB2DIR für das Installationsverzeichnis, in dem die aktuelle Version des DB2-Datenbanksystems installiert ist.</p> | <p>IBM Spectrum Protect-Instanz manuell erstellen (geben Sie den Befehl in einer einzigen Zeile ein):</p> <pre data-bbox="1365 625 1507 842">/opt/tivoli /tsm/db2/in stance/ db2icrt -a server -u Instanznam e Instanznam e</pre> |
| db2set              | <p>Zeigt DB2-Variablen an.</p>  | <p>DB2-Variablen auflisten:</p> <pre data-bbox="1365 968 1442 989">db2set</pre>   |
| CATALOG DATABASE    | <p>Speichert Informationen zur Speicherposition der Datenbank im Systemdatenbankverzeichnis. Die Datenbank kann sich auf der lokalen Workstation oder auf einem fernen Datenbankpartitionsserver befinden. Der Serverkonfigurationsassistent kümmert sich um jeden Katalog, der zur Verwendung der Serverdatenbank benötigt wird. Führen Sie diesen Befehl nach der Konfiguration und Aktivierung eines Servers nur dann manuell aus, wenn es eine Änderung oder Beschädigung in der Umgebung gibt.</p>   | <p>Datenbank katalogisieren:</p> <pre data-bbox="1365 1115 1507 1188">db2 catalog database tsmdb1</pre>   |
| CONNECT TO DATABASE | <p>Stellt eine Verbindung zu einer angegebenen Datenbank für Befehlszeilenschnittstellenzwecke her.</p>   | <p>Eine Verbindung zur IBM Spectrum Protect-Datenbank über eine DB2-Befehlszeilenschnittstelle herstellen:</p> <pre data-bbox="1365 1566 1507 1598">db2 connect to tsmdb1</pre>   |

| Befehl  | Beschreibung   | Beispiel  |
|---|--|---|
| GET<br>DAT<br>ABA<br>SE<br>CON<br>FIG<br>URA<br>TIO<br>N                    | Gibt die Werte einzelner Einträge in einer bestimmten Datenbankkonfigurationsdatei zurück.<br>Wichtig: Dieser Befehl und seine Parameter werden direkt von DB2 definiert und verwaltet. Sie sind an dieser Stelle für Informationszwecke aufgelistet, um zu zeigen, wie die vorhandenen Einstellungen abgerufen werden können. Eine Änderung dieser Einstellungen könnte durch IBM Support oder Service-Bulletins wie z. B. APARs oder "Technical Guidance"-Dokumente (Technotes) empfohlen werden. Ändern Sie diese Einstellungen nicht manuell. Nehmen Sie eine Änderung nur nach einer entsprechenden Anweisung von IBM und nur mithilfe von IBM Spectrum Protect-Serverbefehlen oder -Prozeduren vor.  | Die Konfigurationsdaten für einen Datenbankaliasnamen anzeigen:<br><br>db2 get db<br>cfg for<br>tsmdb1<br><br>Informationen abrufen, um Einstellungen zu überprüfen (z. B. Datenbankkonfiguration, Protokollmodus und Pflege).<br><br>db2 get db<br>config for<br>tsmdb1<br>show detail |
| GET<br>DAT<br>ABA<br>SE<br>MAN<br>AGE<br>R<br>CON<br>FIG<br>URA<br>TIO<br>N | Gibt die Werte einzelner Einträge in einer bestimmten Datenbankkonfigurationsdatei zurück.<br>Wichtig: Dieser Befehl und seine Parameter werden direkt von DB2 definiert und verwaltet. Sie sind an dieser Stelle für Informationszwecke aufgelistet, um zu zeigen, wie die vorhandenen Einstellungen abgerufen werden können. Eine Änderung dieser Einstellungen könnte durch IBM Support oder Service-Bulletins wie z. B. APARs oder "Technical Guidance"-Dokumente (Technotes) empfohlen werden. Ändern Sie diese Einstellungen nicht manuell. Nehmen Sie eine Änderung nur nach einer entsprechenden Anweisung von IBM und nur mithilfe von IBM Spectrum Protect-Serverbefehlen oder -Prozeduren vor.  | Konfigurationsdaten für den Datenbankmanager abrufen:<br><br>db2 get dbm<br>cfg   |
| GET<br>HEA<br>LTH<br>SNA<br>PSH<br>OT                                       | Ruft die Informationen zum Allgemeinzustand für den Datenbankmanager und seine Datenbanken ab. Die zurückgegebenen Informationen stellen eine Momentaufnahme des Status zum Zeitpunkt der Befehlsausgabe dar. IBM Spectrum Protect überwacht den Status der Datenbank mithilfe der Diagnosemomentaufnahme und anderer Mechanismen, die von DB2 bereitgestellt werden. Es kann vorkommen, dass die Diagnosemomentaufnahme oder andere DB2-Dokumentation anzeigt, dass sich ein Element bzw. eine Datenbankressource im Alertstatus befindet. In einem solchen Fall müssen entsprechende Schritte zur Behebung der Situation in Betracht gezogen werden. IBM Spectrum Protect überwacht die Bedingung und reagiert entsprechend. Nicht alle deklarierten Alerts der DB2-Datenbank haben Maßnahmen zur Folge. | Einen Bericht über Anzeiger des DB2-Diagnosemonitors abrufen:<br><br>db2 get<br>health<br>snapshot<br>for<br>database on<br>tsmdb1  |

| Befehl                             | Beschreibung  | Beispiel  |
|------------------------------------|---|---|
| GRANT<br>(Datenbankberechtigungen) | Erteilt Berechtigungen, die sich auf die gesamte Datenbank beziehen, und keine Zugriffsrechte, die sich auf bestimmte Objekte in der Datenbank beziehen.  | Der Benutzer-ID itmuser Zugriffsberechtigung erteilen:<br><br>db2 GRANT<br>CONNECT ON<br>DATABASE<br>TO USER<br>itmuser<br>db2 GRANT<br>CREATETAB<br>ON DATABASE<br>TO USER<br>itmuser            |
| RUNSTATS                           | Aktualisiert statistische Daten zu den Merkmalen einer Tabelle und der zugeordneten Indizes oder Statistiksichten. Zu diesen Merkmalen gehören die Anzahl der Datensätze, die Anzahl der Seiten und die durchschnittliche Datensatzlänge.<br><br>Soll eine Tabelle angezeigt werden, verwenden Sie dieses Dienstprogramm nach dem Aktualisieren oder Reorganisieren der Tabelle.<br><br>Eine Sicht muss für die Optimierung aktiviert sein, damit ihre statistischen Daten für die Optimierung einer Abfrage verwendet werden können. Eine für die Optimierung aktivierte Sicht wird als Statistiksicht bezeichnet. Sie können eine Sicht mit der DB2-Anweisung ALTER VIEW für die Optimierung aktivieren. Verwenden Sie das Dienstprogramm RUNSTATS, wenn sich Änderungen zugrunde liegender Tabellen auf die von der Sicht zurückgegebenen Zeilen auswirken.<br><br>Tipp: Der Server konfiguriert DB2 so, dass der Befehl RUNSTATS nach Bedarf ausgeführt wird. | Statistische Daten für eine einzelne Tabelle aktualisieren.<br><br>db2<br>runstats on<br>table<br>SCHEMA_NAME<br>.TABLE_NAME<br>with<br>distribution<br>and<br>sampled<br>detailed<br>indexes all |
| SETSCHEMA                          | Ändert den Wert des Sonderregisters CURRENT SCHEMA als Vorbereitung für die direkte Ausgabe von SQL-Befehlen über die DB2-Befehlszeilenschnittstelle.<br>Tipp: Ein Sonderregister ist ein Speicherbereich, den der Datenbankmanager für einen Anwendungsprozess definiert. In diesem Bereich werden Informationen gespeichert, auf die in SQL-Anweisungen verwiesen werden kann.  | Das Schema für IBM Spectrum Protect festlegen:<br><br>db2 set<br>schema<br>tsmdb1   |
| START DATABASE MANAGER             | Startet die Hintergrundprozesse der aktuellen Datenbankmanagerinstanz. Der Server startet und stoppt die Instanz und die Datenbank bei jedem Start und Stopp des Servers.<br>Wichtig: Lassen Sie den Server das Starten und Stoppen der Instanz und der Datenbank steuern, sofern keine anderweitige Anweisung durch IBM Support vorliegt.  | Den Datenbankmanager starten:<br><br>db2start   |
| STOP DATABASE MANAGER              | Stoppt die aktuelle Datenbankmanagerinstanz. Der Datenbankmanager bleibt so lange aktiv, bis er explizit gestoppt wird. Dieser Befehl stoppt die Datenbankmanagerinstanz nicht, wenn Anwendungen mit Datenbanken verbunden sind. Liegen keine Datenbankverbindungen, aber Instanzverbindungen vor, erzwingt der Befehl zunächst das Stoppen der Instanzverbindungen. Dann wird der Datenbankmanager gestoppt. Dieser Befehl inaktiviert außerdem alle ausstehenden Datenbankaktivierungen, bevor der Datenbankmanager gestoppt wird.<br><br>Dieser Befehl ist auf einem Client nicht gültig.<br><br>Der Server startet und stoppt die Instanz und die Datenbank bei jedem Start und Stopp des Servers.<br><br>Wichtig: Lassen Sie den Server das Starten und Stoppen der Instanz und der Datenbank steuern, sofern keine anderweitige Anweisung durch IBM Support vorliegt.   | Den Datenbankmanager stoppen:<br><br>db2 stop<br>dbm  |

## AIX: IBM Spectrum Protect deinstallieren

Sie können IBM Spectrum Protect mit den folgenden Methoden deinstallieren. Vor dem Entfernen von IBM Spectrum Protect müssen Sie sicherstellen, dass Ihre Sicherungs- und Archivierungsdaten nicht verloren gehen.

## Vorbereitende Schritte

---

Führen Sie folgende Schritte aus, bevor Sie IBM Spectrum Protect deinstallieren:

- Führen Sie eine Gesamtsicherung der Datenbank aus.
- Speichern Sie eine Kopie der Datenträgerhistory- und Einheitenkonfigurationsdateien.
- Bewahren Sie die Ausgabedatenträger an einem sicheren Ort auf.

## Informationen zu diesem Vorgang

---

Sie können IBM Spectrum Protect mit jeder der folgenden Methoden deinstallieren: grafisch orientierter Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

- AIX: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren  
Sie können IBM Spectrum Protect mit dem Installationsassistenten von IBM® Installation Manager deinstallieren.
- AIX: IBM Spectrum Protect im Konsolenmodus deinstallieren  
Zum Deinstallieren von IBM Spectrum Protect mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.
- AIX: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren  
Zum Deinstallieren von IBM Spectrum Protect im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.
- AIX: IBM Spectrum Protect deinstallieren und erneut installieren  
Wenn Sie IBM Spectrum Protect nicht mit dem Assistenten, sondern manuell erneut installieren wollen, müssen Sie einige Maßnahmen ergreifen, um Ihre Serverinstanznamen und Datenbankverzeichnisse zu bewahren. Während einer Deinstallation werden alle bereits definierten Serverinstanzen entfernt, die Datenbankkataloge für diese Instanzen sind jedoch noch vorhanden.
- AIX: IBM Installation Manager deinstallieren  
Sie können IBM Installation Manager deinstallieren, wenn keine Produkte mehr vorhanden sind, die mit IBM Installation Manager installiert wurden.

## Nächste Schritte

---

Die Vorgehensweise für die Reinstallation der IBM Spectrum Protect-Komponenten finden Sie in AIX: Serverkomponenten installieren.

## AIX: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren


---

Sie können IBM Spectrum Protect mit dem Installationsassistenten von IBM® Installation Manager deinstallieren.

### Vorgehensweise

---

1. Starten Sie Installation Manager.

 In dem Verzeichnis, in dem Installation Manager installiert ist, wechseln Sie in das Unterverzeichnis eclipse (z. B. /opt/IBM/InstallationManager/eclipse) und geben Sie folgenden Befehl aus:

```
./IBMIM
```

2. Klicken Sie auf Deinstallieren.
3. Wählen Sie IBM Spectrum Protect-Server aus und klicken Sie auf Weiter.
4. Klicken Sie auf Deinstallieren.
5. Klicken Sie auf Fertigstellen.


## AIX: IBM Spectrum Protect im Konsolenmodus deinstallieren

---



Zum Deinstallieren von IBM Spectrum Protect mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.

### Vorgehensweise

---

1. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das folgende Unterverzeichnis:
  -  eclipse/tools

Beispiel:

-  AIX-Betriebssysteme/opt/IBM/InstallationManager/eclipse/tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus:
    -  AIX-Betriebssysteme ./imcl -c
  3. Für die Deinstallation geben Sie 5 ein.
  4. Wählen Sie die Deinstallation aus der IBM Spectrum Protect-Paketgruppe aus.
  5. Geben Sie N für 'Next' (Weiter) ein.
  6. Wählen Sie die Deinstallation des IBM Spectrum Protect-Serverpakets aus.
  7. Geben Sie N für 'Next' (Weiter) ein.
  8. Geben Sie U für 'Uninstall' (Deinstallieren) ein.
  9. Geben Sie F für 'Finish' (Fertigstellen) ein.

## AIX: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren

---

Zum Deinstallieren von IBM Spectrum Protect im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.

### Vorbereitende Schritte

---


Sie können die Dateneingabe für eine unbeaufsichtigte Deinstallation der IBM Spectrum Protect-Serverkomponenten mithilfe einer Antwortdatei bereitstellen. IBM Spectrum Protect enthält eine Musterantwortdatei, `uninstall_response_sample.xml`, im Verzeichnis `input`, in dem das Installationspaket extrahiert wird. Diese Datei enthält Standardwerte, durch die Sie unnötige Warnungen vermeiden können.

Wenn Sie alle IBM Spectrum Protect-Komponenten deinstallieren wollen, lassen Sie die Einstellung `modify="false"` für jede Komponente in der Antwortdatei unverändert. Wenn Sie eine Komponente nicht deinstallieren wollen, geben Sie den Wert `modify="true"` an.


Wenn Sie die Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

### Vorgehensweise

---

1. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das folgende Unterverzeichnis:
  -  AIX-Betriebssysteme/eclipse/tools

Beispiel:

-  AIX-Betriebssysteme/opt/IBM/InstallationManager/eclipse/tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus, wobei *Antwortdatei* den Pfad der Antwortdatei einschließlich des Dateinamens angibt:

 AIX-Betriebssysteme

```
./imcl -input Antwortdatei -silent
```

Der folgende Befehl ist ein Beispiel:

 AIX-Betriebssysteme

```
./imcl -input /tmp/input/uninstall_response.xml -silent
```

## AIX: IBM Spectrum Protect deinstallieren und erneut installieren


---

Wenn Sie IBM Spectrum Protect nicht mit dem Assistenten, sondern manuell erneut installieren wollen, müssen Sie einige Maßnahmen ergreifen, um Ihre Serverinstanzen und Datenbankverzeichnisse zu bewahren. Während einer Deinstallation werden alle bereits definierten Serverinstanzen entfernt, die Datenbankkataloge für diese Instanzen sind jedoch noch vorhanden.

### Informationen zu diesem Vorgang

---

Gehen Sie wie folgt vor, um IBM Spectrum Protect manuell zu deinstallieren und erneut zu installieren:

1.  AIX-Betriebssysteme Erstellen Sie eine Liste Ihrer aktuellen Serverinstanzen, bevor Sie mit der Deinstallation beginnen. Führen Sie den folgenden Befehl aus:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

2. Führen Sie die folgenden Befehle für jede Serverinstanz aus:

 AIX-Betriebssysteme

```
db2 attach to Instanzname
db2 get dbm cfg show detail
db2 detach
```

Notieren Sie den Datenbankpfad für jede Instanz.

3. Deinstallieren Sie IBM Spectrum Protect. Siehe AIX: IBM Spectrum Protect deinstallieren.
4. Wenn Sie eine beliebige unterstützte Version von IBM Spectrum Protect deinstallieren (einschließlich Fixpack), wird eine Instanzdatei erstellt. Die Instanzdatei wird erstellt, um die Reinstallation von IBM Spectrum Protect zu erleichtern. Überprüfen Sie diese Datei und verwenden Sie die Informationen, wenn Sie bei der Reinstallation zur Eingabe der Berechtigungsnachweise der Instanz aufgefordert werden. Bei der unbeaufsichtigten Installation geben Sie diese Berechtigungsnachweise mit der Variablen `INSTANCE_CRED` an.

Sie finden die Instanzdatei an der folgenden Position:

-  AIX-Betriebssysteme/etc/tivoli/tsm/instanceList.obj

5. Installieren Sie IBM Spectrum Protect erneut. Siehe AIX: Serverkomponenten installieren.

Ist die Datei `instanceList.obj` nicht vorhanden, müssen Sie Ihre Serverinstanzen wie folgt erneut erstellen:


- a. Erstellen Sie Ihre Serverinstanzen erneut. Siehe AIX: Serverinstanz erstellen.

Tipp: Der Installationsassistent konfiguriert die Serverinstanzen, Sie müssen jedoch überprüfen, ob sie vorhanden sind. Wenn sie nicht vorhanden sind, müssen Sie sie manuell konfigurieren.

- b. Katalogisieren Sie die Datenbank. Melden Sie sich bei jeder Serverinstanz nacheinander als Instanzbenutzer an und geben Sie folgende Befehle aus:

 AIX-Betriebssysteme

```
db2 catalog database tsmdb1
db2 attach to Instanzname
db2 update dbm cfg using dftdbpath Instanzverzeichnis
db2 detach
```

- c.  AIX-Betriebssysteme Überprüfen Sie, ob die Serverinstanz erfolgreich erstellt wurde. Geben Sie den folgenden Befehl aus:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

- d. Überprüfen Sie, ob IBM Spectrum Protect die Serverinstanz erkennt, indem Sie Ihre Verzeichnisse auflisten. Ihr Ausgangsverzeichnis wird angezeigt, wenn Sie es nicht geändert haben. Ihr Instanzverzeichnis wird angezeigt, wenn Sie den Konfigurationsassistenten verwendet haben. Geben Sie den folgenden Befehl aus:

```
db2 list database directory
```

Wenn Sie TSMDB1 in der Liste finden, können Sie den Server starten.

## AIX: IBM Installation Manager deinstallieren

---

Sie können IBM® Installation Manager deinstallieren, wenn keine Produkte mehr vorhanden sind, die mit IBM Installation Manager installiert wurden.

### Vorbereitende Schritte

---

Bevor Sie IBM Installation Manager deinstallieren, müssen Sie sicherstellen, dass alle mit IBM Installation Manager installierten Pakete deinstalliert sind. Schließen Sie IBM Installation Manager, bevor Sie den Deinstallationsprozess starten.

 AIX-Betriebssysteme Geben Sie den folgenden Befehl in eine Befehlszeile ein, um installierte Pakete anzuzeigen:

```
cd /opt/IBM/InstallationManager/eclipse/tools
./imcl listInstalledPackages
```

### Vorgehensweise

---

Gehen Sie wie folgt vor, um IBM Installation Manager zu deinstallieren:

 AIX-Betriebssysteme

1. Öffnen Sie eine Befehlszeile und wechseln Sie in das Verzeichnis `/var/ibm/InstallationManager/uninstall`.
2. Geben Sie den folgenden Befehl aus:

```
./uninstall
```

Einschränkung: Sie müssen mit der Benutzer-ID `root` am System angemeldet sein.

## Linux: Server installieren

---



Zur Installation des Servers gehören Planung, Installation und Erstkonfiguration.

- Linux
- Linux: Installation des Servers planen  
Installieren Sie die Server-Software auf dem Computer, der Speichereinheiten verwaltet, und die Client-Software auf jeder Workstation, die Daten an den vom IBM Spectrum Protect-Server verwalteten Speicher überträgt.
- Linux: Serverkomponenten installieren  
Für die Installation der Serverkomponenten der Version 8.1.3 können Sie den Installationsassistenten, die Befehlszeile im Konsolenmodus oder den unbeaufsichtigten Modus verwenden.
- Linux: Die ersten Schritte nach der Installation von IBM Spectrum Protect  
Nach der Installation von Version 8.1.3 bereiten Sie die Konfiguration vor. Bevorzugte Methode für die Konfiguration der IBM Spectrum Protect-Instanz ist die Verwendung des Konfigurationsassistenten.
- Linux: IBM Spectrum Protect-Server-Fixpack installieren  
IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe.
- Linux: Von Version 8.1.3 auf eine vorherige Serverversion zurücksetzen  
Wenn Sie nach einem Upgrade auf die vorherige Version des Servers zurücksetzen müssen, benötigen Sie eine Datenbankgesamticherung der ursprünglichen Version. Außerdem benötigen Sie die Serverinstallationsmedien für Ihre ursprüngliche Version und Schlüsselkonfigurationsdateien. Führen Sie die Schritte zur Vorbereitung sorgfältig aus, bevor Sie das Upgrade des Servers durchführen. Dadurch könnte das Zurücksetzen auf die vorherige Version des IBM Spectrum Protect-Servers mit minimalem Datenverlust möglich sein.
- Linux: Referenz: DB2-Befehle für IBM Spectrum Protect-Serverdatenbanken  
Verwenden Sie diese Liste als Referenz, wenn der IBM® Support Sie anweist, DB2-Befehle auszugeben.
- Linux: IBM Spectrum Protect deinstallieren  
Sie können IBM Spectrum Protect mit den folgenden Methoden deinstallieren. Vor dem Entfernen von IBM Spectrum Protect müssen Sie sicherstellen, dass Ihre Sicherungs- und Archivierungsdaten nicht verloren gehen.

## Linux: Installation des Servers planen

---

Installieren Sie die Server-Software auf dem Computer, der Speichereinheiten verwaltet, und die Client-Software auf jeder Workstation, die Daten an den vom IBM Spectrum Protect-Server verwalteten Speicher überträgt.

- Linux: Vorausgesetzte Kenntnisse  
Sie müssen mit Ihren Betriebssystemen, Speichereinheiten, Übertragungsprotokollen und Systemkonfigurationen vertraut sein, bevor Sie IBM Spectrum Protect installieren.
- Linux: Planung für optimale Leistung  
Überprüfen Sie vor der Installation des IBM Spectrum Protect-Servers die Merkmale und die Konfiguration des Systems, um sicherzustellen, dass der Server für die optimale Leistung konfiguriert ist.
-  Linux-Betriebssysteme  
Linux: Systemmindestvoraussetzungen für Linux-Systeme  
Für die Installation des IBM Spectrum Protect-Servers auf einem Linux-System wird ein Minimum an Hardware und Software benötigt. Hierzu gehören eine Übertragungsmethode und der aktuelle Einheitentreiber.
-  Linux-Betriebssysteme  
Linux: Kompatibilität des IBM Spectrum Protect-Servers mit anderen DB2-Produkten auf dem System  
Sie können andere Produkte, die DB2-Produkte auf demselben System wie der IBM Spectrum Protect-Server der Version 8.1.3 implementieren und verwenden, mit einigen Einschränkungen installieren.
- Linux: IBM Installation Manager  
IBM Spectrum Protect verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositories installiert oder aktualisiert werden können.
- Linux: Arbeitsblätter für Planungsdetails für den Server  
Sie können die Arbeitsblätter für die Planung der Größe und der Position des für den IBM Spectrum Protect-Server benötigten Speichers verwenden. Sie können darauf auch Namen und Benutzer-IDs aufzeichnen.
- Linux: Kapazitätsplanung  
Zur Kapazitätsplanung für IBM Spectrum Protect gehört die Verwaltung von Ressourcen wie z. B. die Datenbank, das Wiederherstellungsprotokoll und der Bereich für gemeinsam genutzte Ressourcen. Sie müssen den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll schätzen, um die Ressourcen als Teil der Kapazitätsplanung zu maximieren. Der verfügbare Speicherplatz für den Bereich für gemeinsam genutzte Ressourcen muss für jede Installation bzw. jedes Upgrade ausreichen.
- Linux: Empfehlungen für die Serverbenennung  
Verwenden Sie diese Beschreibungen als Referenz bei der Installation oder beim Upgrade eines IBM Spectrum Protect-Servers.
- Linux: Installationsverzeichnisse  
Zu den Installationsverzeichnissen für den IBM Spectrum Protect-Server gehören die Verzeichnisse für den Server, DB2, die


Einheiten, die Sprache und andere Verzeichnisse. Jedes Verzeichnis enthält mehrere zusätzliche Verzeichnisse.

## Linux: Vorausgesetzte Kenntnisse

---

Sie müssen mit Ihren Betriebssystemen, Speichereinheiten, Übertragungsprotokollen und Systemkonfigurationen vertraut sein, bevor Sie IBM Spectrum Protect installieren.

Wartungsreleases, Client-Software und Veröffentlichungen für den Server stehen im IBM® Support Portal zur Verfügung.

 **Linux-Betriebssysteme**Einschränkung: Sie können den Server der Version 8.1.3 mit einigen Einschränkungen auf einem System installieren und ausführen, auf dem bereits DB2 installiert ist. Das gilt unabhängig davon, ob DB2 separat oder als Teil einer anderen Anwendung installiert wurde. Ausführliche Informationen finden Sie in dem Abschnitt über die Kompatibilität mit anderen DB2-Produkten.

Erfahrene DB2-Administratoren können erweiterte SQL-Abfragen durchführen und mithilfe von DB2-Tools die Datenbank überwachen. Sie dürfen die DB2-Tools jedoch nicht zur Änderung der von IBM Spectrum Protect vorgegebenen DB2-Konfigurationseinstellungen verwenden oder die DB2-Umgebung für IBM Spectrum Protect auf andere Weise ändern (z. B. mit anderen Produkten). Der Server der Version 8.1.3 wurde mit der Datendefinitionssprache (DDL) und der vom Server implementierten Datenbankkonfiguration erstellt und ausführlich getestet.

**Achtung:** Sie dürfen die DB2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der DB2-Software und führen Sie kein Upgrade durch, da dies die Datenbank beschädigen kann.

## Linux: Planung für optimale Leistung

---

Überprüfen Sie vor der Installation des IBM Spectrum Protect-Servers die Merkmale und die Konfiguration des Systems, um sicherzustellen, dass der Server für die optimale Leistung konfiguriert ist.

### Vorgehensweise

---

1. Lesen Sie den Abschnitt Linux: Vorausgesetzte Kenntnisse.
2. Lesen Sie jeden der folgenden Unterabschnitte.
  - **Linux: Planung für die Server-Hardware und das Betriebssystem**  
Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
  - **Linux: Planung für Platten für die Serverdatenbank**  
Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
  - **Linux: Planung für Platten für das Serverwiederherstellungsprotokoll**  
Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
  - **Linux: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools**  
Überprüfen Sie die Konfiguration Ihrer Verzeichniscontainer- und Cloud-Containerspeicherpools, um eine optimale Leistung zu gewährleisten.
  - **Linux: Planung für Speicherpools auf DISK- oder FILE-Einheiten**  
Überprüfen Sie mithilfe der Prüfliste, wie Ihre Plattenspeicherpools konfiguriert sind. Diese Prüfliste umfasst Tipps für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden.
  - **Linux: Planung für die Auswahl des korrekten Speichertechnologietyps**  
Speichereinheiten haben eine unterschiedliche Kapazität und unterschiedliche Leistungsmerkmale. Diese Merkmale wirken sich darauf aus, welche Einheiten besser für die Verwendung mit IBM Spectrum Protect geeignet sind.
  - **Linux: Bewährte Verfahren bei der Serverinstallation anwenden**  
Normalerweise hat die Konfiguration und Auswahl der Hardware die deutlichsten Auswirkungen auf die Leistung einer IBM Spectrum Protect-Lösung. Weitere Faktoren, die sich auf die Leistung auswirken, sind die Auswahl und Konfiguration des Betriebssystems sowie die Konfiguration von IBM Spectrum Protect.

## Linux: Planung für die Server-Hardware und das Betriebssystem





---

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.



| Frage   | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen   |
|---|--|---|
| <p>Werden die Betriebssystem- und Hardwarevoraussetzungen erfüllt oder mehr als erfüllt?</p> <ul style="list-style-type: none"> <li>• Anzahl und Geschwindigkeit der Prozessoren</li> <li>• Systemspeicher</li> <li>• Unterstützte Betriebssystemversion</li> </ul> | <p>Wenn Sie die erforderliche Mindestspeicherkapazität verwenden, können Sie eine minimale Arbeitslast unterstützen.</p> <p>Sie können versuchsweise mehr Systemspeicher hinzufügen, um bestimmen zu können, ob sich die Leistung verbessert. Entscheiden Sie dann, ob der Systemspeicher dem Server zugeordnet bleiben soll. Testen Sie die verschiedenen Speicherkapazitäten jeweils anhand des gesamten Tageszyklus der Serverlast.</p> <p>Wenn Sie mehrere Server auf dem System ausführen, addieren Sie die Voraussetzungen für jeden Server, um die Voraussetzungen für das System zu bestimmen.</p> | <p>Überprüfen Sie die Betriebssystemvoraussetzungen in Technote 1243309.</p> <p>Lesen Sie außerdem die Anweisungen in Tasks für Betriebssysteme und andere Anwendungen optimieren.</p> <p>Weitere Informationen zu Voraussetzungen, wenn die entsprechenden Funktionen verwendet werden, finden Sie in den folgenden Abschnitten:</p> <ul style="list-style-type: none"> <li>• Prüfliste für Datendeduplizierung</li> <li>• Prüfliste für Knotenreplikation</li> </ul> <p>Weitere Informationen zu Anforderungen in Bezug auf die Größe des Servers und des Speichers finden Sie im IBM Spectrum Protect-Blueprint.</p> |
| <p>Sind Platten für die optimale Leistung konfiguriert?</p>   | <p>Der Umfang der Optimierung, der für verschiedene Plattensysteme erfolgen kann, variiert. Stellen Sie sicher, dass die Warteschlangenlänge und andere Plattensystemoptionen entsprechend definiert sind.</p>   | <p>Weitere Informationen finden Sie in:</p> <ul style="list-style-type: none"> <li>• "Planung für Platten für die Serverdatenbank"</li> <li>• "Planung für Platten für das Serverwiederherstellungsprotokoll"</li> <li>• "Planung für Speicherpools auf DISK- oder FILE-Einheiten"</li> </ul>   |

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen   |
|---|--|---|
| <p>Verfügt der Server über genügend Speicher?</p>   | <p>Höhere Arbeitslasten und erweiterte Funktionen wie beispielsweise Datendeduplizierung und Knotenreplikation erfordern mehr Systemspeicher als den Mindestspeicher, der im Dokument mit den Systemvoraussetzungen angegeben ist. Verwenden Sie die folgenden Richtlinien, um den Speicherbedarf für Datenbanken anzugeben, die nicht für die Datendeduplizierung aktiviert sind:</p> <ul style="list-style-type: none"> <li>• Für Datenbanken mit einer Größe unter 500 GB benötigen Sie 16 GB Speicher.</li> <li>• Für Datenbanken mit einer Größe von 500 GB bis 1 TB benötigen Sie 24 GB Speicher.</li> <li>• Für Datenbanken mit einer Größe von 1 TB bis 1,5 TB benötigen Sie 32 GB Speicher.</li> <li>• Für Datenbanken mit einer Größe über 1,5 TB benötigen Sie 40 GB Speicher.</li> </ul> <p>Stellen Sie sicher, dass Sie für die Replikationsverarbeitung zusätzlichen Speicherbereich für die aktive Protokolldatei und das Archivprotokoll zuordnen.</p> | <p>Weitere Informationen zu Voraussetzungen, wenn die entsprechenden Funktionen verwendet werden, finden Sie in den folgenden Abschnitten:</p> <ul style="list-style-type: none"> <li>• Prüfliste für Datendeduplizierung</li> <li>• Prüfliste für Knotenreplikation</li> <li>• Speicherbedarf</li> </ul> |
| <p>Verfügt das System über genügend Hostbusadapter (HBAs), um die Datenoperationen, die der IBM Spectrum Protect-Server gleichzeitig ausführen muss, handhaben zu können?</p> | <p>Sie müssen wissen, für welche Operationen die gleichzeitige Verwendung von Hostbusadaptern erforderlich ist.</p> <p>Ein Server muss beispielsweise Sicherungsdaten mit 1 GB/s speichern, während er gleichzeitig eine Speicherpoolumlagerung ausführt, für deren Ausführung eine Kapazität von 0,5 GB/s erforderlich ist. Die Hostbusadapter müssen alle Daten mit der erforderlichen Geschwindigkeit handhaben können.</p>   | <p>Siehe HBA-Kapazität optimieren.</p>  |

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen   |
|--|---|---|
| Ist die Netzbandbreite größer als der geplante maximale Durchsatz für Sicherungen?   | <p>Die Netzbandbreite muss dem System die Ausführung von Operationen wie Sicherungen innerhalb der zulässigen Zeit oder gemäß den vereinbarten Service-Levels ermöglichen.</p> <p>Bei der Knotenreplikation muss die Netzbandbreite größer als der geplante maximale Durchsatz sein.</p>  | <p>Weitere Informationen finden Sie in:</p> <ul style="list-style-type: none"> <li>• Netzleistung optimieren</li> <li>• Prüfliste für Knotenreplikation</li> </ul>  |
| Verwenden Sie ein bevorzugtes Dateisystem für IBM Spectrum Protect-Serverdateien?  | <p>Verwenden Sie ein Dateisystem, das optimale Leistung und Datenverfügbarkeit gewährleistet. Der Server verwendet die direkte E/A mit Dateisystemen, die die Funktion unterstützen. Die Verwendung der direkten E/A kann den Durchsatz verbessern und die Prozessornutzung verringern. Weitere Informationen zum bevorzugten Dateisystem für Ihr Betriebssystem finden Sie in IBM Spectrum Protect server-supported file systems.</p>  | <p>Weitere Informationen finden Sie in Betriebssystem für die Plattenleistung konfigurieren.</p>  |
| Planen Sie, genügend Seitenauslagerungsbereich zu konfigurieren?   | <p>Seitenauslagerungsbereich (oder Auslagerungsspeicher) erweitert den Speicher, der für die Verarbeitung verfügbar ist. Wenn der freie Arbeitsspeicher im System knapp wird, werden Programme oder Daten, die nicht im Gebrauch sind, aus dem Speicher in den Seitenauslagerungsbereich versetzt. Mit dieser Aktion wird Speicherbereich für andere Aktivitäten, wie z. B. Datenbankoperationen, freigegeben.</p> <p> Linux-Betriebssysteme Verwenden Sie den größeren der beiden folgenden Werte: mindestens 32 GB Seitenauslagerungsbereich oder 50 % des Arbeitsspeichers.</p> |   |
|  Linux-Betriebssysteme Planen Sie, nach der Installation des Servers die Kernelparameter zu optimieren? |  Linux-Betriebssysteme Sie müssen Kernelparameter optimieren.  |  Linux-Betriebssysteme Informationen zur Optimierung von Kernelparametern finden Sie in Linux: Kernelparameter für Linux-Systeme optimieren. |

## Linux: Planung für Platten für die Serverdatenbank

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen  |
|--|---|--|
| Befindet sich die Datenbank auf schnellen Platten mit kurzer Latenzzeit?   | <p>Verwenden Sie die folgenden Laufwerke nicht für die IBM Spectrum Protect-Datenbank:</p> <ul style="list-style-type: none"> <li>• Nearline SAS (NL-SAS)</li> <li>• Serial Advanced Technology Attachment (SATA)</li> <li>• Parallel Advanced Technology Attachment (PATA)</li> </ul> <p>Verwenden Sie keine internen Platten, die standardmäßig Teil der Hardware der meisten Server ist.</p> <p>Enterprise-Solid-State-Laufwerke mit Fibre Channel- oder SAS-Schnittstellen bieten die beste Leistung.</p> <p>Wenn Sie planen, die Dateneduplizierungsfunktionen von IBM Spectrum Protect zu verwenden, legen Sie den Schwerpunkt auf die Plattenleistung (gemessen in E/A-Operationen pro Sekunde).</p> | Weitere Informationen finden Sie in Prüfliste für Dateneduplizierung.  |
| Ist die Datenbank auf anderen Platten oder LUNs gespeichert als die aktive Protokolldatei, das Archivprotokoll und die Speicherpooldatenträger?                      | Das Trennen der Serverdatenbank von anderen Serverkomponenten trägt zur Reduktion von Konkurrenzsituationen für dieselben Ressourcen durch unterschiedliche Operationen, die gleichzeitig ausgeführt werden müssen, bei.<br>Tipp: Die Datenbank und das Archivprotokoll können ein Array gemeinsam nutzen, wenn Sie die Solid-State-Laufwerk-Technologie (SSD-Technologie) verwenden.   |  |
| Wissen Sie bei Verwendung von RAID, wie die optimale RAID-Stufe für Ihr System ausgewählt wird? Definieren Sie alle LUNs mit derselben Größe und demselben RAID-Typ? | <p>Wenn ein System viele Schreibvorgänge ausführen muss, ist die Leistung bei RAID 10 besser als bei RAID 5. RAID 10 benötigt jedoch mehr Platten als RAID 5, um dieselbe nutzbare Speichermenge bereitzustellen.</p> <p>Handelt es sich bei Ihrem Plattensystem um ein RAID-System, definieren Sie alle LUNs mit derselben Größe und demselben RAID-Typ. Verwenden Sie beispielsweise nicht gleichzeitig 4+1 RAID 5 mit 4+2 RAID 6.</p>  |  |
| Planen Sie, wenn eine Option zum Definieren der Stripgröße oder der Segmentgröße verfügbar ist, die Größe beim Konfigurieren des Plattensystems zu optimieren?       | Wenn Sie die Stripgröße oder Segmentgröße definieren können, verwenden Sie auf Plattensystemen für die Datenbank Größen von 64 KB oder 128 KB.  | Die Blockgröße, die für die Datenbank verwendet wird, variiert abhängig vom Tabellenbereich. Die meisten Tabellenbereiche verwenden 8-KB-Blöcke; einige verwenden jedoch 32-KB-Blöcke. |

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen   |
|---|---|---|
| <p>Planen Sie, mindestens vier Verzeichnisse, die auch als Speicherpfade bezeichnet werden, auf vier verschiedenen LUNs für die Datenbank zu erstellen?</p> <p>Erstellen Sie exakt ein Verzeichnis pro Array in dem Subsystem. Wenn weniger als drei Arrays vorhanden sind, erstellen Sie in jedem Array einen anderen LUN-Datenträger.</p> | <p>Für größere Arbeitslasten und bei Verwendung einiger Funktionen sind mehr Datenbankspeicherpfade als die Mindestvoraussetzungen erforderlich.</p> <p>Serveroperationen wie die Datenduplizierung verursachen eine hohe Anzahl Ein-/Ausgabeoperationen pro Sekunde (IOPS) für die Datenbank. Die Leistung derartiger Operationen ist besser, wenn die Datenbank über mehr Verzeichnisse verfügt.</p> <p>Verwenden Sie für Serverdatenbanken, die größer als 2 TB sind oder die wahrscheinlich auf diese Größe anwachsen, acht Verzeichnisse.</p> <p>Berücksichtigen Sie das geplante Wachstum des Systems bei der Bestimmung der Anzahl zu erstellender Speicherpfade. Die höhere Anzahl Speicherpfade wird vom Server effizienter genutzt, wenn die Speicherpfade bei der Ersterstellung des Servers bereits vorhanden sind.</p> <p>Verwenden Sie die Variable <i>DB2_PARALLEL_IO</i>, um die parallele E/A für Tabellenbereiche mit einem einzelnen Container zu erzwingen oder für Tabellenbereiche, die über Container auf mehr als einer physischen Platte verfügen. Wenn Sie die Variable <i>DB2_PARALLEL_IO</i> nicht definieren, entspricht die E/A-Parallelität der Anzahl Container, die von dem Tabellenbereich verwendet werden. Wenn ein Tabellenbereich beispielsweise vier Container umfasst, beträgt der verwendete Grad an E/A-Parallelität 4.</p> | <p>Weitere Informationen finden Sie in:</p> <ul style="list-style-type: none"> <li>• Prüfliste für Datenduplizierung</li> <li>• Prüfliste für Knotenreplikation</li> </ul> <p>Hilfreiche Informationen zur Vorhersage des Wachstums beim Duplizieren von Daten durch den Server finden Sie in Technote 1596944.</p> <p>Aktuelle Informationen zur Datenbankgröße, zur Datenbankreorganisation und zu Leistungsaspekten für IBM Spectrum Protect-Server finden Sie in Technote 1683633.</p> <p>Informationen zum Definieren der Variable <i>DB2_PARALLEL_IO</i> finden Sie in Empfohlene Einstellungen für IBM DB2-Registry-Variablen.</p> |
| <p>Haben alle Verzeichnisse für die Datenbank dieselbe Größe?</p>   | <p>Verzeichnisse, die alle dieselbe Größe haben, stellen einen konsistenten Grad an Parallelität für Datenbankoperationen sicher. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als andere sind, verringert sich dadurch das Potenzial für den optimierten parallelen Vorabesezugriff.</p> <p>Diese Richtlinie gilt auch, wenn Sie nach der Erstkonfiguration des Servers Speicherpfade hinzufügen müssen.</p>  |   |
| <p>Planen Sie, die Warteschlangenlänge der Datenbank-LUNs auf AIX-Systemen zu erhöhen?</p>  | <p>Die Standardwarteschlangenlänge ist häufig zu niedrig definiert.</p>   | <p>Siehe AIX-Systeme für die Plattenleistung konfigurieren.</p>   |

## Linux: Planung für Platten für das Serverwiederherstellungsprotokoll

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen  |
|---|---|--|
| Sind die aktive Protokolldatei und das Archivprotokoll auf anderen Platten oder LUNs gespeichert als die Datenbank und die Speicherpooldatenträger? | Stellen Sie sicher, dass die Platten, auf die die aktive Protokolldatei gestellt wird, auf dem Server oder System nicht für andere Zwecke verwendet werden. Stellen Sie die aktive Protokolldatei nicht auf Platten, die die Serverdatenbank, das Archivprotokoll oder Systemdateien, wie Seitenauslagerungsbereich oder Auslagerungsspeicher, enthalten.   | Das Trennen der Serverdatenbank von der aktiven Protokolldatei und dem Archivprotokoll trägt zur Reduktion von Konkurrenzsituationen für dieselben Ressourcen durch unterschiedliche Operationen, die gleichzeitig ausgeführt werden müssen, bei.  |
| Befinden sich die Protokolle auf Platten mit nicht flüchtigem Schreibcache?   | Nicht flüchtiger Schreibcache ermöglicht es, Daten so schnell wie möglich in die Protokolle zu schreiben. Schnellere Schreiboperationen für die Protokolle können die Leistung für Serveroperationen verbessern.  |  |
| Legen Sie für die Protokolle eine Größe fest, die der Arbeitslast entspricht?   | <p>Wenn Sie sich über die Arbeitslast im Unklaren sind, verwenden Sie die größtmögliche Größe.</p> <p><b>Aktive Protokolldatei</b><br/>Die maximale Größe beträgt 512 GB; sie wird über die Serveroption <code>ACTIVELOGSIZE</code> festgelegt.</p> <p>Stellen Sie sicher, dass mindestens 8 GB freier Speicherbereich im Dateisystem für aktive Protokolldateien verfügbar sind, nachdem die aktiven Protokolldateien mit fester Größe erstellt wurden.</p> <p><b>Archivprotokoll</b><br/>Die Größe des Archivprotokolls wird durch die Größe des Dateisystems begrenzt, in dem es sich befindet, und nicht durch eine Serveroption. Das Archivprotokoll muss mindestens so groß wie die aktive Protokolldatei sein.</p> | <ul style="list-style-type: none"> <li>• Ausführliche Informationen zur Festlegung der Protokollgröße enthalten die Informationen zum Wiederherstellungsprotokoll in Technote 1421060.</li> <li>• Informationen zur Festlegung der Größe bei Verwendung der Datendeduplizierung finden Sie in Prüfliste für Datendeduplizierung.</li> </ul>                                |
| Definieren Sie ein Archivübernahmeprotokoll? Stellen Sie dieses Protokoll auf eine andere Platte als das Archivprotokoll?                           | Das Archivübernahmeprotokoll dient der Verwendung durch den Server im Notfall, wenn das Archivprotokoll voll ist. Für das Archivübernahmeprotokoll können langsamere Platten verwendet werden.  | <p>Geben Sie die Position des Archivübernahmeprotokolls mithilfe der Serveroption <code>ARCHFAILOVERLOGDIRECTORY</code> an.</p> <p>Überwachen Sie die Belegung des Verzeichnisses für das Archivübernahmeprotokoll. Wenn das Archivübernahmeprotokoll vom Server verwendet werden muss, ist der Speicherplatz für das Archivprotokoll möglicherweise nicht groß genug.</p> |
| Verwenden Sie, wenn Sie die aktive Protokolldatei spiegeln, nur einen einzigen Typ von Spiegelung?  | <p>Sie können das Protokoll mithilfe einer der folgenden Methoden spiegeln. Verwenden Sie für das Protokoll nur einen einzigen Typ von Spiegelung.</p> <ul style="list-style-type: none"> <li>• Verwenden Sie die Option <code>MIRRORLOGDIRECTORY</code>, die für den IBM Spectrum Protect-Server verfügbar ist, um eine Position für die Spiegelung anzugeben.</li> <li>• Verwenden Sie die Softwarespiegelung, wie z. B. Logical Volume Manager (LVM) unter AIX.</li> <li>• Verwenden Sie die Spiegelung in der Hardware des Plattensystems.</li> </ul>   | <p>Stellen Sie, wenn Sie die aktive Protokolldatei spiegeln, sicher, dass die Platten für die aktive Protokolldatei und die Spiegelkopie dieselbe Geschwindigkeit und Zuverlässigkeit haben.</p> <p>Weitere Informationen finden Sie in Wiederherstellungsprotokoll konfigurieren und optimieren.</p>  |

## Linux: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools

Überprüfen Sie die Konfiguration Ihrer Verzeichniscontainer- und Cloud-Containerspeicherpools, um eine optimale Leistung zu gewährleisten.

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen   |
|--|--|---|
| <p>Verwenden Sie, gemessen in Anzahl Ein-/Ausgabeoperationen pro Sekunde (IOPS), schnellen Plattenspeicher für die IBM Spectrum Protect-Datenbank?</p> | <p>Verwenden Sie eine Hochleistungsplatte für die Datenbank. Verwenden Sie die Solid-State-Laufwerk-Technologie (SSD-Technologie) für die Datendeduplizierungsverarbeitung.</p> <p>Stellen Sie sicher, dass die Datenbank über eine Mindestkapazität von 3000 E/A-Operationen pro Sekunde (IOPS) verfügt. Addieren Sie zu diesem Mindestwert pro TB Daten, die täglich (vor der Datendeduplizierung) gesichert werden, 1000 E/A-Operationen pro Sekunde.</p> <p>Beispielsweise würde ein IBM Spectrum Protect-Server, der täglich 3 TB Daten aufnimmt, 6000 E/A-Operationen pro Sekunde (IOPS) für die Datenbankplatten benötigen:</p> $\text{mindestens } 3000 \text{ IOPS} + 3000 (3 \text{ TB} \times 1000 \text{ IOPS}) = 6000 \text{ IOPS}$   | <p>Empfehlungen zur Plattenauswahl finden Sie in "Planung für Platten für die Serverdatenbank".</p> <p>Weitere Informationen zu IOPS finden Sie in den IBM Spectrum Protect-Blueprints.</p> |
| <p>Ist genügend Speicherplatz für die Größe Ihrer Datenbank vorhanden?</p>   | <p>Verwenden Sie mindestens 40 GB Systemspeicher für IBM Spectrum Protect-Server, die Daten deduplizieren, mit einer Datenbankgröße von 100 GB. Wenn die Speicherkapazität für Sicherungsdaten wächst, ist unter Umständen ein höherer Speicherbedarf erforderlich.</p> <p>Überwachen Sie regelmäßig die Speicherbelegung, um festzustellen, ob mehr Speicherplatz erforderlich ist.</p> <p>Verwenden Sie weiteren Systemspeicher, um das Caching von Datenbankseiten zu verbessern. Die folgenden Richtlinien für die Speichergröße basieren auf dem Volumen an neuen Daten, das jeden Tag gesichert wird:</p> <ul style="list-style-type: none"> <li>• 128 GB Systemspeicher für tägliche Sicherungen von Daten, wobei die Datenbankgröße zwischen 1 und 2 TB liegt</li> <li>• 192 GB Systemspeicher für tägliche Sicherungen von Daten, wobei die Datenbankgröße zwischen 2 und 4 TB liegt</li> </ul> | <p>Speicherbedarf</p>   |

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen   |
|---|--|---|
| <p>Haben Sie die Speicherkapazität für die die aktive Protokolldatei und das Archivprotokoll der Datenbank korrekt festgelegt?</p>  | <p>Geben Sie in der Konfiguration des Servers eine minimale Größe von 128 GB für die aktive Protokolldatei an, indem Sie die Serveroption ACTIVELOGSIZE auf den Wert 131072 setzen.</p> <p>Als Anfangsgröße für das Archivprotokoll wird eine Größe von 1 TB vorgeschlagen. Die Größe des Archivprotokolls wird durch die Größe des Dateisystems begrenzt, in dem es sich befindet, und nicht durch eine Serveroption. Stellen Sie sicher, dass im Vergleich zur Größe des Archivprotokolls mindestens 10 % zusätzlicher Plattenspeicher für das Dateisystem vorhanden sind.</p> <p>Verwenden Sie für die Datenbankarchivprotokolle ein Verzeichnis mit einer anfänglichen freien Kapazität von mindestens 1 TB. Geben Sie das Verzeichnis mithilfe der Serveroption ARCHLOGDIRECTORY an.</p> <p>Definieren Sie Speicherbereich für das Archivübernahmeprotokoll mithilfe der Serveroption ARCHFAILOVERLOGDIRECTORY.</p> | <p>Weitere Informationen zur Kapazitätsermittlung für Ihr System finden Sie in den IBM Spectrum Protect-Blueprints.</p>   |
| <p>Ist die Komprimierung für die Archivprotokoll- und Datenbanksicherungen aktiviert?</p>   | <p>Aktivieren Sie die Serveroption ARCHLOGCOMPRESS, um Speicherbereich einzusparen.</p> <p>Diese Komprimierungsoption unterscheidet sich von der Inline-Komprimierung. Die Inline-Komprimierung ist ab IBM Spectrum Protect Version 7.1.5 und höher standardmäßig aktiviert.</p> <p>Einschränkung: Sie dürfen diese Option nicht verwenden, wenn das Volumen der pro Tag gesicherten Daten 6 TB überschreitet.</p>   | <p>Weitere Informationen zur Komprimierung für Ihr System finden Sie in den IBM Spectrum Protect-Blueprints.</p>  |
| <p>Befinden sich die Datenbank und Protokolle von IBM Spectrum Protect auf separaten Plattendatenträgern (LUNs)?</p> <p>Ist der Datenträger, der für die Datenbank verwendet wird, gemäß den bewährten Verfahren für eine transaktionsorientierte Datenbank konfiguriert?</p> | <p>Die Datenbank darf keine Plattendatenträger mit IBM Spectrum Protect-Datenbankprotokollen oder -Speicherpools oder mit einer anderen Anwendung oder einem anderen Dateisystem gemeinsam nutzen.</p>   | <p>Weitere Informationen zur Konfiguration der Serverdatenbank und des Wiederherstellungsprotokolls finden Sie in Konfiguration und Optimierung der Serverdatenbank und des Wiederherstellungsprotokolls.</p> |
| <p>Verwenden Sie mindestens acht Prozessorkerne (2,2-GHz-Prozessorkerne oder entsprechende Prozessorkerne) für jeden IBM Spectrum Protect-Server, der mit Datendeduplizierung verwendet werden soll?</p>  | <p>Wenn die clientseitige Datendeduplizierung verwendet werden soll, müssen Sie sicherstellen, dass für Clientsysteme während einer Sicherungsoperation genügend Ressourcen zur Ausführung der Datendeduplizierungsverarbeitung verfügbar sind. Verwenden Sie pro Sicherungsprozess mit clientseitiger Datendeduplizierung einen Prozessor, der mindestens einem 2,2-GHz-Prozessorkern entspricht.</p>   | <ul style="list-style-type: none"> <li>• Effektive Planung und Verwendung der Deduplizierung</li> <li>• IBM Spectrum Protect Blueprints</li> </ul>  |



| Frage   | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen  |
|---|---|--|
| Haben Sie genügend Speicherplatz für die Datenbank zugeordnet?  | <p>Als grobe Schätzung sollten Sie 100 GB Datenbankspeicher für jeweils 50 TB Daten einplanen, die in deduplizierten Speicherpools geschützt werden sollen. <i>Geschützte Daten</i> ist das Datenvolumen vor der Dateneduplizierung, einschließlich aller Versionen gespeicherter Objekte.</p> <p>Als bewährtes Verfahren sollten Sie einen neuen Containerspeicherpool ausschließlich für die Dateneduplizierung definieren. Die Dateneduplizierung erfolgt auf der Speicherpoolebene; mit Ausnahme von verschlüsselten Daten werden alle Daten in einem Speicherpool dedupliziert.</p>  |  |
| Haben Sie die Speicherpoolkapazität geschätzt, um genügend Speicherplatz für die Größe Ihrer Umgebung zu konfigurieren? | <p>Sie können den Kapazitätsbedarf für einen deduplizierten Speicherpool wie folgt schätzen:</p> <ol style="list-style-type: none"> <li>1. Schätzen Sie die Basisgröße der Quelldaten.</li> <li>2. Schätzen Sie die Größe der täglichen Sicherung anhand einer geschätzten Änderungs- und Wachstumsrate.</li> <li>3. Bestimmen Sie die Anforderungen in Bezug auf die Aufbewahrungsdauer.</li> <li>4. Schätzen Sie das Gesamtvolumen an Quelldaten unter Berücksichtigung der Basisgröße, der Größe der täglichen Sicherung und der Anforderungen in Bezug auf die Aufbewahrungsdauer.</li> <li>5. Wenden Sie den Faktor für das Deduplizierungsverhältnis an.</li> <li>6. Wenden Sie den Faktor für das Komprimierungsverhältnis an.</li> <li>7. Runden Sie die Schätzung auf, um die Nutzung transienter Speicherpools zu berücksichtigen.</li> </ol> | Ein Beispiel zur Verwendung dieses Verfahrens finden Sie in Effektive Planung und Verwendung der Deduplizierung. |

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen  |
|---|---|--|
| Haben Sie die Platten-E/A auf viele Platteneinheiten und Controller verteilt?   | <p>Verwenden Sie Arrays, die aus so vielen Platten wie möglich bestehen; dies wird auch als "Wide-Striping" bezeichnet. Stellen Sie sicher, dass Sie exakt ein Datenbankverzeichnis pro Array in dem Subsystem verwenden.</p> <p>Definieren Sie die Registry-Variablen <i>DB2_PARALLEL_IO</i>, um die parallele E/A für jeden verwendeten Tabellenbereich zu aktivieren, wenn sich die Container in dem Tabellenbereich über mehrere physische Platten erstrecken.</p> <p>Wenn E/A-Bandbreite verfügbar ist und die Dateien groß sind (beispielsweise 1 MB), kann der Prozess zur Suche nach Duplikaten die Ressourcen eines gesamten Prozessors in Anspruch nehmen. Wenn Dateien kleiner sind, können andere Engpässe auftreten.</p> <p>Geben Sie acht oder mehr Dateisysteme für die Einheitenklasse des deduplizierten Speicherpools an, damit die Ein-/Ausgabe auf so viele LUNs und physische Einheiten wie möglich verteilt wird.</p> | <p>Richtlinien zur Konfiguration von Speicherpools finden Sie in "Planung für Speicherpools auf DISK- oder FILE-Einheiten".</p> <p>Informationen zum Definieren der Variable <i>DB2_PARALLEL_IO</i> finden Sie in Empfohlene Einstellungen für IBM DB2-Registry-Variablen.</p> |
| Haben Sie tägliche Operationen auf der Basis Ihrer Sicherungsstrategie geplant? | <p>Die Operationsfolge sieht gemäß den bewährten Verfahren wie folgt aus:</p> <ol style="list-style-type: none"> <li>1. Clientsicherung</li> <li>2. Speicherpoolschutz</li> <li>3. Knotenreplikation</li> <li>4. Datenbanksicherung</li> <li>5. Bestandsverfall</li> </ol>  | <ul style="list-style-type: none"> <li>• Dateneduplizierungs- und Knotenreplikationsprozesse planen</li> <li>• Tägliche Operation für Verzeichniscontainerspeicherpools</li> </ul>   |
| Ist genügend Speicher zur Verwaltung der DB2-Sperrenliste vorhanden?            | <p>Wenn Sie Daten deduplizieren, die große Dateien oder gleichzeitig eine große Anzahl Dateien umfassen, kann der Prozess zur Speicherknappheit führen. Wenn der Sperrenlistenspeicher nicht ausreichend ist, können Sicherheitsfehler, Datenverwaltungsprozessfehler oder Serverausfälle auftreten.</p> <p>Bei Dateigrößen über 500 GB, die durch die Dateneduplizierung verarbeitet werden, ist es sehr wahrscheinlich, dass der Speicherplatz knapp wird. Wenn jedoch viele Sicherungsoperationen die clientseitige Dateneduplizierung verwenden, kann dieses Problem auch bei Dateien mit geringerer Größe auftreten.</p>   | <p>Informationen zur Optimierung des DB2-Parameters LOCKLIST finden Sie in Serverseitige Dateneduplizierung optimieren.</p>  |

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen  |
|--|---|--|
| Ist genügend Bandbreite verfügbar, um Daten auf einen IBM Spectrum Protect-Server zu übertragen?       | <p>Um Daten auf einen IBM Spectrum Protect-Server zu übertragen, verwenden Sie die clientseitige oder serverseitige Datendeduplizierung und die Komprimierung, um die erforderliche Bandbreite zu verringern.</p> <p>Verwenden Sie einen Server der Version 7.1.5 oder höher, um die Inline-Komprimierung verwenden zu können, und einen Client der Version 7.1.6 oder höher, um die erweiterte Komprimierungsverarbeitung zu aktivieren.</p>   | Weitere Informationen finden Sie in der Beschreibung der Clientoption <code>enablededup</code> . |
| Haben Sie festgelegt, wie viele Speicherpoolverzeichnisse jedem Speicherpool zugeordnet werden sollen? | <p>Ordnen Sie Verzeichnisse einem Speicherpool mithilfe des Befehls <code>DEFINE STGPOOLDIRECTORY</code> zu.</p> <p>Erstellen Sie mehrere Speicherpoolverzeichnisse und stellen Sie sicher, dass jedes Verzeichnis auf einem anderen Plattendatenträger (LUN) gesichert wird.</p>   |  |
| Haben Sie genügend Plattenspeicherplatz in dem Cloud-Containerspeicherpool zugeordnet?                 | <p>Um Sicherheitsfehler zu verhindern, stellen Sie sicher, dass das lokale Verzeichnis über genügend Speicherplatz verfügt. Verwenden Sie die folgende Liste als Leitfaden für optimalen Plattenspeicherplatz:</p> <ul style="list-style-type: none"> <li>• Berechnen Sie für SAS-Platten (SAS = Serial-Attached SCSI) und rotierende Platten das Volumen neuer Daten, das nach der täglichen Datenreduktion (Komprimierung und Datendeduplizierung) erwartet wird. Ordnen Sie bis zu 100 Prozent dieses Volumens (in Terabyte) für den Plattenspeicherplatz zu.</li> <li>• Stellen Sie 3 TB für flash-basierte Speichersysteme mit schnellen Netzverbindungen zu leistungsfähigen On-Premises-Cloudsystemen bereit.</li> <li>• Stellen Sie 5 TB für Systeme mit Solid-State-Laufwerk (SSD) mit schnellen Netzverbindungen zu leistungsfähigen Cloudsystemen bereit.</li> </ul> |  |

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen |
|---|---|-----------------------|
| <p>Haben Sie den geeigneten Typ des lokalen Speichers ausgewählt?</p> | <p>Stellen Sie sicher, dass Datenübertragungen aus dem lokalen Speicher in die Cloud beendet werden, bevor der nächste Sicherungszyklus beginnt.</p> <p>Tipp: Daten werden kurz nach dem Versetzen in die Cloud aus dem lokalen Speicher entfernt.</p> <p>Verwenden Sie die folgenden Richtlinien:</p> <ul style="list-style-type: none"> <li>• Verwenden Sie Flash- oder SSD-Speicher für große Systeme, die über leistungsfähige Cloudsysteme verfügen. Stellen Sie sicher, dass Sie über eine dedizierte 10-GB-WAN-Verbindung mit einer Hochgeschwindigkeitsverbindung zum Objektspeicher verfügen. Verwenden Sie beispielsweise Flash- oder SSD-Speicher, wenn Sie über eine dedizierte 10-GB-WAN-Verbindung sowie eine Hochgeschwindigkeitsverbindung zu einem IBM® Cloud Object Storage-Speicherort oder zu einem Amazon S3-Datencenter (Amazon S3 = Amazon Simple Storage Service) verfügen.</li> <li>• Verwenden Sie SAS-Platten mit 15000 U/min mit größerer Kapazität für die folgenden Szenarios: <ul style="list-style-type: none"> <li>◦ Systeme mittlerer Größe</li> <li>◦ Langsamere Cloudverbindungen, z. B. 1 GB</li> <li>◦ Bei Verwendung von IBM Cloud Object Storage als Service-Provider in mehreren Regionen</li> </ul> </li> <li>• Berechnen Sie für SAS-Platten oder rotierende Platten das Volumen neuer Daten, das nach der täglichen Datenreduktion (Komprimierung und Datendeduplizierung) erwartet wird. Ordnen Sie bis zu 100 Prozent dieses Volumens (in Terabyte) für den Plattenspeicherplatz zu.</li> </ul> |                       |

## Linux: Planung für Speicherpools auf DISK- oder FILE-Einheiten

Überprüfen Sie mithilfe der Prüfliste, wie Ihre Plattenspeicherpools konfiguriert sind. Diese Prüfliste umfasst Tipps für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden.

| Frage | Tasks, Merkmale, Optionen oder Einstellungen | Weitere Informationen |
|-------|--|-----------------------|
|-------|--|-----------------------|

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen  |
|---|--|--|
| <p>Können die Speicherpool-LUNs Durchsatzraten von 256 KB für sequenzielle Lese- und Schreibvorgänge aufrechterhalten, um die Arbeitslast innerhalb der Zeitvorgaben adäquat handhaben zu können?</p> | <p>Bei der Planung für Spitzenbelastungen müssen Sie alle Daten berücksichtigen, die der Server gleichzeitig aus Plattenspeicherpools lesen oder in Plattenspeicherpools schreiben soll. Berücksichtigen Sie beispielsweise den Spitzenwert für den Datenfluss bei Clientsicherungsoperationen und Serverdatenversetzungsoperationen, wie z. B. Umlagerung, die gleichzeitig ausgeführt werden.</p> <p>Der IBM Spectrum Protect-Server verwendet beim Lesen aus Speicherpools und Schreiben in Speicherpools in erster Linie 256-KB-Blöcke.</p> <p>Wenn das Plattensystem über die entsprechende Funktionalität verfügt, konfigurieren Sie das Plattensystem für die optimale Leistung mit sequenziellen Lese-/Schreiboperationen statt mit wahlfreien Lese-/Schreiboperationen.</p> | <p>Weitere Informationen finden Sie in Basisleistung von Plattensystemen analysieren.</p>  |
| <p>Ist die Platte für die Verwendung von Lese- und Schreibcache konfiguriert?</p>   | <p>Verwenden Sie mehr Cache, um eine bessere Leistung zu erzielen.</p>   |  |
| <p>Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, eine geeignete Größe für die Speicherpooldatenträger festgelegt?</p>  | <p>Lesen Sie die Informationen in Optimale Anzahl und Größe von Datenträgern für Speicherpools, die Platten verwenden. Wenn Sie nicht über die nötigen Informationen zum Schätzen der Größe für Datenträger mit der Einheitenklasse FILE verfügen, beginnen Sie mit einer Datenträgergröße von 50 GB.</p>  | <p>In der Regel treten häufiger Probleme auf, wenn die Datenträger zu klein sind. Wenn Datenträger größer als erforderlich sind, treten nur selten Probleme auf. Wenn Sie die zu verwendende Datenträgergröße festlegen, sollten Sie als Vorsichtsmaßnahme eine größere Größe als erforderlich wählen.</p> |
| <p>Verwenden Sie für Speicherpools, die die Einheitenklasse FILE verwenden, vorab zugeordnete Datenträger?</p>  | <p>Arbeitsdatenträger können eine Dateifragmentierung zur Folge haben.</p> <p>Um sicherzustellen, dass für einen Speicherpool immer genügend Datenträger verfügbar sind, setzen Sie den Parameter MAXSCRATCH auf einen Wert größer als null.</p>   | <p>Ordnen Sie mithilfe des Befehls DEFINE VOLUME Datenträger in dem Speicherpool vorab zu.</p> <p>Verwenden Sie den Serverbefehl DEFINE STGPOOL oder UPDATE STGPOOL, um den Parameter MAXSCRATCH zu definieren.</p>  |
| <p>Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, die maximale Anzahl Clientsitzungen mit der Anzahl definierter Datenträger verglichen?</p>                                    | <p>Es müssen immer genügend verwendbare Datenträger in den Speicherpools vorhanden sein, um die erwartete maximale Anzahl gleichzeitig ausgeführter Clientsitzungen handhaben zu können. Bei den Datenträgern kann es sich um Arbeitsdatenträger, leere Datenträger oder teilweise gefüllte Datenträger handeln.</p>   | <p>Bei Speicherpools, die die Einheitenklasse FILE verwenden, kann jeweils nur eine einzige Sitzung oder ein einziger Prozess auf einen Datenträger schreiben.</p>   |

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen  |
|--|---|--|
| Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, den Parameter MOUNTLIMIT für die Einheitenklasse auf einen Wert gesetzt, der für die Anzahl Datenträger, die parallel angehängt werden könnten, ausreichend hoch ist? | <p>Für Speicherpools, die die Datendeduplizierung verwenden, liegt der Wert für den Parameter MOUNTLIMIT in der Regel zwischen 500 und 1000. Setzen Sie den Wert für MOUNTLIMIT auf die maximale Anzahl Mountpunkte, die für alle aktiven Sitzungen erforderlich sind. Berücksichtigen Sie Parameter, die sich auf die maximale Anzahl erforderlicher Mountpunkte auswirken:</p> <ul style="list-style-type: none"> <li>Die Serveroption MAXSESSIONS, die die maximal zulässige Anzahl gleichzeitig ablaufender IBM Spectrum Protect-Sitzungen angibt</li> <li>Der Parameter MAXNUMMP, der die maximale Anzahl Mountpunkte definiert, die jeder Clientknoten verwenden kann</li> </ul> <p>Wenn beispielsweise die maximalen Anzahl Sicherungssitzungen für Clientknoten normalerweise 100 ist und für jeden der Knoten MAXNUMMP=2 definiert ist, multiplizieren Sie 100 Knoten mit 2 Mountpunkten für jeden Knoten, um den Wert 200 für den Parameter MOUNTLIMIT zu erhalten.</p> | Verwenden Sie den Serverbefehl REGISTER NODE oder UPDATE NODE, um den Parameter MAXNUMMP für Clientknoten zu definieren.   |
| Haben Sie für Speicherpools, die die Einheitenklasse DISK verwenden, festgelegt, wie viele Speicherpooldatenträger in jedes Dateisystem gestellt werden sollen?  | <p>Die Konfiguration des Speichers für einen Speicherpool, der eine Einheitenklasse DISK verwendet, ist davon abhängig, ob Sie RAID für das Plattensystem verwenden.</p> <p>Wenn Sie RAID nicht verwenden, konfigurieren Sie ein einziges Dateisystem pro physischer Platte und definieren Sie exakt einen Speicherpooldatenträger für jedes Dateisystem.</p> <p>Wenn Sie RAID 5 mit <math>n + 1</math> Datenträgern verwenden, konfigurieren Sie den Speicher auf eine der folgenden Arten:</p> <ul style="list-style-type: none"> <li>Konfigurieren Sie <math>n</math> Dateisysteme auf der LUN und definieren Sie exakt einen Speicherpooldatenträger pro Dateisystem.</li> <li>Konfigurieren Sie ein einziges Dateisystem und <math>n</math> Speicherpooldatenträger für die LUN.</li> </ul>  | Ein Beispiellayout, bei dem diese Richtlinie eingehalten wird, zeigt Beispiellayout für Serverspeicherpools.   |
| Haben Sie Ihre Speicherpools für die Verteilung der Ein-/Ausgabe auf mehrere Dateisysteme erstellt?  | <p>Stellen Sie sicher, dass sich jedes Dateisystem auf einer anderen LUN auf dem Plattensystem befindet.</p> <p>Normalerweise sind 10-30 Dateisysteme ein geeigneter Wert, Sie müssen jedoch sicherstellen, dass die Dateisysteme nicht kleiner als etwa 250 GB sind.</p>   | <p>Ausführliche Informationen finden Sie in:</p> <ul style="list-style-type: none"> <li>Plattenspeicher für den Server optimieren</li> <li>Speicherpools und Datenträger optimieren und konfigurieren</li> </ul> |

## Linux: Planung für die Auswahl des korrekten Speichertechnologietyps

Speichereinheiten haben eine unterschiedliche Kapazität und unterschiedliche Leistungsmerkmale. Diese Merkmale wirken sich darauf aus, welche Einheiten besser für die Verwendung mit IBM Spectrum Protect geeignet sind.

### Vorgehensweise

Die folgende Tabelle unterstützt Sie bei der Auswahl des korrekten Speichertechnologietyps für die Speicherressourcen, die der Server erfordert.

Tabelle 1. Speichertechnologietypen für IBM Spectrum Protect-Speicherbedarf

| <b>Speichertechnologietyp</b>   | <b>Datenbank</b>   | <b>Aktive Protokolldatei</b>  | <b>Archivprotokoll und Archivübernahmeprotokoll</b>  | <b>Speicherpools</b>   |
|---|--|---|--|--|
| <b>Solid-State-Laufwerk (SSD)</b>   | <p>Stellen Sie die Datenbank auf ein Solid-State-Laufwerk, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Sie verwenden die IBM Spectrum Protect-Dateneduplizierung.</li> <li>• Sie sichern täglich mehr als 8 TB neuer Daten.</li> </ul>   | <p>Wenn Sie die IBM Spectrum Protect-Datenbank auf ein Solid-State-Laufwerk stellen (dies ist das bewährte Verfahren), stellen Sie auch die aktive Protokolldatei auf ein Solid-State-Laufwerk. Wenn kein Speicherplatz verfügbar ist, verwenden Sie stattdessen eine Hochleistungsplatte.</p>  | <p>Reservieren Sie die Solid-State-Laufwerke für die Verwendung mit der Datenbank und der aktiven Protokolldatei. Das Archivprotokoll und die Archivübernahmeprotokolle können auf langsamere Speichertechnologietypen gestellt werden.</p>                          | <p>Reservieren Sie die Solid-State-Laufwerke für die Verwendung mit der Datenbank und der aktiven Protokolldatei. Speicherpools können auf langsamere Speichertechnologietypen gestellt werden.</p>  |
| <p><b>Hochleistungsplatte mit den folgenden Kenndaten:</b></p> <ul style="list-style-type: none"> <li>• <b>Platte mit 15.000 U/min</b></li> <li>• <b>Fibre Channel - oder Serial-attach und SCSI-Schnittstelle (SAS-Schnittstelle)</b></li> </ul> | <p>Verwenden Sie Hochleistungsplatten, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Der Server führt keine Dateneduplizierung aus.</li> <li>• Der Server führt keine Knotenreplikation aus.</li> </ul> <p>Trennen Sie die Serverdatenbank von den zugehörigen Protokollen und Speicherpools sowie von Daten für andere Anwendungen.</p> | <p>Verwenden Sie Hochleistungsplatten, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Der Server führt keine Dateneduplizierung aus.</li> <li>• Der Server führt keine Knotenreplikation aus.</li> </ul> <p>Trennen Sie aus Gründen der Leistung und Verfügbarkeit die aktive Protokolldatei von der Serverdatenbank, den Archivprotokollen und den Speicherpools.</p> | <p>Sie können Hochleistungsplatten für das Archivprotokoll und die Archivübernahmeprotokolle verwenden. Trennen Sie aus Gründen der Verfügbarkeit diese Protokolle von der Datenbank und der aktiven Protokolldatei.</p>   | <p>Verwenden Sie Hochleistungsplatten für Speicherpools, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Daten werden häufig gelesen.</li> <li>• Daten werden häufig geschrieben.</li> </ul> <p>Trennen Sie aus Gründen der Leistung und Verfügbarkeit die Speicherpooldaten von der Serverdatenbank und den Protokollen sowie von Daten für andere Anwendungen.</p>   |
| <p><b>Platte mit mittlerer Leistung oder Hochleistungsplatte mit den folgenden Kenndaten:</b></p> <ul style="list-style-type: none"> <li>• <b>Platte mit 10.000 U/min</b></li> <li>• <b>Fibre Channel - oder SAS-Schnittstelle</b></li> </ul>     | <p>Wenn das Plattensystem eine Kombination verschiedener Plattentechnologien verwendet, verwenden Sie die schnelleren Platten für die Datenbank und die aktive Protokolldatei. Trennen Sie die Serverdatenbank von den zugehörigen Protokollen und Speicherpools sowie von Daten für andere Anwendungen.</p>   | <p>Wenn das Plattensystem eine Kombination verschiedener Plattentechnologien verwendet, verwenden Sie die schnelleren Platten für die Datenbank und die aktive Protokolldatei. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die aktive Protokolldatei von der Serverdatenbank, den Archivprotokollen und den Speicherpools.</p>   | <p>Sie können eine Platte mit mittlerer Leistung oder eine Hochleistungsplatte für das Archivprotokoll und die Archivübernahmeprotokolle verwenden. Trennen Sie aus Gründen der Verfügbarkeit diese Protokolle von der Datenbank und der aktiven Protokolldatei.</p> | <p>Verwenden Sie eine Platte mit mittlerer Leistung oder eine Hochleistungsplatte für Speicherpools, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Daten werden häufig gelesen.</li> <li>• Daten werden häufig geschrieben.</li> </ul> <p>Trennen Sie aus Gründen der Leistung und Verfügbarkeit die Speicherpooldaten von der Serverdatenbank und den Protokollen sowie von Daten für andere Anwendungen.</p> |

| Speichertechnologietyp                      | Datenbank   | Aktive Protokolldatei  | Archivprotokoll und Archivübernahmeprotokoll  | Speicherpools  |
|---|---|--|---|--|
| <b>SATA, Network-attached Storage (NAS)</b> | Verwenden Sie diesen Speicher nicht für die Datenbank. Stellen Sie die Datenbank nicht auf XIV-Speichersysteme. | Verwenden Sie diesen Speicher nicht für die aktive Protokolldatei. | Die Verwendung dieser langsameren Speichertechnologie ist akzeptabel, da diese Protokolle einmal geschrieben und nur selten gelesen werden. | Verwenden Sie diese langsamere Speichertechnologie, wenn die folgenden Bedingungen erfüllt sind: <ul style="list-style-type: none"> <li>• Daten werden selten geschrieben, beispielsweise einmal.</li> <li>• Daten werden selten gelesen.</li> </ul> |
| <b>Bänder und virtuelle Bänder</b>          |   |  |   | Verwenden Sie diese Speichermedien für die langfristige Aufbewahrung oder wenn Daten nur selten verwendet werden.  |

## Linux: Bewährte Verfahren bei der Serverinstallation anwenden

Normalerweise hat die Konfiguration und Auswahl der Hardware die deutlichsten Auswirkungen auf die Leistung einer IBM Spectrum Protect-Lösung. Weitere Faktoren, die sich auf die Leistung auswirken, sind die Auswahl und Konfiguration des Betriebssystems sowie die Konfiguration von IBM Spectrum Protect.

### Vorgehensweise

- Nachfolgend sind die wichtigsten bewährten Verfahren für die Erzielung der optimalen Leistung und die Vermeidung von Problemen aufgeführt.
- Bestimmen Sie anhand der Tabelle die bewährten Verfahren, die für Ihre Umgebung gelten.

| Bewährtes Verfahren  | Weitere Informationen  |
|--|--|
| Verwenden Sie schnelle Platten für die Serverdatenbank. Enterprise-Solid-State-Laufwerke mit Fibre Channel- oder SAS-Schnittstellen bieten die beste Leistung. | Verwenden Sie schnelle Platten mit kurzer Latenzzeit für die Datenbank. Die Verwendung von Solid-State-Laufwerken ist von entscheidender Bedeutung, wenn Sie die Datenduplizierung und Knotenreplikation verwenden. Vermeiden Sie die Verwendung von SATA-Laufwerken (SATA = Serial Advanced Technology Attachment) und PATA-Laufwerken (PATA = Parallel Advanced Technology Attachment). Ausführliche Informationen und weitere Tipps finden Sie in: <ul style="list-style-type: none"> <li>◦ "Planung für Platten für die Serverdatenbank"</li> <li>◦ "Planung für die Auswahl des korrekten Speichertechnologietyps"</li> </ul> |
| Stellen Sie sicher, dass das Serversystem über genügend Speicher verfügt.  | Überprüfen Sie die Betriebssystemvoraussetzungen in Technote 1243309. Höhere Arbeitslasten erfordern mehr als die Mindestvoraussetzungen. Erweiterte Funktionen wie beispielsweise Datenduplizierung und Knotenreplikation können mehr Speicher als den Mindestspeicher erfordern, der im Dokument mit den Systemvoraussetzungen angegeben ist. <p>Wenn Sie die Ausführung mehrerer Instanzen planen, ist für jede Instanz der für einen einzelnen Server aufgelistete Speicher erforderlich. Multiplizieren Sie den für einen einzelnen Server erforderlichen Speicher mit der Anzahl der für das System geplanten Instanzen.</p> |



| Bewährtes Verfahren   | Weitere Informationen  |
|---|--|
| Trennen Sie die Serverdatenbank, die aktive Protokolldatei, das Archivprotokoll und die Plattenspeicherpools voneinander.   | <p>Stellen Sie alle IBM Spectrum Protect-Speicherressourcen auf unterschiedliche Platten. Trennen Sie Speicherpoolplatten von den Platten für die Serverdatenbank und die Protokolle.</p> <p>Speicherpooloperationen können Datenbankoperationen beeinträchtigen, wenn sich die Speicherpools und die Datenbank auf denselben Platten befinden. Im Idealfall werden auch die Serverdatenbank und die Protokolle voneinander getrennt.</p> <p>Ausführliche Informationen und weitere Tipps finden Sie in:</p> <ul style="list-style-type: none"> <li>o "Planung für Platten für die Serverdatenbank"</li> <li>o "Planung für Platten für das Serverwiederherstellungsprotokoll"</li> <li>o "Planung für Speicherpools auf DISK- oder FILE-Einheiten"</li> </ul> |
| Verwenden Sie mindestens vier Verzeichnisse für die Serverdatenbank. Verwenden Sie für größere Server oder Server, die erweiterte Funktionen verwenden, acht Verzeichnisse.   | <p>Stellen Sie jedes Verzeichnis auf eine LUN, die von anderen LUNs und von anderen Anwendungen getrennt ist.</p> <p>Ein Server wird als großer Server betrachtet, wenn seine Datenbank größer als 2 TB ist oder wahrscheinlich diese Größe erreichen wird. Verwenden Sie für derartige Server acht Verzeichnisse.</p> <p>Siehe "Planung für Platten für die Serverdatenbank".</p>   |
| Wenn Sie die Datendeduplizierung und/oder die Knotenreplikation verwenden, beachten Sie die Richtlinien für die Datenbankkonfiguration und andere Elemente.   | <p>Konfigurieren Sie den Server gemäß den Richtlinien, da die Datenbank in Bezug darauf, wie gut die Ausführung des Servers bei Verwendung dieser Funktionen ist, extrem wichtig ist. Ausführliche Informationen und weitere Tipps finden Sie in:</p> <ul style="list-style-type: none"> <li>o Prüfliste für Datendeduplizierung</li> <li>o Prüfliste für Knotenreplikation</li> </ul>   |
| Beachten Sie bei Speicherpools, die Einheitenklassen des Typs FILE verwenden, die Richtlinien für die Größe von Speicherpooldatenträgern. In der Regel sind Datenträger mit einer Größe von 50 GB am besten geeignet. | <p>Lesen Sie die Informationen in Optimale Anzahl und Größe von Datenträgern für Speicherpools, die Platten verwenden zur Bestimmung der Datenträgergröße.</p> <p>Konfigurieren Sie Speicherpools und Dateisysteme auf der Basis der Anforderungen in Bezug auf den Durchsatz und nicht nur auf der Basis der Kapazitätsanforderungen.</p> <p>Trennen Sie die Speichereinheiten, die von IBM Spectrum Protect verwendet werden, von anderen Anwendungen mit hoher Ein-/Ausgabe und stellen Sie sicher, dass der Durchsatz für diesen Speicher ausreichend ist.</p> <p>Weitere Informationen finden Sie in Prüfliste für Speicherpools auf FILE- oder DISK-Einheiten.</p>   |
| Planen Sie IBM Spectrum Protect-Clientoperationen und -Serververwaltungsaktivitäten, um eine Überschneidung von Operationen zu verhindern oder auf ein Mindestmaß zu reduzieren.                                      | <p>Weitere ausführliche Informationen liefern die folgenden Themen:</p> <ul style="list-style-type: none"> <li>o Zeitplan für tägliche Operationen optimieren</li> <li>o Prüfliste für Serverkonfiguration</li> </ul>  |
| Überwachen Sie Operationen kontinuierlich.  | <p>Die Überwachung ermöglicht es Ihnen, Probleme frühzeitig erkennen und Ursachen leichter ermitteln zu können. Bewahren Sie Aufzeichnungen von Überwachungsberichten bis zu einem Jahr lang auf, um Trends schneller erkennen und Wachstum besser planen zu können. Siehe Umgebung im Hinblick auf die Leistung überwachen und verwalten.</p>   |




## Linux: Systemmindestvoraussetzungen für Linux-Systeme

Für die Installation des IBM Spectrum Protect-Servers auf einem Linux-System wird ein Minimum an Hardware und Software benötigt. Hierzu gehören eine Übertragungsmethode und der aktuelle Einheitsreiber.

Die folgenden Tabellen enthalten die Mindesthardware- und -softwarevoraussetzungen für die Installation eines IBM Spectrum Protect-Servers. Verwenden Sie diese Voraussetzungen als Ausgangspunkt für Systeme ohne Datendeduplizierung. Die optimale IBM Spectrum Protect-Umgebung ist mit Datendeduplizierung mithilfe der IBM Spectrum Protect Blueprints konfiguriert. Die neuesten Informationen zu den Systemvoraussetzungen finden Sie unter Technote 1243309.

Das IBM Spectrum Protect-Einheitentreiberpaket enthält keinen Einheitentreiber für dieses Betriebssystem, weil ein generischer SCSI-Einheitentreiber verwendet wird. Konfigurieren Sie den Einheitentreiber, bevor der IBM Spectrum Protect-Server für Bandeinheiten verwendet wird. Das IBM Spectrum Protect-Treiberpaket enthält Treibertools und ACSLS-Dämonen. IBM®-Treiberpakete finden Sie auf der Fix Central-Website.

Informationen zu Voraussetzungen, unterstützten Einheiten, Clientinstallationspaketen und Fixes sind im IBM Support Portal for IBM Spectrum Protect verfügbar. Rufen Sie nach der Installation von IBM Spectrum Protect und vor der individuellen Anpassung die Website auf, laden Sie alle anwendbaren Fixes herunter und wenden Sie diese Fixes an.

-  Linux-BetriebssystemeLinux: Servermindestvoraussetzungen für Linux x86\_64  
Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux x86\_64-Betriebssystem installieren.
-  Linux-BetriebssystemeLinux: Servermindestvoraussetzungen für Linux on System z  
Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux on System z-Betriebssystem installieren.
-  Linux-BetriebssystemeLinux: Servermindestvoraussetzungen für Linux on Power Systems (Little Endian)  
Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux on Power Systems-Betriebssystem (Little Endian) installieren.

## Linux: Servermindestvoraussetzungen für Linux x86\_64

---

Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux x86\_64-Betriebssystem installieren.

### Hardwarevoraussetzungen

---

In Tabelle 1 sind die Hardwaremindestvoraussetzungen für den Server beschrieben. Wenn der Server die Mindestvoraussetzungen nicht erfüllt, schlägt die Installation fehl. Weitere Informationen zur Planung des Plattenspeicherplatzes finden Sie in Linux: Kapazitätsplanung.

Tabelle 1. Hardwarevoraussetzungen

| Hardwaretyp | Hardwarevoraussetzungen                |
|-------------|--|
| Server      | Ein AMD64- oder Intel EMT-64-Prozessor |

| Hardwaretyp     | Hardwarevoraussetzungen  |
|-----------------|--|
| Plattenspeicher | <p>Folgende Mindestwerte für den Plattenspeicher:</p> <ul style="list-style-type: none"> <li>• 5 GB für das Installationsverzeichnis</li> <li>• 512 MB für das Verzeichnis /var</li> <li>• 2 GB für das Verzeichnis /tmp</li> <li>• 128 MB im Ausgangsverzeichnis des Rootbenutzers</li> <li>• 2 GB für den Bereich der gemeinsam genutzten Ressourcen</li> </ul> <p>Für den Fall, dass ein Problem auftritt und eine Diagnose erforderlich ist, wird empfohlen, temporären oder anderen Speicherbereich für ein FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) oder für andere temporäre Verwendungszwecke (z. B. für die Erfassung von Traceprotokollen) auf dem System verfügbar zu haben.</p> <p>Sehr viel zusätzlicher Plattenspeicherplatz ist für Datenbank- und Protokolldateien erforderlich. Die Größe der Datenbank ist von der Anzahl der zu speichernden Clientdateien und von der Methode abhängig, mit der sie vom Server verwaltet werden. Der Standardspeicherbereich der aktiven Protokolldatei beträgt 16 GB, das für die meisten Arbeitslasten und Konfigurationen benötigte Minimum. Wenn Sie die aktive Protokolldatei erstellen, benötigen Sie mindestens 64 GB für die Replikation. Wird sowohl Replikation als auch Datendeduplizierung verwendet, erstellen Sie eine aktive Protokolldatei mit einer Größe von 128 GB. Ordnen Sie mindestens die dreifache Größe des Standardspeicherbereichs der aktiven Protokolldatei für das Archivprotokoll zu (48 GB). Stellen Sie sicher, dass Sie über ausreichende Ressourcen verfügen, wenn Sie die Datendeduplizierung verwenden oder eine hohe Clientauslastung erwarten.</p> <p>Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN.</p> <p>Lesen Sie den Abschnitt zur Linux: Kapazitätsplanung, um weitere Informationen zum Plattenspeicherplatz zu erhalten.</p> |
| Hauptspeicher   | <p>Folgende Mindestwerte für den Hauptspeicher:</p> <ul style="list-style-type: none"> <li>• 16 GB für Standardserverbetrieb ohne Datendeduplizierung und Knotenreplikation</li> <li>• 24 GB für Datendeduplizierung oder Knotenreplikation</li> <li>• 32 GB für Knotenreplikation mit Datendeduplizierung</li> </ul> <p>Speziellere Angaben zum Speicherbedarf für große Datenbanken und höhere Aufnahmefähigkeit finden Sie in der Tabelle für die Serverspeicheroptimierung von IBM Spectrum Protect.</p> <p>Ausführliche Informationen zum Speicherbedarf bei Verwendung der Datendeduplizierung finden Sie unter IBM Spectrum Protect Blueprint für Ihr Betriebssystem.</p>   |

## Softwarevoraussetzungen

In Tabelle 2 sind die für einen Server auf einem Linux x86\_64-System erforderlichen Softwaremindestvoraussetzungen beschrieben.

Tabelle 2. Softwarevoraussetzungen

| Softwaretyp    | Softwaremindestvoraussetzungen   |
|----------------|--|
| Betriebssystem | <p>Für den IBM Spectrum Protect-Server unter Linux x86_64 ist eines der folgenden Betriebssysteme erforderlich:</p> <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux 6.7</li> <li>• Red Hat Enterprise Linux 7, einschließlich Updates</li> <li>• SUSE Linux Enterprise Server 11, Service-Pack 4 oder höher</li> <li>• SUSE Linux Enterprise Server 12</li> <li>• Ubuntu Server LTS, Version 16.04 oder höher</li> </ul> |

| Softwaretyp           | Softwaremindestvoraussetzungen   |
|-----------------------|--|
| Bibliotheken          | <p>Auf dem IBM Spectrum Protect-System installierte GNU C-Bibliotheken Version 2.3.3-98.38 oder höher.<br/>Für Red Hat Enterprise Linux Server:</p> <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 (32- und 64-Bit-Pakete sind erforderlich)</li> <li>• numactl.x86_64</li> </ul> <p>Für SUSE Linux Enterprise Server:</p> <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 Version 4.3 oder höher (32- und 64-Bit-Pakete sind erforderlich)</li> </ul> <p>Für Ubuntu LTS Server:</p> <ul style="list-style-type: none"> <li>• libaio1</li> </ul> <p>Führen Sie einen der folgenden Schritte aus, um festzustellen, ob SELinux installiert ist und sich im restriktiven Modus befindet:</p> <ul style="list-style-type: none"> <li>• Überprüfen Sie die Datei /etc/sysconfig/selinux.</li> <li>• Führen Sie den Betriebssystembefehl <code>sestatus</code> aus.</li> <li>• Überprüfen Sie die Datei /var/log/messages auf SELinux-Nachrichten.</li> </ul> <p>Führen Sie einen der folgenden Schritte aus, um SELinux zu inaktivieren:</p> <ul style="list-style-type: none"> <li>• Geben Sie den toleranten Modus an, indem Sie den Befehl <code>setenforce 0</code> als Superuser ausgeben.</li> <li>• Ändern Sie die Datei /etc/sysconfig/selinux und führen Sie einen Neustart der Maschine durch.</li> </ul> |
| Übertragungsprotokoll | <ul style="list-style-type: none"> <li>• TCP/IP Version 4 oder Version 6 (Standard für Linux)</li> <li>• Shared Memory-Protokoll (mit IBM Spectrum Protect Linux x86_64-Client)</li> </ul>   |
| Verarbeitung          | Asynchrone Ein-/Ausgabe muss aktiviert sein. Installieren Sie für Linux-Kernel mit 2.6 oder höher die Bibliothek libaio, um die asynchrone Ein-/Ausgabe zu aktivieren.   |
| Einheitentreiber      | <p>Der IBM Spectrum Protect-Durchgriffseinheitentreiber wird für Einheiten eines anderen Herstellers verwendet. Er verwendet die SCSI-Durchgriffsschnittstelle für die Kommunikation mit Bandeinheiten und Bandarchiven. Der generische Linux-SCSI-Einheitentreiber (<code>sg</code>) ist für Bandlaufwerke und Bandarchive erforderlich. Das IBM Spectrum Protect-Einheitentreiberpaket enthält Einheitentreibertools und ACSLS-Dämonen.</p> <p>Für die Bandarchive bzw. Bandlaufwerke IBM® 3590, 3592 oder Ultrium sind die IBM Einheitentreiber erforderlich. Installieren Sie die aktuellen Einheitentreiber. IBM-Treiberpakete finden Sie bei Fix Central.</p> <p>Konfigurieren Sie die Einheitentreiber, bevor Sie den Server für Bandeinheiten verwenden.</p> <p>Tipp: Bandspeicher wird in Ubuntu Server LTS nicht unterstützt.</p>  |
| Sonstige Software     | <p>Korn-Shell (<code>ksh</code>) ist erforderlich.</p> <p>Um IBM Spectrum Protect-Benutzer mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol) zu authentifizieren, müssen Sie einen der folgenden Verzeichnisserver verwenden:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server Version 6.3</li> <li>• IBM Security Directory Server Version 6.4</li> </ul>  |

## Linux: Servermindestvoraussetzungen für Linux on System z

Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux on System z-Betriebssystem installieren.

### Hardwarevoraussetzungen

In Tabelle 1 sind die für Ihr IBM Spectrum Protect-System unter Linux on System z erforderlichen Hardwaremindestvoraussetzungen beschrieben. Weitere Informationen zur Planung des Plattenspeicherplatzes finden Sie in Linux: Kapazitätsplanung.

Tabelle 1. Hardwarevoraussetzungen

| Hardwaretyp     | Hardwarevoraussetzungen  |
|-----------------|--|
| Server          | Eine native logische 64-Bit-Partition (LPAR) oder eine z/VM-Gastmaschine unter IBM® zSeries, IBM System z9, IBM System z10 oder IBM zEnterprise System (z114 und z196).  |
| Plattenspeicher | <p>Folgende Mindestwerte für den Plattenspeicher:</p> <ul style="list-style-type: none"> <li>• 5 GB für das Installationsverzeichnis</li> <li>• 512 MB für das Verzeichnis /var</li> <li>• 2 GB für das Verzeichnis /tmp</li> <li>• 128 MB im Ausgangsverzeichnis des Rootbenutzers</li> <li>• 2 GB für den Bereich der gemeinsam genutzten Ressourcen</li> </ul> <p>Für den Fall, dass ein Problem auftritt und eine Diagnose erforderlich ist, wird empfohlen, temporären oder anderen Speicherbereich für ein FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) oder für andere temporäre Verwendungszwecke (z. B. für die Erfassung von Traceprotokollen) auf dem System verfügbar zu haben.</p> <p>Sehr viel zusätzlicher Plattenspeicherplatz ist für Datenbank- und Protokolldateien erforderlich. Die Größe der Datenbank ist von der Anzahl der zu speichernden Clientdateien und von der Methode abhängig, mit der sie vom Server verwaltet werden. Der Standardspeicherbereich der aktiven Protokolldatei beträgt 16 GB, das für die meisten Arbeitslasten und Konfigurationen benötigte Minimum. Wenn Sie die aktive Protokolldatei erstellen, benötigen Sie mindestens 64 GB für die Replikation. Wird sowohl Replikation als auch Datendeduplizierung verwendet, erstellen Sie eine aktive Protokolldatei mit einer Größe von 128 GB. Ordnen Sie mindestens die dreifache Größe des Standardspeicherbereichs der aktiven Protokolldatei für das Archivprotokoll zu (48 GB). Stellen Sie sicher, dass Sie über ausreichende Ressourcen verfügen, wenn Sie die Datendeduplizierung verwenden oder eine hohe Clientauslastung erwarten.</p> <p>Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN.</p> <p>Lesen Sie den Abschnitt zur Linux: Kapazitätsplanung, um weitere Informationen zum Plattenspeicherplatz zu erhalten.</p> |
| Hauptspeicher   | <p>Folgende Mindestwerte für den Hauptspeicher:</p> <ul style="list-style-type: none"> <li>• 16 GB für Standardserverbetrieb ohne Datendeduplizierung und Knotenreplikation</li> <li>• 24 GB für Datendeduplizierung oder Knotenreplikation</li> <li>• 32 GB für Knotenreplikation mit Datendeduplizierung</li> </ul> <p>Speziellere Angaben zum Speicherbedarf für große Datenbanken und höhere Aufnahmefähigkeit finden Sie in der Tabelle für die Serverspeicheroptimierung von IBM Spectrum Protect.</p> <p>Ausführliche Informationen zum Speicherbedarf bei Verwendung der Datendeduplizierung finden Sie unter IBM Spectrum Protect Blueprint für Ihr Betriebssystem.</p>   |

## Softwarevoraussetzungen

In Tabelle 2 sind die für Ihr IBM Spectrum Protect-System unter Linux on System z erforderlichen Softwaremindestvoraussetzungen beschrieben.

Tabelle 2. Softwarevoraussetzungen

| Softwaretyp | Softwaremindestvoraussetzungen  |
|-------------|---|
| Server      | <p>Für den IBM Spectrum Protect-Server unter Linux on System z (s390x-64-Bit-Architektur) ist eines der folgenden Betriebssysteme erforderlich:</p> <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux 7.1</li> <li>• SUSE Linux Enterprise Server 12</li> </ul> |

| Softwaretyp           | Softwaremindestvoraussetzungen  |
|-----------------------|---|
| Bibliotheken          | <p>Eine auf dem IBM Spectrum Protect-System installierte GNU C-Bibliothek Version 2.4-31.43.6.<br/>Für SUSE Linux Enterprise Server:</p> <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 Version 4.3 oder höher (32- und 64-Bit-Pakete sind erforderlich)</li> <li>• libxlc-1.2.0.0.151119a.s390x oder höher</li> </ul> <p>Für Red Hat Enterprise Linux Server:</p> <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 (32- und 64-Bit-Pakete sind erforderlich)</li> <li>• numactl.x86_64</li> <li>• libxlc-1.2.0.0.151119a.s390x oder höher</li> </ul> |
| Übertragungsprotokoll | <ul style="list-style-type: none"> <li>• TCP/IP Version 4 oder Version 6 (Standard für Linux)</li> <li>• Shared Memory-Protokoll (mit IBM Spectrum Protect Version 8.1.3 Linux on System z-Client)</li> </ul>   |
| Verarbeitung          | Asynchrone Ein-/Ausgabe muss aktiviert sein. Installieren Sie für Linux-Kernel mit 2.6 oder höher die Bibliothek libaio, um die asynchrone Ein-/Ausgabe zu aktivieren.  |
| Sonstige Software     | <p>Korn-Shell (ksh) ist erforderlich.</p> <p>Um IBM Spectrum Protect-Benutzer mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol) zu authentifizieren, müssen Sie einen der folgenden Verzeichnisserver verwenden:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server Version 6.3</li> <li>• IBM Security Directory Server Version 6.4</li> </ul>  |

## Linux: Servermindestvoraussetzungen für Linux on Power Systems (Little Endian)

Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux on Power Systems-Betriebssystem (Little Endian) installieren.

### Hardwarevoraussetzungen

In Tabelle 1 sind die Hardwaremindestvoraussetzungen für den Server beschrieben. Wenn der Server die Mindestvoraussetzungen nicht erfüllt, schlägt die Installation fehl. Weitere Informationen zur Planung des Plattenspeicherplatzes finden Sie in Linux: Kapazitätsplanung.

Tabelle 1. Hardwarevoraussetzungen

| Hardwaretyp | Hardwarevoraussetzungen  |
|-------------|--|
| Server      | Ein Linux on Power Systems-Server (Little Endian) auf einem IBM® System. Zum Beispiel ein auf der Website Linux on IBM Power Systems aufgelisteter Server. |

| Hardwaretyp     | Hardwarevoraussetzungen   |
|-----------------|---|
| Plattenspeicher | <p>Folgender Mindestplattenspeicher:</p> <ul style="list-style-type: none"> <li>• 5 GB für das Installationsverzeichnis</li> <li>• 128 MB im Ausgangsverzeichnis des Rootbenutzers</li> <li>• 2 GB für den Bereich der gemeinsam genutzten Ressourcen</li> </ul> <p>Für den Fall, dass ein Problem auftritt und eine Diagnose erforderlich ist, wird empfohlen, temporären oder anderen Speicherbereich für ein FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) oder für andere temporäre Verwendungszwecke (z. B. für die Erfassung von Traceprotokollen) auf dem System verfügbar zu haben.</p> <p>Sehr viel zusätzlicher Plattenspeicherplatz ist für Datenbank- und Protokolldateien erforderlich. Die Größe der Datenbank ist von der Anzahl der zu speichernden Clientdateien und von der Methode abhängig, mit der sie vom Server verwaltet werden. Der Standardspeicherbereich der aktiven Protokolldatei beträgt 16 GB, das für die meisten Arbeitslasten und Konfigurationen benötigte Minimum. Wenn Sie die aktive Protokolldatei erstellen, benötigen Sie mindestens 64 GB für die Replikation. Wird sowohl Replikation als auch Datendeduplizierung verwendet, erstellen Sie eine aktive Protokolldatei mit einer Größe von 128 GB. Ordnen Sie mindestens die dreifache Größe des Standardspeicherbereichs der aktiven Protokolldatei für das Archivprotokoll zu (48 GB). Stellen Sie sicher, dass Sie über ausreichende Ressourcen verfügen, wenn Sie die Datendeduplizierung verwenden oder eine hohe Clientauslastung erwarten.</p> <p>Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN.</p> <p>Lesen Sie den Abschnitt zur Linux: Kapazitätsplanung, um weitere Informationen zum Plattenspeicherplatz zu erhalten.</p> |
| Hauptspeicher   | <ul style="list-style-type: none"> <li>• 16 GB für Standardserverbetrieb ohne Datendeduplizierung und Knotenreplikation</li> <li>• 24 GB für Datendeduplizierung oder Knotenreplikation</li> <li>• 32 GB für Knotenreplikation mit Datendeduplizierung</li> </ul> <p>Speziellere Angaben zum Speicherbedarf für große Datenbanken und höhere Aufnahmefähigkeit finden Sie in der Tabelle für die Serverspeicheroptimierung von IBM Spectrum Protect.</p> <p>Ausführliche Informationen zum Speicherbedarf bei Verwendung der Datendeduplizierung finden Sie unter IBM Spectrum Protect Blueprint für Ihr Betriebssystem.</p>  |

## Softwarevoraussetzungen

In Tabelle 2 sind die für Ihr System erforderlichen Softwaremindestvoraussetzungen beschrieben.

Tabelle 2. Softwarevoraussetzungen

| Softwaretyp           | Softwaremindestvoraussetzungen   |
|-----------------------|--|
| Betriebssystem        | Red Hat Enterprise Linux (RHEL) 7.3 mit PPC64LE-Architektur.   |
| Bibliotheken          | GNU-C-Bibliotheken Version 2.4-31.30 und höher.<br>libaio.so.1 (32- und 64-Bit-Pakete).  |
| Übertragungsprotokoll | <ul style="list-style-type: none"> <li>• TCP/IP Version 4 oder Version 6 (Standard für Linux)</li> <li>• Shared Memory-Protokoll (mit einem Client der Version 8.1.3)</li> </ul>   |
| Verarbeitung          | Asynchrone Ein-/Ausgabe muss aktiviert sein. Installieren Sie für Linux-Kernel mit 2.6 oder höher die Bibliothek libaio, um die asynchrone Ein-/Ausgabe zu aktivieren.   |
| Sonstige Software     | <p>Korn-Shell (ksh) ist erforderlich.</p> <p>Um IBM Spectrum Protect-Benutzer mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol) zu authentifizieren, müssen Sie einen der folgenden Verzeichnisserver verwenden:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server Version 6.3</li> <li>• IBM Security Directory Server Version 6.4</li> </ul> |

Einschränkung: Unformatierte logische Datenträger werden nicht unterstützt.

## Linux: Kompatibilität des IBM Spectrum Protect-Servers mit anderen DB2-Produkten auf dem System

Sie können andere Produkte, die DB2-Produkte auf demselben System wie der IBM Spectrum Protect-Server der Version 8.1.3 implementieren und verwenden, mit einigen Einschränkungen installieren.

Damit andere Produkte, die ein DB2-Produkt auf demselben System wie der IBM Spectrum Protect-Server verwenden, installiert und verwendet werden können, müssen die folgenden Bedingungen erfüllt sein:

Tabelle 1. Kompatibilität des IBM Spectrum Protect-Servers mit anderen DB2-Produkten auf dem System

| Bedingung                      | Anweisungen   |
|--------------------------------|---|
| Versionsschnittstelle          | Die anderen Produkte, die ein DB2-Produkt verwenden, müssen DB2 Version 9 oder höher verwenden. DB2-Produkte verfügen ab Version 9 über die Unterstützung für Produktkapselung und -trennung. Ab dieser Version können Sie mehrere Kopien von DB2-Produkten mit unterschiedlichen Codeversionen auf demselben System ausführen. Ausführliche Informationen finden Sie in dem Abschnitt über mehrere DB2-Kopien in der Produktinformation zu DB2.  |
| Benutzer-IDs und Verzeichnisse | Stellen Sie sicher, dass die Benutzer-IDs, die IDs der abgeschirmten Benutzer, die Installationsposition, andere Verzeichnisse und zugehörige Informationen nicht von mehreren DB2-Installationen gemeinsam genutzt werden. Ihre Angaben müssen sich von den IDs und Positionen unterscheiden, die Sie für die Installation und Konfiguration des IBM Spectrum Protect-Servers verwendet haben. Wenn Sie den Assistenten dsmicfgx für die Konfiguration des Servers verwendet haben, haben Sie diese Werte während der Ausführung des Assistenten eingegeben. Wenn Sie eine manuelle Konfiguration durchgeführt haben, überprüfen Sie im Bedarfsfall die verwendeten Prozeduren, um sich die für den Server verwendeten Werte in Erinnerung zu rufen.   |
| Ressourcenanzuordnung          | <p>Sie müssen die Ressourcen und das Leistungsspektrum des Systems gegen die Anforderungen für den IBM Spectrum Protect-Server und die anderen Anwendungen, die das DB2-Produkt verwenden, abwägen. Damit den anderen DB2-Anwendungen genügend Ressourcen zur Verfügung stehen, müssen Sie unter Umständen die Einstellungen des IBM Spectrum Protect-Servers ändern, so dass der Server weniger Systemspeicher und -ressourcen verwendet. Wenn die Verarbeitungsprozesse für die anderen DB2-Anwendungen und der IBM Spectrum Protect-Server um Prozessor- und Speicherressourcen konkurrieren, kann die Leistung des Servers in Bezug auf die Verarbeitung der erwarteten Clientauslastung oder anderer Serveroperationen beeinträchtigt werden.</p> <p>Um die Ressourcen zu trennen und die Möglichkeit zur Optimierung und Zuordnung von Prozessor-, Speicher- und anderen Systemressourcen für mehrere Anwendungen zu verbessern, sollten Sie Unterstützung für logische Partitionen (LPAR), Auslastungspartitionierung (WPAR) oder andere Unterstützung für virtuelle Workstations einsetzen. Führen Sie eine DB2-Anwendung beispielsweise auf einem eigenen virtuellen System aus.</p> |

## Linux: IBM Installation Manager

IBM Spectrum Protect verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositorys installiert oder aktualisiert werden können.

Wenn die erforderliche Version von IBM Installation Manager noch nicht installiert ist, wird sie automatisch installiert oder aktualisiert, wenn Sie IBM Spectrum Protect installieren. Die Software muss auf dem System installiert bleiben, damit IBM Spectrum Protect später nach Bedarf aktualisiert oder deinstalliert werden kann.

Die folgende Liste enthält Erläuterungen einiger Begriffe, die in IBM Installation Manager verwendet werden:

### Angebot

Eine installierbare Einheit eines Softwareprodukts.

Das Angebot 'IBM Spectrum Protect' enthält alle Datenträger, die IBM Installation Manager für die Installation von IBM Spectrum Protect benötigt.

### Paket

Die Gruppe der Softwarekomponenten, die für die Installation eines Angebots benötigt werden.

Das IBM Spectrum Protect-Paket enthält folgende Komponenten:

- Installationsprogramm IBM Installation Manager



- Das Angebot 'IBM Spectrum Protect'

#### Paketgruppe

Eine Gruppe von Paketen mit demselben übergeordneten Verzeichnis.

Die Standardpaketgruppe für das IBM Spectrum Protect-Paket ist `IBM Installation Manager`.

#### Repository

Ein ferner oder lokaler Speicherbereich für Daten und andere Anwendungsressourcen.

Das IBM Spectrum Protect-Paket wird in einem Repository in IBM Fix Central gespeichert.

#### Verzeichnis für gemeinsam genutzte Ressourcen

Ein Verzeichnis, das Softwaredateien oder Plug-ins enthält, die von Paketen gemeinsam genutzt werden.

In dem Verzeichnis für gemeinsam genutzte Ressourcen speichert IBM Installation Manager installationsbezogene Dateien, darunter Dateien, die für das Rollback zu einer vorherigen Version von IBM Spectrum Protect verwendet werden.

## Linux: Arbeitsblätter für Planungsdetails für den Server

Sie können die Arbeitsblätter für die Planung der Größe und der Position des für den IBM Spectrum Protect-Server benötigten Speichers verwenden. Sie können darauf auch Namen und Benutzer-IDs aufzeichnen.

| Element  | Erforderlicher Speicherbereich | Anzahl der Verzeichnisse | Position der Verzeichnisse |
|--|--------------------------------|--------------------------|----------------------------|
| Die Datenbank  |                                |                          |                            |
| Aktive Protokolldatei  |                                |                          |                            |
| Archivprotokoll  |                                |                          |                            |
| Optional: Protokollspiegel für die aktive Protokolldatei                         |                                |                          |                            |
| Optional: Sekundäres Archivprotokoll (Übernahmeverzeichnis für Archivprotokolle) |                                |                          |                            |

| Element   | Namen und Benutzer-IDs | Position |
|---|------------------------|----------|
| Die <i>Instanzbenutzer-ID</i> für den Server. Mit dieser ID starten Sie den IBM Spectrum Protect-Server und führen ihn aus.   |                        |          |
| Das <i>Ausgangsverzeichnis</i> des Servers. In diesem Verzeichnis befindet sich die Instanzbenutzer-ID.   |                        |          |
| Der Datenbankinstanzname  |                        |          |
| Das <i>Instanzverzeichnis</i> für den Server. Dieses Verzeichnis enthält spezielle Dateien für diese Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien). |                        |          |
| Der Servername; verwenden Sie einen eindeutigen Namen für jeden Server.   |                        |          |

## Linux: Kapazitätsplanung

Zur Kapazitätsplanung für IBM Spectrum Protect gehört die Verwaltung von Ressourcen wie z. B. die Datenbank, das Wiederherstellungsprotokoll und der Bereich für gemeinsam genutzte Ressourcen. Sie müssen den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll schätzen, um die Ressourcen als Teil der Kapazitätsplanung zu maximieren. Der verfügbare Speicherplatz für den Bereich für gemeinsam genutzte Ressourcen muss für jede Installation bzw. jedes Upgrade ausreichen.

- Linux: Speicherbedarf für die Datenbank schätzen  
Sie können den Speicherbedarf für die Datenbank auf der Basis der maximalen Anzahl Dateien schätzen, die sich gleichzeitig im Serverspeicher befinden können, oder auf der Basis der Speicherpoolkapazität.
- Linux: Speicherplatzbedarf für das Wiederherstellungsprotokoll  
In IBM Spectrum Protect beinhaltet der Begriff *Wiederherstellungsprotokoll* die aktive Protokolldatei, das Archivprotokoll, den Spiegel der aktiven Protokolldatei und das Archivübernahmeprotokoll. Der für das Wiederherstellungsprotokoll erforderliche Speicherbereich ist von verschiedenen Faktoren, wie z. B. dem Umfang der Clientaktivität mit dem Server, abhängig.
- Linux: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen  
Um den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei zu bestimmen, geben Sie den Befehl QUERY LOG ein. Um die Speicherauslastung in der Datenbank und den Wiederherstellungsprotokollen zu überwachen, können Sie auch das Aktivitätenprotokoll auf Nachrichten überprüfen.
- Linux: Rollbackdateien der Installation löschen  
Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, löschen, um Speicherplatz im Verzeichnis für gemeinsam genutzte Ressourcen freizugeben. Zu den Dateitypen, die Sie löschen können, gehören z. B. Dateien, die für eine Rollbackoperation benötigt wurden.

## Linux: Speicherbedarf für die Datenbank schätzen

---

Sie können den Speicherbedarf für die Datenbank auf der Basis der maximalen Anzahl Dateien schätzen, die sich gleichzeitig im Serverspeicher befinden können, oder auf der Basis der Speicherpoolkapazität.

### Informationen zu diesem Vorgang

---

Anfänglich sollte mindestens 25 GB Speicherplatz in der Datenbank verwendet werden. Stellen Sie entsprechend Speicherplatz im Dateisystem bereit. Eine Datenbankgröße von 25 GB ist für eine Testumgebung oder eine Umgebung, die nur einen Speicherarchivmanager umfasst, ausreichend. Für einen Produktionsserver, der Clientlasten unterstützt, sollte die Datenbank größer sein. Wenn Sie Plattenspeicherpools (DISK) mit wahlfreiem Zugriff verwenden, ist mehr Datenbank- und Protokollspeicherbereich erforderlich als für Speicherpools mit sequenziellem Zugriff.

Die maximale Größe der IBM Spectrum Protect-Datenbank beträgt 6 TB.

Informationen zur Festlegung der Größe einer Datenbank in einer Produktionsumgebung, die auf der Anzahl Dateien und der Speicherpoolgröße basiert, enthalten die folgenden Abschnitte.

- Linux: Speicherbedarf für die Datenbank auf der Basis der Anzahl Dateien schätzen  
Wenn die maximale Anzahl Dateien, die sich zu einem bestimmten Zeitpunkt im Serverspeicher befinden, geschätzt werden kann, können Sie diese Zahl verwenden, um den Speicherbedarf für die Datenbank zu schätzen.
- Linux: Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität schätzen  
Um den Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität zu schätzen, verwenden Sie ein Verhältnis von 1-5 %. Sind beispielsweise 200 TB Speicherpoolkapazität erforderlich, sollte die Größe der Datenbank erwartungsgemäß zwischen 2 und 10 TB betragen. Als allgemeine Regel gilt: Wählen Sie die Größe ihrer Datenbank so groß wie möglich, um zu verhindern, dass der Speicherplatz knapp wird. Wenn der Speicherplatz knapp wird, können Serveroperationen und Clientspeicheroperationen fehlschlagen.
- Linux: Datenbankmanager und temporärer Speicherbereich  
Der Datenbankmanager des IBM Spectrum Protect-Servers verwaltet System Speicher und Plattenspeicher für die Datenbank und ordnet diesen Speicher zu. Der benötigte Datenbankspeicherbereich ist von der Größe des verfügbaren System Speichers und von der Serverauslastung abhängig.

## Linux: Speicherbedarf für die Datenbank auf der Basis der Anzahl Dateien schätzen

---

Wenn die maximale Anzahl Dateien, die sich zu einem bestimmten Zeitpunkt im Serverspeicher befinden, geschätzt werden kann, können Sie diese Zahl verwenden, um den Speicherbedarf für die Datenbank zu schätzen.

### Informationen zu diesem Vorgang

---

Um den Speicherbedarf auf der Basis der maximalen Anzahl Dateien im Serverspeicher zu schätzen, verwenden Sie die folgenden Richtlinien:

- 600-1000 Byte für jede gespeicherte Version einer Datei einschließlich der Imagesicherungen.  
Einschränkung: Diese Richtlinie umfasst nicht den Speicherplatz, der während der Datendeduplizierung verwendet wird.
- 100-200 Byte für jede Datei im Cache, jede Kopierspeicherpooldatei, jede Datei im Pool für aktive Daten und jede deduplizierte Datei.

- Zusätzlicher Speicherbereich ist für die Datenbankoptimierung erforderlich, um variable Datenzugriffsmuster und die Server-Back-End-Verarbeitung von Daten zu unterstützen. Die Größe des zusätzlichen Speicherplatzes entspricht 50 % der Schätzung für die Gesamtanzahl Byte für Dateiobjekte.

In dem folgenden Beispiel für einen einzelnen Client basieren bei Berechnungen auf den Maximalwerten in den vorhergehenden Richtlinien. Bei den Beispielen wird die mögliche Verwendung der Dateiagregation nicht berücksichtigt. Im Allgemeinen wird durch das Aggregieren kleiner Dateien der erforderliche Speicherplatz in der Datenbank reduziert. Die Dateiagregation betrifft keine speicherwarteten Dateien.

## Vorgehensweise

1. Berechnen Sie die Anzahl Dateiversionen. Addieren Sie alle folgenden Werte, um die Anzahl Dateiversionen zu erhalten:
  - a. Berechnen Sie die Anzahl gesicherter Dateien. Beispiel: Möglicherweise werden bis zu 500.000 Clientdateien gleichzeitig gesichert. In diesem Beispiel sind die Speichermaßnahmen so definiert, dass maximal drei Kopien gesicherter Dateien aufbewahrt werden:
 
$$500.000 \text{ Dateien} * 3 \text{ Kopien} = 1.500.000 \text{ Dateien}$$
  - b. Berechnen Sie die Anzahl Archivierungsdateien. Beispiel: Bis zu 100.000 Clientdateien können archivierte Kopien sein.
  - c. Berechnen Sie die Anzahl speicherwarteter Dateien. Beispiel: Bis zu 200.000 Clientdateien können von Client-Workstations umgelagert werden.

Bei Verwendung von 1000 Byte pro Datei beträgt der Gesamtspeicherplatz in der Datenbank, der für die zu dem Client gehörigen Dateien erforderlich ist, 1,8 GB:

$$(1.500.000 + 100.000 + 200.000) * 1000 = 1,8 \text{ GB}$$

2. Berechnen Sie die Anzahl Dateien im Cache, Kopierspeicherpooldateien, Dateien im Pool für aktive Daten und deduplizierter Dateien:
  - a. Berechnen Sie die Anzahl der Cachekopien. Beispiel: In einem Plattenspeicherpool mit 5 GB Kapazität ist Caching aktiviert. Die obere Umlagerungsschwelle des Pools ist 90 % und die untere Umlagerungsschwelle ist 70 %. Das heißt 20 % des Plattenpools (oder 1 GB) wird von Cachedateien belegt. Wenn die durchschnittliche Dateigröße ungefähr 10 KB beträgt, enthält der Cache zu jedem beliebigen Zeitpunkt etwa 100.000 Dateien:
 
$$100.000 \text{ Dateien} * 200 \text{ Byte} = 19 \text{ MB}$$
  - b. Berechnen Sie die Anzahl Kopierspeicherpooldateien. Alle primären Speicherpools werden im Kopierspeicherpool gesichert:
 
$$(1.500.000 + 100.000 + 200.000) * 200 \text{ Byte} = 343 \text{ MB}$$
  - c. Berechnen Sie die Anzahl Dateien im Speicherpool für aktive Daten. Alle aktiven Clientsicherungsdaten in primären Speicherpools werden in den Speicherpool für aktive Daten kopiert. Angenommen, es sind 500.000 Versionen der 1.500.000 Sicherungsdateien im primären Speicherpool aktiv:
 
$$500.000 * 200 \text{ Byte} = 95 \text{ MB}$$
  - d. Berechnen Sie die Anzahl deduplizierter Dateien. Angenommen, ein deduplizierter Speicherpool enthält 50.000 Dateien:
 
$$50.000 * 200 \text{ Byte} = 10 \text{ MB}$$

Auf der Basis der vorhergehenden Berechnungen sind etwa 0,5 GB zusätzlicher Speicherplatz in der Datenbank für die Cachedateien, die Kopierspeicherpooldateien, die Dateien im Pool für aktive Daten und die deduplizierten Dateien des Clients erforderlich.

3. Berechnen Sie den zusätzlichen Speicherplatz, der für die Datenbankoptimierung benötigt wird. Um optimalen Datenzugriff und optimale Verwaltung durch den Server bereitzustellen, ist zusätzlicher Speicherplatz in der Datenbank erforderlich. Die Größe des zusätzlichen Speicherplatzes in der Datenbank beträgt 50 % des Gesamtspeicherbedarfs für Dateiobjekte.
 
$$(1,8 + 0,5) * 50 \% = 1,2 \text{ GB}$$
4. Die Gesamtgröße des für den Client erforderlichen Datenbankspeicherbereichs berechnen. Die Gesamtgröße beträgt ca. 3,5 GB:
 
$$1,8 + 0,5 + 1,2 = 3,5 \text{ GB}$$
5. Berechnen Sie den Gesamtspeicherplatz in der Datenbank, der für alle Clients erforderlich ist. Wenn der Client, der in den vorhergehenden Berechnungen verwendet wurde, ein typischer Client ist und Sie beispielsweise über 500 Clients verfügen, können Sie den Gesamtspeicherplatz in der Datenbank, der für alle Clients erforderlich ist, mithilfe der folgenden Berechnung schätzen:
 
$$500 * 3,5 = 1,7 \text{ TB}$$

## Ergebnisse

Tipp: In den Beispielen oben handelt es sich bei den Ergebnissen um Schätzungen. Die tatsächliche Größe der Datenbank kann aufgrund von Faktoren wie beispielsweise der Anzahl Verzeichnisse und der Länge der Pfad- und Dateinamen von der geschätzten Größe abweichen. Sie sollten die Datenbank regelmäßig überwachen und die Größe wie erforderlich anpassen.

## Nächste Schritte

Während des normalen Betriebs erfordert der IBM Spectrum Protect-Server möglicherweise temporären Speicherplatz in der Datenbank. Dieser Speicherplatz wird aus den folgenden Gründen benötigt:

- Zum Speichern der Ergebnisse der Sortierung oder Änderung der Reihenfolge, die noch nicht in der Datenbank aufbewahrt und in der Datenbank nicht unmittelbar optimiert werden. Die Ergebnisse werden vorübergehend in der Datenbank zur Verarbeitung gespeichert.
- Zum Erteilen des Verwaltungszugriffs auf die Datenbank über eine der folgenden Methoden:
  - Ein DB2-ODBC-Client (ODBC = Open Database Connectivity)
  - Ein Oracle-JDBC-Client (JDBC = Java™ Database Connectivity)
  - SQL (Structured Query Language) für den Server über die Befehlszeile eines Verwaltungsclients

Erwägen Sie die Verwendung von zusätzlichen 50 GB an temporärem Speicherplatz pro 500 GB Speicherbereich für Dateiobjekte und Optimierung. Siehe die Richtlinien in der folgenden Tabelle. In dem Beispiel, das im vorhergehenden Schritt verwendet wurde, sind insgesamt 1,7 TB Speicherplatz in der Datenbank für Dateiobjekte und die Optimierung für 500 Clients erforderlich. Auf der Basis dieser Berechnung sind 200 GB für temporären Speicherplatz erforderlich. Der erforderliche Gesamt Speicherplatz in der Datenbank beträgt 1,9 TB.

| Datenbankgröße      | Mindestens erforderlicher temporärer Speicherplatz |
|---------------------|--|
| < 500 GB            | 50 GB  |
| ≥ 500 GB und < 1 TB | 100 GB   |
| ≥ 1 TB und < 1,5 TB | 150 GB   |
| ≥ 1,5 und < 2 TB    | 200 GB   |
| ≥ 2 und < 3 TB      | 250-300 GB   |
| ≥ 3 und < 4 TB      | 350-400 GB   |

## Linux: Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität schätzen

Um den Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität zu schätzen, verwenden Sie ein Verhältnis von 1-5 %. Sind beispielsweise 200 TB Speicherpoolkapazität erforderlich, sollte die Größe der Datenbank erwartungsgemäß zwischen 2 und 10 TB betragen. Als allgemeine Regel gilt: Wählen Sie die Größe ihrer Datenbank so groß wie möglich, um zu verhindern, dass der Speicherplatz knapp wird. Wenn der Speicherplatz knapp wird, können Serveroperationen und Clientspeicheroperationen fehlschlagen.

## Linux: Datenbankmanager und temporärer Speicherbereich

Der Datenbankmanager des IBM Spectrum Protect-Servers verwaltet Systemspeicher und Plattenspeicher für die Datenbank und ordnet diesen Speicher zu. Der benötigte Datenbankspeicherbereich ist von der Größe des verfügbaren Systemspeichers und von der Serverauslastung abhängig.

Der Datenbankmanager sortiert Daten in einer bestimmten Reihenfolge, gemäß der SQL-Anweisung, mit der Sie die Daten anfordern. Je nach Auslastung des Servers und wenn es mehr Daten gibt, als der Datenbankmanager verwalten kann, werden die (der Reihenfolge nach sortierten) Daten temporärem Plattenspeicher zugeordnet. Daten werden temporärem Plattenspeicher zugeordnet, wenn die Ergebnismenge sehr umfangreich ist. Der Datenbankmanager verwaltet den verwendeten Speicher dynamisch, wenn Daten temporärem Plattenspeicher zugeordnet werden.

Bei der Verfallsverarbeitung kann beispielsweise eine umfangreiche Ergebnismenge generiert werden. Wenn der Systemspeicher in der Datenbank zur Speicherung der Ergebnismenge nicht ausreicht, wird ein Teil der Daten temporärem Plattenspeicher zugeordnet. Wenn während der Verfallsverarbeitung ein Knoten oder ein Dateibereich ausgewählt wird, der für die Verarbeitung zu groß ist, kann der Datenbankmanager die Daten im Speicher nicht sortieren. Der Datenbankmanager muss temporären Speicherbereich zum Sortieren der Daten verwenden.

Bei der Ausführung von Datenbankoperationen sollten Sie in den folgenden Szenarios eine Erweiterung des Speicherplatzes in der Datenbank vornehmen:

- Der Speicherbereich der Datenbank ist klein und die Serveroperation, die temporären Speicherbereich benötigt, belegt den verbleibenden freien Speicherbereich.
- Die Dateibereiche sind groß oder den Dateibereichen ist eine Maßnahme zugeordnet, durch die viele Dateiversionen erstellt werden.
- Der IBM Spectrum Protect-Server muss mit begrenztem Speicher ausgeführt werden. Die Datenbank verwendet den Hauptspeicher des IBM Spectrum Protect-Servers für Datenbankoperationen. Ist der verfügbare Speicher jedoch nicht ausreichend, ordnet der IBM Spectrum Protect-Server der Datenbank temporären Speicherbereich auf Platte zu. Wenn beispielsweise 10G Speicher zur Verfügung stehen und Datenbankoperationen 12G Speicher benötigen, verwendet die Datenbank temporären Speicherbereich.
- Bei der Implementierung eines IBM Spectrum Protect-Servers wird ein Fehler aufgrund fehlenden Datenbankspeicherbereichs (`out of database space`) angezeigt. Überwachen Sie das Serveraktivitätenprotokoll auf Nachrichten, die sich auf den Datenbankspeicherbereich beziehen.

Wichtig: Sie dürfen die DB2-Software, die mit IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht verändern. Führen Sie keine Installation bzw. kein Upgrade auf eine andere Version, ein anderes Release oder ein anderes Fixpack der DB2-Software durch, um eine Beschädigung der Datenbank zu vermeiden.

## Linux: Speicherplatzbedarf für das Wiederherstellungsprotokoll

---

In IBM Spectrum Protect beinhaltet der Begriff *Wiederherstellungsprotokoll* die aktive Protokolldatei, das Archivprotokoll, den Spiegel der aktiven Protokolldatei und das Archivübernahmeprotokoll. Der für das Wiederherstellungsprotokoll erforderliche Speicherbereich ist von verschiedenen Faktoren, wie z. B. dem Umfang der Clientaktivität mit dem Server, abhängig.

- **Linux: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll**  
Wenn Sie den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll schätzen, müssen Sie einigen zusätzlichen Speicherbereich für gelegentlich auftretende hohe Lasten und Übernahmesituationen einkalkulieren.
- **Linux: Speicherbereich des Spiegels für aktive Protokolldateien**  
Die aktive Protokolldatei kann gespiegelt werden, sodass die gespiegelte Kopie verwendet werden kann, falls die aktiven Protokolldateien nicht gelesen werden können. Es kann nur ein einziger Spiegel der aktiven Protokolldatei vorhanden sein.
- **Linux: Speicherbereich des Übernahmeverzeichnisses für Archivprotokolle**  
Das Übernahmeverzeichnis für Archivprotokolle wird vom Server verwendet, wenn der Speicherbereich des Verzeichnisses für Archivprotokolle nicht mehr ausreicht.

## Linux: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll

---

Wenn Sie den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll schätzen, müssen Sie einigen zusätzlichen Speicherbereich für gelegentlich auftretende hohe Lasten und Übernahmesituationen einkalkulieren.

In IBM Spectrum Protect-Servern der Version 7.1 und höher kann die aktive Protokolldatei eine maximale Größe von 512 GB haben. Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist.

Berücksichtigen Sie bei der Schätzung der Größe der aktiven Protokolldatei die folgenden allgemeinen Richtlinien:

- Die empfohlene Anfangsgröße für die aktive Protokolldatei ist 16 GB.
- Stellen Sie sicher, dass die aktive Protokolldatei mindestens groß genug ist, um die gleichzeitig ablaufende Aktivität handhaben zu können, die der Server in der Regel handhabt. Versuchen Sie als Vorsichtsmaßnahme das größte Arbeitsvolumen zu schätzen, das der Server jeweils handhabt. Stellen Sie für die aktive Protokolldatei zusätzlichen Speicherbereich bereit, der, falls erforderlich, verwendet werden kann. Ziehen Sie 20 % zusätzlichen Speicherbereich in Betracht.
- Überwachen Sie den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei. Passen Sie die Größe der aktiven Protokolldatei wie erforderlich abhängig von Faktoren wie Clientaktivität und Ebene der Serveroperationen an.
- Stellen Sie sicher, dass das Verzeichnis, das die aktive Protokolldatei enthält, mindestens genauso groß wie die aktive Protokolldatei ist. Ein Verzeichnis, das größer als die aktive Protokolldatei ist, kann Übernahmesituationen handhaben, sollten diese auftreten.
- Stellen Sie sicher, dass das Dateisystem, das das Verzeichnis für aktive Protokolldateien enthält, über mindestens 8 GB freien Speicherbereich für Anforderungen zum Versetzen temporärer Protokolle verfügt.

Die vorgeschlagene Anfangsgröße für das Archivprotokoll beträgt 48 GB.

Das Archivprotokollverzeichnis muss groß genug sein, um die Protokolldateien aufnehmen zu können, die seit der vorherigen Gesamtsicherung generiert wurden. Wenn Sie beispielsweise täglich eine Gesamtsicherung der Datenbank ausführen, muss das Archivprotokollverzeichnis groß genug sein, um die Protokolldateien für die gesamte Clientaktivität aufnehmen zu können, die während 24 Stunden stattfindet. Um Speicherbereich wiederherzustellen, löscht der Server veraltete Archivprotokolldateien nach einer

Gesamtsicherung der Datenbank. Wenn das Archivprotokollverzeichnis voll wird und kein Verzeichnis für Archivübernahmeprotokolle vorhanden ist, verbleiben Protokolldateien im Verzeichnis für aktive Protokolldateien. Diese Bedingung kann zur Folge haben, dass das Verzeichnis für aktive Protokolldateien vollständig gefüllt und der Server gestoppt wird. Bei einem Serverneustart wird ein Teil des vorhandenen Speicherbereichs für die aktive Protokolldatei freigegeben wird.

Nach der Installation des Servers können Sie die Archivprotokollauslastung und den Speicherbereich im Archivprotokollverzeichnis überwachen. Wenn sich der Speicherbereich im Archivprotokollverzeichnis füllt, können die folgenden Probleme auftreten:

- Der Server kann keine Datenbankgesamticherungen ausführen. Untersuchen und beheben Sie dieses Problem.
- Andere Anwendungen schreiben in das Archivprotokollverzeichnis und belegen den für das Archivprotokoll erforderlichen Speicherbereich. Nutzen Sie den Speicherbereich für das Archivprotokoll nicht gemeinsam mit anderen Anwendungen, einschließlich anderer IBM Spectrum Protect-Server. Stellen Sie sicher, dass jeder Server über eine separate Speicherposition verfügt, dessen Eigner dieser spezifische Server ist und der von diesem spezifischen Server verwaltet wird.
- Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen schätzen  
Grundlegende Clientspeicheroperationen umfassen Sicherung, Archivierung und Speicherbereichsverwaltung. Der Protokollspeicherbereich muss groß genug sein, um alle Speichertransaktionen handhaben zu können, die gleichzeitig aktiv sind.
- Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, schätzen  
Wenn Sie Clientoption RESOURCEUTILIZATION auf einen größeren Wert als den Standardwert gesetzt ist, erhöht sich die gleichzeitige Last für den Server.
- Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Operationen für gleichzeitiges Schreiben schätzen  
Wenn Clientsicherungsoperationen Speicherpools verwenden, die für gleichzeitiges Schreiben konfiguriert sind, erhöht sich der Protokollspeicherbedarf, der für jede Datei erforderlich ist.
- Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen und Serveroperationen schätzen  
Die Umlagerung von Daten in Serverspeicher, Identifikationsprozesse für die Datenduplizierung, Wiederherstellung und Verfallsverarbeitung werden möglicherweise gleichzeitig mit Clientspeicheroperationen ausgeführt. Verwaltungstasks wie Verwaltungsbefehle oder SQL-Abfragen von Verwaltungsclients können ebenfalls gleichzeitig mit Clientspeicheroperationen ausgeführt werden. Serveroperationen und Verwaltungstasks, die gleichzeitig ausgeführt werden, können den erforderlichen Speicherbereich für die aktive Protokolldatei erhöhen.
- Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls unter Bedingungen mit extremen Abweichungen schätzen  
Probleme in Bezug auf knapp werdenden Speicherbereich für die aktive Protokolldatei können auftreten, wenn viele Transaktionen, die sehr schnell ausgeführt werden, zusammen mit einigen Transaktionen vorhanden sind, deren Ausführung sehr viel länger dauern kann. Ein typischer Fall sind viele aktive Workstation- oder Dateiserversicherungssitzungen und wenige aktive Serversicherungssitzungen für sehr große Datenbanken. Trifft diese Situation für Ihre Umgebung zu, müssen Sie möglicherweise die Größe der aktiven Protokolldatei erhöhen, damit die Arbeit erfolgreich ausgeführt werden kann.
- Linux: Beispiel: Größe des Archivprotokolls bei Datenbankgesamticherungen schätzen  
Der IBM Spectrum Protect-Server löscht nicht benötigte Dateien nur dann aus dem Archivprotokoll, wenn eine Datenbankgesamticherung ausgeführt wird. Demzufolge müssen Sie beim Schätzen des für das Archivprotokoll erforderlichen Speicherbereichs auch die Häufigkeit, mit der Datenbankgesamticherungen ausgeführt werden, berücksichtigen.
- Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Datenduplizierungsoperationen schätzen  
Wenn Sie Daten deduplizieren, müssen Sie die Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll berücksichtigen.

## Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen schätzen

Grundlegende Clientspeicheroperationen umfassen Sicherung, Archivierung und Speicherbereichsverwaltung. Der Protokollspeicherbereich muss groß genug sein, um alle Speichertransaktionen handhaben zu können, die gleichzeitig aktiv sind.

Um die Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen zu bestimmen, führen Sie die folgende Berechnung aus:

Anzahl Clients x In jeder Transaktion gespeicherte Dateien  
x Für jede Datei benötigter Protokollspeicherbereich

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Grundlegende Clientspeicheroperationen

| Element   | Beispielwerte | Beschreibung  |
|---|---------------|---|
| Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern | 300           | Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern. |

| Element  | Beispielwerte        | Beschreibung   |
|--|----------------------|--|
| Anzahl während jeder Transaktion gespeicherter Dateien   | 4096                 | Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.  |
| Für jede Datei erforderlicher Protokollspeicherbereich   | 3053 Byte            | Der Wert von 3053 Byte für jede Datei in einer Transaktion gibt die Protokollbyte an, die erforderlich sind, wenn Dateien von einem Windows-Client gesichert werden, auf dem Dateinamen eine Länge von 12-120 Byte haben.<br><br>Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients für Sichern/Archivieren gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet. |
| Aktive Protokolldatei: vorgeschlagene Größe  | 19,5 GB <sup>1</sup> | Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.<br><br>(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 Byte = 3,5 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>3,5 + 16 = 19,5 GB  |
| Archivprotokoll: vorgeschlagene Größe  | 58,5 GB <sup>1</sup> | Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtpeicherbedarf für das Archivprotokoll zu schätzen.<br><br>3,5 x 3 = 10,5 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:<br><br>10,5 + 48 = 58,5 GB   |
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |                      |  |

## Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, schätzen

Wenn Sie Clientoption RESOURCEUTILIZATION auf einen größeren Wert als den Standardwert gesetzt ist, erhöht sich die gleichzeitige Last für den Server.

Um die Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, zu bestimmen, führen Sie die folgende Berechnung aus:

Anzahl Clients x Anzahl Sitzungen pro Client x Anzahl während  
jeder Transaktion gespeicherter Dateien x pro Datei erforderlicher  
Protokollspeicherbereich

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Mehrere Clientsitzungen

| Element | Beispielwerte | Beschreibung |
|---------|---------------|--------------|
|---------|---------------|--------------|

| Element   | Beispielwerte        |                     | Beschreibung   |
|---|----------------------|---------------------|--|
| Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern | 300                  | 1000                | Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.  |
| Mögliche Sitzungen für jeden Client   | 3                    | 3                   | Die Einstellung der Clientoption RESOURCEUTILIZATION ist größer als der Standardwert. Jede Clientsitzung führt maximal drei Sitzungen parallel aus.  |
| Anzahl während jeder Transaktion gespeicherter Dateien  | 4096                 | 4096                | Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.  |
| Für jede Datei erforderlicher Protokollspeicherbereich  | 3053                 | 3053                | Der Wert von 3053 Byte für jede Datei in einer Transaktion gibt die Protokollbyte an, die erforderlich sind, wenn Dateien von einem Windows-Client gesichert werden, auf dem Dateinamen eine Länge von 12-120 Byte haben.<br><br>Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet. |
| Aktive Protokolldatei: vorgeschlagene Größe   | 26,5 GB <sup>1</sup> | 51 GB <sup>1</sup>  | Die folgende Berechnung wurde für 300 Clients ausgeführt. 1 Gigabyte entspricht 1.073.741.824 Byte.<br><br>(300 Clients x 3 Sitzungen pro Client x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 = 10,5 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>10,5 + 16 = 26,5 GB<br><br>Die folgende Berechnung wurde für 1000 Clients ausgeführt. 1 Gigabyte entspricht 1.073.741.824 Byte.<br><br>(1000 Clients x 3 Sitzungen pro Client x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 = 35 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>35 + 16 = 51 GB                       |
| Archivprotokoll: vorgeschlagene Größe   | 79,5 GB <sup>1</sup> | 153 GB <sup>1</sup> | Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, wird die Schätzung für die aktive Protokolldatei mit 3 multipliziert:<br><br>10,5 x 3 = 31,5 GB<br><br>35 x 3 = 105 GB<br><br>Erhöhen Sie diese Werte um die vorgeschlagene Anfangsgröße von 48 GB:<br><br>31,5 + 48 = 79,5 GB<br><br>105 + 48 = 153 GB  |



| Element   | Beispielwerte | Beschreibung |
|---|---------------|--------------|
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre aktive Protokolldatei und passen Sie die Größe, falls erforderlich, an.</p> |               |              |

## Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Operationen für gleichzeitiges Schreiben schätzen

Wenn Clientsicherungsoperationen Speicherpools verwenden, die für gleichzeitiges Schreiben konfiguriert sind, erhöht sich der Protokollspeicherbedarf, der für jede Datei erforderlich ist.

Der Protokollspeicherbereich, der für jede Datei erforderlich ist, erhöht sich um ungefähr 200 Byte für jeden Kopienspeicherpool, der für eine Operation für gleichzeitiges Schreiben verwendet wird. In dem Beispiel in der folgenden Tabelle werden Daten in einem primären Speicherpool und darüber hinaus in zwei Kopienspeicherpools gespeichert. Die geschätzte Protokollgröße erhöht sich für jede Datei um 400 Byte. Wenn Sie den vorgeschlagenen Wert von 3053 Byte Protokollspeicherbereich pro Datei verwenden, sind insgesamt 3453 Byte erforderlich.

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Operationen für gleichzeitiges Schreiben

| Element   | Beispielwerte      | Beschreibung  |
|---|--------------------|---|
| Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern | 300                | Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.   |
| Anzahl während jeder Transaktion gespeicherter Dateien  | 4096               | Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.   |
| Für jede Datei erforderlicher Protokollspeicherbereich  | 3453 Byte          | <p>3053 Byte plus 200 Byte für jeden Kopienspeicherpool.</p> <p>Der Wert von 3053 Byte für jede Datei in einer Transaktion stellt die Anzahl der Protokollbyte dar, die bei der Sicherung von Dateien auf einem Windows-Client benötigt werden, wo die Dateinamen 12 - 120 Byte haben.</p> <p>Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients für Sichern/Archivieren gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.</p> |
| Aktive Protokolldatei: vorgeschlagene Größe   | 20 GB <sup>1</sup> | <p>Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.</p> <p><math>(300 \text{ Clients} \times 4096 \text{ während jeder Transaktion gespeicherte Dateien} \times 3453 \text{ Byte pro Datei}) \div 1.073.741.824 \text{ Byte} = 4,0 \text{ GB}</math></p> <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>   |

| Element  | Beispielwerte      | Beschreibung   |
|--|--------------------|--|
| Archivprotokoll: vorgeschlagene Größe  | 60 GB <sup>1</sup> | <p>Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Speicherbedarf für das Archivprotokoll zu schätzen:</p> $4 \text{ GB} \times 3 = 12 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $12 + 48 = 60 \text{ GB}$ |
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |                    |  |

## Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen und Serveroperationen schätzen

Die Umlagerung von Daten in Serverspeicher, Identifikationsprozesse für die Dateneduplizierung, Wiederherstellung und Verfallsverarbeitung werden möglicherweise gleichzeitig mit Clientspeicheroperationen ausgeführt. Verwaltungstasks wie Verwaltungsbefehle oder SQL-Abfragen von Verwaltungsclients können ebenfalls gleichzeitig mit Clientspeicheroperationen ausgeführt werden. Serveroperationen und Verwaltungstasks, die gleichzeitig ausgeführt werden, können den erforderlichen Speicherbereich für die aktive Protokolldatei erhöhen.

Beispielsweise wird bei der Umlagerung von Dateien aus dem Speicherpool mit wahlfreiem Zugriff (DISK) in einem Plattenspeicherpool mit sequenziellem Zugriff (FILE) für jede Datei, die umgelagert wird, ungefähr 110 Byte Protokollspeicherbereich verwendet. Beispiel: Angenommen, es sind 300 Clients für Sichern/Archivieren vorhanden, von denen jeder 100.000 Dateien jede Nacht sichert. Die Dateien sind anfänglich in einem DISK-Speicherpool gespeichert und werden dann in einen FILE-Speicherpool umgelagert. Um die Größe des Speicherbereichs für die aktive Protokolldatei zu schätzen, die für die Datenumlagerung erforderlich ist, verwenden Sie die folgende Berechnung. Die Anzahl Clients in der Berechnung stellt die maximale Anzahl zu einem beliebigen Zeitpunkt dar, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern.

$300 \text{ Clients} \times 100.000 \text{ Dateien pro Client} \times 110 \text{ Byte} = 3,1 \text{ GB}$

Addieren Sie diesen Wert zu der Schätzung für die Größe der aktiven Protokolldatei, die für grundlegende Clientspeicheroperationen berechnet wurde.

## Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls unter Bedingungen mit extremen Abweichungen schätzen

Probleme in Bezug auf knapp werdenden Speicherbereich für die aktive Protokolldatei können auftreten, wenn viele Transaktionen, die sehr schnell ausgeführt werden, zusammen mit einigen Transaktionen vorhanden sind, deren Ausführung sehr viel länger dauern kann. Ein typischer Fall sind viele aktive Workstation- oder Dateiserversicherungssitzungen und wenige aktive Serversicherungssitzungen für sehr große Datenbanken. Trifft diese Situation für Ihre Umgebung zu, müssen Sie möglicherweise die Größe der aktiven Protokolldatei erhöhen, damit die Arbeit erfolgreich ausgeführt werden kann.

## Linux: Beispiel: Größe des Archivprotokolls bei Datenbankgesamtsicherungen schätzen

Der IBM Spectrum Protect-Server löscht nicht benötigte Dateien nur dann aus dem Archivprotokoll, wenn eine Datenbankgesamtsicherung ausgeführt wird. Demzufolge müssen Sie beim Schätzen des für das Archivprotokoll erforderlichen Speicherbereichs auch die Häufigkeit, mit der Datenbankgesamtsicherungen ausgeführt werden, berücksichtigen.

Wenn beispielsweise einmal pro Woche eine Datenbankgesamticherung ausgeführt wird, muss der Speicherbereich für das Archivprotokoll groß genug sein, um die Informationen einer vollständigen Woche im Archivprotokoll aufnehmen zu können.

Die unterschiedliche Größe des Archivprotokolls für täglich ausgeführte Datenbankgesamticherungen wird in dem Beispiel in der folgenden Tabelle gezeigt.

Tabelle 1. Datenbankgesamticherungen

| Element   | Beispielwerte       | Beschreibung  |
|---|---------------------|---|
| Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern | 300                 | Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.   |
| Anzahl während jeder Transaktion gespeicherter Dateien  | 4096                | Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.   |
| Für jede Datei erforderlicher Protokollspeicherbereich  | 3453 Byte           | 3053 Byte für jede Datei plus 200 Byte für jeden Kopierspeicherpool.<br><br>Der Wert von 3053 Byte für jede Datei in einer Transaktion stellt die Anzahl der Protokollbyte dar, die bei der Sicherung von Dateien auf einem Windows-Client benötigt werden, wo die Dateinamen 12 - 120 Byte haben.<br><br>Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet. |
| Aktive Protokolldatei: vorgeschlagene Größe   | 20 GB <sup>1</sup>  | Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.<br><br>(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3453 Byte pro Datei) ÷ 1.073.741.824 Byte = 4,0 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>4 + 16 = 20 GB   |
| Archivprotokoll: vorgeschlagene Größe bei einer Datenbankgesamticherung pro Tag   | 60 GB <sup>1</sup>  | Aufgrund der Voraussetzung, dass Archivprotokolle über drei Sicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen:<br><br>4 GB x 3 = 12 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:<br><br>12 + 48 = 60 GB   |
| Archivprotokoll: vorgeschlagene Größe bei einer Datenbankgesamticherung pro Woche                                       | 132 GB <sup>1</sup> | Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen. Multiplizieren Sie das Ergebnis mit der Anzahl Tage, die zwischen Datenbankgesamticherungen liegen.<br><br>(4 GB x 3 ) x 7 = 84 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:<br><br>84 + 48 = 132 GB  |

| Element  | Beispielwerte | Beschreibung |
|--|---------------|--------------|
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Anfangsgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |               |              |

## Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Dateneduplizierungsoperationen schätzen

Wenn Sie Daten deduplizieren, müssen Sie die Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll berücksichtigen.

Die folgenden Faktoren haben Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll:

### Volumen der deduplizierten Daten

Welche Auswirkungen die Dateneduplizierung auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll hat, ist von dem Prozentsatz an Daten abhängig, der für die Deduplizierung auswählbar ist. Ist der Prozentsatz an Daten, die dedupliziert werden können, relativ hoch, ist mehr Protokollspeicherbereich erforderlich.

### Größe und Anzahl Speicherbereiche

Für jeden Speicherbereich, der durch einen Prozess zum Identifizieren doppelter Daten identifiziert wird, sind ungefähr 1.500 Byte Speicherbereich für die aktive Protokolldatei erforderlich. Werden beispielsweise 250.000 Speicherbereiche durch einen erkennen identifiziert, beträgt die geschätzte Größe der aktiven Protokolldatei 358 MB:

```
250.000 während jedes Prozesses ermittelte Speicherbereiche x 1.500 Byte
für jeden Speicherbereich = 358 MB
```

Betrachten Sie das folgende Szenario. 300 Clients für Sichern/Archivieren sichern jede Nacht bis zu 100.000 Dateien. Diese Aktivität hat eine Last von 30.000.000 Dateien zur Folge. Die durchschnittliche Anzahl Speicherbereiche für jede Datei ist 2. Demzufolge beträgt die Gesamtzahl Speicherbereiche 60.000.000 und der Speicherbedarf für das Archivprotokoll 84 GB:

```
60.000.000 Speicherbereiche x 1.500 Byte pro Speicherbereich = 84 GB
```

Ein Prozess zum Identifizieren doppelter Daten wird für Aggregate von Dateien ausgeführt. Ein Aggregat besteht aus Dateien, die in einer bestimmten Transaktion gespeichert sind, wie durch die Serveroption TXNGROUPMAX angegeben. Angenommen, die Serveroption TXNGROUPMAX ist auf den Standardwert 4096 gesetzt. Wenn die durchschnittliche Anzahl Speicherbereiche für jede Datei 2 beträgt, ist die Gesamtzahl Speicherbereiche in jedem Aggregat 8192 und der für die aktive Protokolldatei erforderliche Speicherbedarf 12 MB:

```
8192 Speicherbereiche in jedem Aggregat x 1500 Byte pro Speicherbereich =
12 MB
```

### Timing und Anzahl der Prozesse zum Identifizieren doppelter Daten

Das Timing und die Anzahl Prozesse zum Identifizieren doppelter Daten haben ebenfalls Auswirkungen auf die Größe der aktiven Protokolldatei. Bei Verwendung der in dem vorhergehenden Beispiel berechneten Größe der aktiven Protokolldatei von 12 MB beträgt die gleichzeitige Last für die aktive Protokolldatei 120 MB, wenn 10 Prozesse zum Identifizieren doppelter Daten parallel ausgeführt werden:

```
12 MB pro Prozess x 10 Prozesse = 120 MB
```

### Dateigröße

Große Dateien, die für die Identifizierung doppelter Daten verarbeitet werden, können ebenfalls Auswirkungen auf die Größe der aktiven Protokolldatei haben. Beispiel: Angenommen, ein Client für Sichern/Archivieren sichert ein Dateisystemimage mit einer Größe von 80 GB. Die Anzahl doppelter Speicherbereiche für dieses Objekt kann groß sein, wenn beispielsweise die in das Dateisystemimage eingeschlossenen Dateien mit Teilsicherungen gesichert wurden. Beispiel: Angenommen, ein Dateisystemimage hat 1,2 Millionen doppelte Speicherbereiche. Die 1,2 Millionen Speicherbereiche in dieser großen Datei stellen eine einzige Transaktion für einen Prozess zum Identifizieren doppelter Daten dar. Der Gesamtspeicherbereich in der aktiven Protokolldatei, der für dieses einzelne Objekt erforderlich ist, beträgt 1,7 GB:

```
1.200.000 Speicherbereich x 1.500 Byte pro Speicherbereich = 1,7 GB
```

Wenn andere, kleinere Prozesse zum Identifizieren doppelter Daten zu demselben Zeitpunkt ausgeführt werden wie der Prozess zum Identifizieren doppelter Daten für ein einzelnes großes Objekt, ist in der aktiven Protokolldatei möglicherweise nicht genügend Speicherbereich verfügbar. Beispiel: Angenommen, ein Speicherpool ist für die Deduplizierung aktiviert. Der Speicherpool enthält gemischte Daten, einschließlich vieler relativ kleiner Dateien mit einer Größe von 10 KB bis zu mehreren

hundert KB. Der Speicherpool enthält außerdem einige wenige große Objekte mit einem hohen Prozentsatz an doppelten Speicherbereichen.

Um nicht nur den Speicherbedarf zu berücksichtigen, sondern auch das Timing und die Dauer gleichzeitig ablaufender Transaktionen, erhöhen Sie die geschätzte Größe der aktiven Protokolldatei um den Faktor 2. Beispiel: Angenommen, das Ergebnis Ihrer Berechnungen für den Speicherbedarf lautet 25 GB (23,3 GB + 1,7 GB für die Deduplizierung eines großen Objekts). Wenn Deduplizierungsverarbeitung gleichzeitig ausgeführt werden, beträgt die vorgeschlagene Größe der aktiven Protokolldatei 50 GB. Die vorgeschlagene Größe des Archivprotokolls ist 150 GB.

Die Beispiele in den folgenden Tabellen zeigen Berechnungen für aktive Protokolldateien und Archivprotokolle. In dem Beispiel in der ersten Tabelle wird eine durchschnittliche Größe von 700 KB für Speicherbereiche verwendet. In dem Beispiel in der zweiten Tabelle wird eine durchschnittliche Größe von 256 KB verwendet. Wie den Beispielen zu entnehmen ist, zeigt die durchschnittliche Größe doppelter Speicherbereiche von 256 KB eine größere geschätzte Größe für die aktive Protokolldatei an. Um betriebsbezogene Probleme für den Server auf ein Mindestmaß reduzieren oder zu verhindern, verwenden Sie 256 KB für die Schätzung der Größe der aktiven Protokolldatei in Ihrer Produktionsumgebung.

Tabelle 1. Durchschnittliche Größe doppelter Speicherbereiche von 700 KB

| Element  | Beispielwerte |               | Beschreibung   |
|--|---------------|---------------|--|
| Größe des größten zu deduplizierenden Objekts  | 800 GB        | 4 TB          | Die Granularität der Verarbeitung für die Deduplizierung bezieht sich auf die Dateiebene. Demzufolge stellt die größte einzelne zu deduplizierende Datei die umfangreichste Transaktion und eine entsprechend hohe Last für die aktive Protokolldatei und das Archivprotokoll dar.   |
| Durchschnittliche Größe der Speicherbereiche   | 700 KB        | 700 KB        | Die Deduplizierungsalgorithmen verwenden eine variable Blockmethode. Nicht alle deduplizierten Speicherbereiche für eine bestimmte Datei haben dieselbe Größe, daher wird bei dieser Berechnung eine durchschnittliche Speicherbereichsgröße vorausgesetzt.  |
| Speicherbereiche für eine bestimmte Datei  | 1.198.372 Bit | 6.135.667 Bit | Bei Verwendung der durchschnittlichen Speicherbereichsgröße (700 KB), geben diese Berechnungen die Gesamtzahl Speicherbereiche für ein bestimmtes Objekt an.<br><br>Die folgende Berechnung wurde für ein Objekt mit einer Größe von 800 GB ausgeführt: $(800 \text{ GB} \div 700 \text{ KB}) = 1.198.372 \text{ Bit}$<br><br>Die folgende Berechnung wurde für ein Objekt mit einer Größe von 4 TB ausgeführt: $(4 \text{ TB} \div 700 \text{ KB}) = 6.135.667 \text{ Bit}$ |
| Aktive Protokolldatei: vorgeschlagene Größe, die für die Deduplizierung eines einzelnen großen Objekts während eines einzelnen Prozesses zum Identifizieren doppelter Daten erforderlich ist | 1,7 GB        | 8,6 GB        | Der geschätzte Speicherbereich für die aktive Protokolldatei, der für diese Transaktion benötigt wird.   |

| Element  | Beispielwerte       |                       | Beschreibung  |
|--|---------------------|-----------------------|---|
| Aktive Protokolldatei:<br>vorgeschlagene<br>Gesamtgröße  | 66 GB <sup>1</sup>  | 79,8 GB <sup>1</sup>  | <p>Multiplizieren Sie, nachdem zusätzlich zur Deduplizierung andere Aspekte der Last auf dem Server berücksichtigt wurden, die vorhandene Schätzung mit dem Faktor 2. In diesen Beispielen wird der zum Deduplizieren eines einzelnen großen Objekts erforderliche Speicherbereich für die aktive Protokolldatei im Zusammenhang mit den vorherigen Schätzungen für die erforderliche Größe der aktiven Protokolldatei betrachtet.</p> <p>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:</p> $(23,3 \text{ GB} + 1,7 \text{ GB}) \times 2 = 50 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:</p> $50 + 16 = 66 \text{ GB}$ <p>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:</p> $(23,3 \text{ GB} + 8,6 \text{ GB}) \times 2 = 63,8 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:</p> $63,8 + 16 = 79,8 \text{ GB}$ |
| Archivprotokoll:<br>vorgeschlagene<br>Größe  | 198 GB <sup>1</sup> | 239,4 GB <sup>1</sup> | <p>Multiplizieren Sie die geschätzte Größe der aktiven Protokolldatei mit dem Faktor 3.</p> <p>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:</p> $50 \text{ GB} \times 3 = 150 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $150 + 48 = 198 \text{ GB}$ <p>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:</p> $63,8 \text{ GB} \times 3 = 191,4 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $191,4 + 48 = 239,4 \text{ GB}$  |
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die die Deduplizierung verwendet, ist 32 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die die Deduplizierung verwendet, ist 96 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 32 GB bzw. 96 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |                     |                       |   |

Tabelle 2. Durchschnittliche Größe doppelter Speicherbereiche von 256 KB

| Element                                       | Beispielwerte |      | Beschreibung   |
|---|---------------|------|--|
| Größe des größten zu deduplizierenden Objekts | 800 GB        | 4 TB | Die Granularität der Verarbeitung für die Deduplizierung bezieht sich auf die Dateiebene. Demzufolge stellt die größte einzelne zu deduplizierende Datei die umfangreichste Transaktion und eine entsprechend hohe Last für die aktive Protokolldatei und das Archivprotokoll dar. |

| Element  | Beispielwerte        |                       | Beschreibung   |
|--|----------------------|-----------------------|--|
| Durchschnittliche Größe der Speicherbereiche   | 256 KB               | 256 KB                | Die Deduplizierungsalgorithmen verwenden eine variable Blockmethode. Nicht alle deduplizierten Speicherbereiche für eine bestimmte Datei haben dieselbe Größe, daher wird bei dieser Berechnung eine durchschnittliche Speicherbereichsgröße vorausgesetzt.  |
| Speicherbereiche für eine bestimmte Datei  | 3.276.800 Bit        | 16.777.216 Bit        | Bei Verwendung der durchschnittlichen Speicherbereichsgröße, geben diese Berechnungen die Gesamtzahl Speicherbereiche für ein bestimmtes Objekt an.<br><br>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:<br><br>$(800 \text{ GB} \div 256 \text{ KB}) = 3.276.800 \text{ Bit}$<br><br>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:<br><br>$(4 \text{ TB} \div 256 \text{ KB}) = 16.777.216 \text{ Bit}$  |
| Aktive Protokolldatei: vorgeschlagene Größe, die für die Deduplizierung eines einzelnen großen Objekts während eines einzelnen Prozesses zum Identifizieren doppelter Daten erforderlich ist | 4,5 GB               | 23,4 GB               | Die geschätzte Größe des Speicherbereichs für die aktive Protokolldatei, die für diese Transaktion erforderlich ist.   |
| Aktive Protokolldatei: vorgeschlagene Gesamtgröße  | 71,6 GB <sup>1</sup> | 109,4 GB <sup>1</sup> | Nachdem Sie neben der Deduplizierung andere Aspekte der Serverauslastung mit berücksichtigt haben, multiplizieren Sie die vorhandene Schätzung mit dem Faktor 2. In diesen Beispielen wird der zum Deduplizieren eines einzelnen großen Objekts erforderliche Speicherbereich für die aktive Protokolldatei im Zusammenhang mit den vorherigen Schätzungen für die erforderliche Größe der aktiven Protokolldatei betrachtet.<br><br>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:<br><br>$(23,3 \text{ GB} + 4,5 \text{ GB}) \times 2 = 55,6 \text{ GB}$<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>$55,6 + 16 = 71,6 \text{ GB}$<br><br>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:<br><br>$(23,3 \text{ GB} + 23,4 \text{ GB}) \times 2 = 93,4 \text{ GB}$<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>$93,4 + 16 = 109,4 \text{ GB}$ |

| Element  | Beispielwerte         |                       | Beschreibung   |
|--|-----------------------|-----------------------|--|
| Archivprotokoll:<br>vorgeschlagene<br>Größe  | 214,8 GB <sup>1</sup> | 328,2 GB <sup>1</sup> | <p>Die geschätzte Größe der aktiven Protokolldatei multipliziert mit dem Faktor 3.</p> <p>Die folgende Berechnung wurde für ein Objekt mit einer Größe von 800 GB ausgeführt:</p> $55,6 \text{ GB} \times 3 = 166,8 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $166,8 + 48 = 214,8 \text{ GB}$ <p>Die folgende Berechnung wurde für ein Objekt mit einer Größe von 4 TB ausgeführt:</p> $93,4 \text{ GB} \times 3 = 280,2 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $280,2 + 48 = 328,2 \text{ GB}$ |
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die die Deduplizierung verwendet, ist 32 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die die Deduplizierung verwendet, ist 96 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 32 GB bzw. 96 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |                       |                       |  |

## Linux: Speicherbereich des Spiegels für aktive Protokolldateien

Die aktive Protokolldatei kann gespiegelt werden, sodass die gespiegelte Kopie verwendet werden kann, falls die aktiven Protokolldateien nicht gelesen werden können. Es kann nur ein einziger Spiegel der aktiven Protokolldatei vorhanden sein.

Die Erstellung einer Protokollspiegel ist eine vorgeschlagene Option. Wenn Sie die aktive Protokolldatei vergrößern, wird der Protokollspiegel automatisch vergrößert. Die Spiegelung des Protokolls kann sich negativ auf die Leistung auswirken, da die doppelte E/A-Aktivität erforderlich ist, um den Spiegel zu verwalten. Der zusätzliche Speicherbereich, den der Protokollspiegel benötigt, ist ein weiterer Faktor, der bei der Entscheidung über die Erstellung eines Protokollspiegels berücksichtigt werden muss.

Wenn das Spiegelprotokollverzeichnis voll wird, gibt der Server Fehlernachrichten in das Aktivitätenprotokoll und in die Datei db2diag.log aus. Die Serveraktivität wird fortgesetzt.

## Linux: Speicherbereich des Übernahmeverzeichnis für Archivprotokolle

Das Übernahmeverzeichnis für Archivprotokolle wird vom Server verwendet, wenn der Speicherbereich des Verzeichnisses für Archivprotokolle nicht mehr ausreicht.

Durch Angabe eines Übernahmezeichnisses für Archivprotokolle können Probleme verhindert werden, die auftreten, wenn der Speicherbereich der Archivprotokolldatei nicht mehr ausreicht. Wenn sowohl das Verzeichnis für Archivprotokolle als auch das Laufwerk oder das Dateisystem, in dem sich das Übernahmeverzeichnis für Archivprotokolle befindet, voll wird, bleiben die Daten im Verzeichnis für aktive Protokolldateien. Dadurch kann die aktive Protokolldatei vollständig ausgefüllt werden, was einen Serverhalt verursacht.

## Linux: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen

Um den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei zu bestimmen, geben Sie den Befehl QUERY LOG ein. Um die Speicherauslastung in der Datenbank und den Wiederherstellungsprotokollen zu überwachen, können Sie auch das Aktivitätenprotokoll auf Nachrichten überprüfen.

### Aktive Protokolldatei



Wenn der verfügbare Speicherbereich für die aktive Protokolldatei zu gering ist, werden die folgenden Nachrichten im Aktivitätenprotokoll angezeigt:

**ANR4531I: IC\_AUTOBACKUP\_LOG\_USED\_SINCE\_LAST\_BACKUP\_TRIGGER**

Diese Nachricht wird angezeigt, wenn der Speicherbereich für die aktive Protokolldatei die angegebene maximale Größe überschreitet. Der IBM Spectrum Protect-Server startet eine Datenbankgesamticherung.

Um die maximale Protokollgröße zu ändern, stoppen Sie den Server. Öffnen Sie die Datei dmserv.opt und geben Sie für die Option ACTIVELOGSIZE einen neuen Wert an. Starten Sie anschließend den Server erneut.

**ANR0297I: IC\_BACKUP\_NEEDED\_LOG\_USED\_SINCE\_LAST\_BACKUP**

Diese Nachricht wird angezeigt, wenn der Speicherbereich für die aktive Protokolldatei die angegebene maximale Größe überschreitet. Sie müssen die Datenbank manuell sichern.

Um die maximale Protokollgröße zu ändern, stoppen Sie den Server. Öffnen Sie die Datei dmserv.opt und geben Sie für die Option ACTIVELOGSIZE einen neuen Wert an. Starten Sie anschließend den Server erneut.

**ANR4529I: IC\_AUTOBACKUP\_LOG\_UTILIZATION\_TRIGGER**

Das Verhältnis des belegten Speicherbereichs für die aktive Protokolldatei zum verfügbaren Speicherbereich für die aktive Protokolldatei überschreitet den Schwellenwert für die Protokollauslastung. Wenn mindestens eine einzige Datenbankgesamticherung ausgeführt wurde, startet der IBM Spectrum Protect-Server eine Teilsicherung der Datenbank. Andernfalls startet der Server eine Datenbankgesamticherung.

**ANR0295I: IC\_BACKUP\_NEEDED\_LOG\_UTILIZATION**

Das Verhältnis des belegten Speicherbereichs für die aktive Protokolldatei zum verfügbaren Speicherbereich für die aktive Protokolldatei überschreitet den Schwellenwert für die Protokollauslastung. Sie müssen die Datenbank manuell sichern.

## Archivprotokoll

---

Wenn der verfügbare Speicherbereich für das Archivprotokoll zu gering ist, wird die folgende Nachricht im Aktivitätenprotokoll angezeigt:

**ANR0299I: IC\_BACKUP\_NEEDED\_ARCHLOG\_USED**

Das Verhältnis des belegten Speicherbereichs für das Archivprotokoll zum verfügbaren Speicherbereich für das Archivprotokoll überschreitet den Schwellenwert für die Protokollauslastung. Der IBM Spectrum Protect-Server startet eine automatische Datenbankgesamticherung.

## Datenbank

---

Wenn der verfügbare Speicherbereich für Datenbankaktivitäten zu gering ist, wird die folgende Nachricht im Aktivitätenprotokoll angezeigt:

**ANR2992W: IC\_LOG\_FILE\_SYSTEM\_UTILIZATION\_WARNING\_2**

Der belegte Speicherplatz in der Datenbank überschreitet den Schwellenwert für die Belegung des Speicherplatzes in der Datenbank. Um den Speicherplatz für die Datenbank zu vergrößern, verwenden Sie den Befehl EXTEND DBSPACE oder das Dienstprogramm DSMSERV FORMAT mit dem Parameter DBDIR.

**ANR1546W: FILESYSTEM\_DBPATH\_LESS\_1GB**

Der verfügbare Speicherbereich in dem Verzeichnis, in dem sich die Serverdatenbankdateien befinden, beträgt weniger als 1 GB.

Wenn ein IBM Spectrum Protect-Server mit dem Dienstprogramm DSMSERV FORMAT oder dem Konfigurationsassistenten erstellt wird, werden auch eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien erstellt, in denen Datenbankinformationen gespeichert werden sollen, die vom Datenbankmanager verwendet werden. Der in dieser Nachricht angegebene Pfad gibt die Speicherposition der Datenbankinformationen an, die vom Datenbankmanager verwendet werden. Ist in dem Pfad kein Speicherbereich verfügbar, ist der Server nicht mehr funktionsfähig.

Sie müssen dem Dateisystem Speicherbereich hinzufügen oder in dem Dateisystem oder auf der Platte Speicherbereich freigeben.

## Linux: Rollbackdateien der Installation löschen

---

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, löschen, um Speicherplatz im Verzeichnis für gemeinsam genutzte Ressourcen freizugeben. Zu den Dateitypen, die Sie löschen können, gehören z. B. Dateien, die für eine Rollbackoperation benötigt wurden.

## Informationen zu diesem Vorgang

---

Zum Löschen der nicht mehr benötigten Dateien verwenden Sie den grafisch orientierten Installationsassistenten oder die Befehlszeile im Konsolenmodus.

- Linux: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen  
Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der IBM® Installation Manager-Benutzerschnittstelle löschen.
- Linux: Rollbackdateien für die Installation mit der Befehlszeile löschen  
Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der Befehlszeile löschen.


## Linux: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen

---

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der IBM® Installation Manager-Benutzerschnittstelle löschen.

### Vorgehensweise

---

1. Öffnen Sie IBM Installation Manager.  
 In dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das Unterverzeichnis eclipse (z. B. /opt/IBM/InstallationManager/eclipse) und geben Sie folgenden Befehl aus, um IBM Installation Manager zu starten:  

```
./IBMIM
```
2. Klicken Sie auf Datei > Benutzervorgaben.
3. Wählen Sie Dateien für Rollback aus.
4. Klicken Sie auf Gespeicherte Dateien löschen und dann auf OK.

## Linux: Rollbackdateien für die Installation mit der Befehlszeile löschen

---

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der Befehlszeile löschen.

### Vorgehensweise

---

1. In dem Verzeichnis, in dem IBM® Installation Manager installiert ist, wechseln Sie in das folgende Unterverzeichnis:
  -  Linux-Betriebssysteme/eclipse/tools
 Beispiel:
  -  Linux-Betriebssysteme/opt/IBM/InstallationManager/eclipse/tools
2. Geben Sie im Verzeichnis tools den folgenden Befehl aus, um eine IBM Installation Manager-Befehlszeile zu starten:
  -  Linux-Betriebssysteme./imcl -c
3. Geben Sie **P** ein, um Benutzervorgaben auszuwählen.
4. Geben Sie **3** ein, um Dateien für Rollback auszuwählen.
5. Geben Sie **D** ein, um die Dateien für Rollback zu löschen.
6. Geben Sie **A** ein, um die Änderungen anzuwenden und zum Benutzervorgabenmenü zurückzukehren.
7. Geben Sie **C** ein, um das Benutzervorgabenmenü zu verlassen.
8. Geben Sie **X** ein, um Installation Manager zu beenden.

## Linux: Empfehlungen für die Serverbenennung

---

Verwenden Sie diese Beschreibungen als Referenz bei der Installation oder beim Upgrade eines IBM Spectrum Protect-Servers.

### Instanzenbenutzer-ID

---

Die Instanzbenutzer-ID wird als Basis für andere Namen verwendet, die sich auf die Serverinstanz beziehen. Die Instanzbenutzer-ID wird auch als Instanzeigner bezeichnet.

Zum Beispiel: tsminst1

Die Instanzbenutzer-ID ist die Benutzer-ID, die über das Eigentumsrecht oder über Schreib-/Lesezugriffsberechtigung für alle Verzeichnisse verfügen muss, die Sie für die Datenbank und das Wiederherstellungsprotokoll erstellen. Der Server wird standardmäßig mit der Instanzbenutzer-ID ausgeführt. Diese Benutzer-ID benötigt außerdem Schreib-/Lesezugriff für die Verzeichnisse, die für die Einheitenklasse FILE verwendet werden.

## Ausgangsverzeichnis für die Instanzbenutzer-ID

---

Das Ausgangsverzeichnis kann während der Erstellung der Instanzbenutzer-ID erstellt werden. Hierfür wird die Option für die Erstellung eines Ausgangsverzeichnisses (-m) verwendet, falls es noch nicht vorhanden ist. Abhängig von den lokalen Einstellungen kann das Verzeichnis folgendes Format haben: `/home/Instanzbenutzer-ID`

Zum Beispiel: `/home/tsminst1`

Das Ausgangsverzeichnis dient hauptsächlich zur Aufbewahrung des Profils für die Benutzer-ID und für Sicherheitseinstellungen.

## Datenbankinstanzname

---

Der Datenbankinstanzname muss mit der Instanzbenutzer-ID identisch sein, mit der Sie die Serverinstanz ausführen.

Zum Beispiel: `tsminst1`

## Instanzverzeichnis

---

Das Instanzverzeichnis enthält spezielle Dateien für eine Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien). Es kann einen beliebigen Namen haben. Um die Identifizierung zu erleichtern, sollten Sie einen Namen verwenden, der das Verzeichnis mit dem Instanznamen verknüpft.

Sie können das Instanzverzeichnis als Unterverzeichnis des Ausgangsverzeichnisses für die Instanzbenutzer-ID erstellen. Zum Beispiel: `/home/Instanzbenutzer-ID/Instanzbenutzer-ID`

Im folgenden Beispiel befindet sich das Instanzverzeichnis im Ausgangsverzeichnis der Benutzer-ID `tsminst1`:  
`/home/tsminst1/tsminst1`

Sie können das Verzeichnis auch an einer anderen Position erstellen, zum Beispiel: `/tsmserver/tsminst1`

Im Instanzverzeichnis sind folgende Dateien für die Serverinstanz gespeichert:

- Serveroptionsdatei `dmserv.opt`
- Die Serverschlüsseldatenbankdatei `cert.kdb` und die `.arm`-Dateien (werden von Clients und anderen Servern zum Importieren der Secure Sockets Layer-Zertifikate des Servers verwendet)
- Einheitenkonfigurationsdatei, wenn die Serveroption `DEVCONFIG` keinen vollständig qualifizierten Namen angibt
- Protokolldatei für Datenträger, wenn die Serveroption `VOLUMEHISTORY` keinen vollständig qualifizierten Namen angibt
- Datenträger für Speicherpools mit dem Typ `DEVTYPE=FILE`, wenn das Verzeichnis für die Einheitenklasse nicht vollständig angegeben oder nicht vollständig qualifiziert ist
- Benutzerexits
- Traceausgabe (wenn nicht vollständig qualifiziert)

## Datenbankname


---

Der Datenbankname lautet für jede Serverinstanz immer `TSMDB1`. Dieser Name kann nicht geändert werden.

## Servername


---

Der Servername ist ein interner Name für IBM Spectrum Protect und wird für Operationen verwendet, bei denen eine Datenübertragung zwischen mehreren IBM Spectrum Protect-Servern auftritt. Zum Beispiel bei der Kommunikation zwischen Servern und bei der gemeinsamen Nutzung von Speicherarchiven.

 Linux-Betriebssysteme Der Servername wird auch verwendet, wenn Sie den Server dem Operations Center hinzufügen, so dass er mit dieser Schnittstelle verwaltet werden kann. Verwenden Sie einen eindeutigen Namen für jeden Server. Verwenden Sie einen Namen, der die Position oder den Zweck des Servers angibt, um die Identifikation im Operations Center (oder mit einem Befehl `QUERY SERVER`) zu erleichtern. Nachdem ein IBM Spectrum Protect-Server als Hub- oder Peripherieserver konfiguriert wurde, dürfen Sie seinen Namen nicht mehr ändern.

Wenn Sie den Assistenten verwenden, wird als Standardname der Hostname des von Ihnen verwendeten Systems vorgeschlagen. Sie können einen anderen, für Ihre Umgebung aussagekräftigen Namen verwenden. Befinden sich mehrere Server auf dem System, können

Sie bei Verwendung des Assistenten den Standardnamen nur für einen der Server angeben. Sie müssen einen eindeutigen Namen für jeden Server eingeben.

 Linux-Betriebssysteme Zum Beispiel:

- LOHNBUCHHALTUNG
- VERTRIEB

## Verzeichnisse für Datenbankbereich und Wiederherstellungsprotokoll

---

Die Verzeichnisse können gemäß den lokalen Vorgaben benannt werden. Sie sollten Namen verwenden, die die Verzeichnisse mit der Serverinstanz verknüpfen, um die Identifikation zu erleichtern.

Beispiel für das Archivprotokoll:

-  Linux-Betriebssysteme/tsminst1\_archlog

## Linux: Installationsverzeichnisse

---

Zu den Installationsverzeichnissen für den IBM Spectrum Protect-Server gehören die Verzeichnisse für den Server, DB2, die Einheiten, die Sprache und andere Verzeichnisse. Jedes Verzeichnis enthält mehrere zusätzliche Verzeichnisse.

Das Verzeichnis `/opt/tivoli/tsm/server/bin` ist das Standardverzeichnis, das den Servercode und die Lizenzierung enthält.

Das während der Installation des IBM Spectrum Protect-Servers installierte DB2-Produkt hat die in den DB2-Informationsquellen dokumentierte Verzeichnisstruktur. Schützen Sie diese Verzeichnisse und Dateien wie die Serververzeichnisse. Das Standardverzeichnis heißt `/opt/tivoli/tsm/db2`.

Sie können folgende Sprachen verwenden: Englisch (US), Deutsch, Französisch, Italienisch, Spanisch, Portugiesisch (Brasilien), Koreanisch, Japanisch, traditionelles Chinesisch, vereinfachtes Chinesisch, Chinesisch GBK, Chinesisch Big5 und Russisch.

## Linux: Serverkomponenten installieren

---


Für die Installation der Serverkomponenten der Version 8.1.3 können Sie den Installationsassistenten, die Befehlszeile im Konsolenmodus oder den unbeaufsichtigten Modus verwenden.

### Informationen zu diesem Vorgang

---

Mithilfe der IBM Spectrum Protect-Installationssoftware können Sie die folgenden Komponenten installieren:

- Server  
Tipp: Die Datenbank (DB2), Global Security Kit (GSKit) und IBM® Java™ Runtime Environment (JRE) werden automatisch installiert, wenn Sie die Serverkomponente auswählen.
- Sprachen des Servers
- Lizenz
- Einheiten
- IBM Spectrum Protect for SAN
- Operations Center

 Linux-Betriebssysteme Für die Installation eines Servers der Version 8.1.3 anhand dieses Leitfadens müssen Sie 30 - 45 Minuten einplanen.

- Linux: Installationspaket abrufen  
Das Installationspaket für IBM Spectrum Protect kann von einer IBM Download-Site heruntergeladen werden, z. B. von Passport Advantage oder IBM Fix Central.
- Linux: IBM Spectrum Protect mit dem Installationsassistenten installieren  
Sie können den Server mit dem grafisch orientierten Assistenten von IBM Installation Manager installieren.
- Linux: IBM Spectrum Protect im Konsolenmodus installieren  
Sie können IBM Spectrum Protect mithilfe der Befehlszeile im Konsolenmodus installieren.
- Linux: IBM Spectrum Protect im unbeaufsichtigten Modus installieren  
Sie können den Server im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlernachrichten in Protokolldateien gespeichert.
- Linux: Serversprachenpakete installieren  
Übersetzungen für den Server ermöglichen das Anzeigen von Nachrichten und Hilfetext auf dem Server in verschiedenen

Sprachen. Die Übersetzungen gestatten auch die Verwendung länderspezifischer Einstellungen für das Datums-, Uhrzeit- und Zahlenformat.

## Linux: Installationspaket abrufen

---

Das Installationspaket für IBM Spectrum Protect kann von einer IBM® Download-Site heruntergeladen werden, z. B. von Passport Advantage oder IBM Fix Central.

 Linux-Betriebssysteme

### Vorbereitende Schritte

---

Wenn Sie die Dateien herunterladen wollen, legen Sie als Systembenutzergrenzwert für die maximale Dateigröße 'unlimited' (unbegrenzt) fest, um sicherzustellen, dass die Dateien ordnungsgemäß heruntergeladen werden können:

1. Geben Sie den folgenden Befehl aus, um den Wert für die maximale Dateigröße abzufragen:

```
ulimit -Hf
```

2. Wenn als Systembenutzergrenzwert für die maximale Dateigröße nicht 'unlimited' (unbegrenzt) angegeben ist, geben Sie 'unlimited' gemäß den Anweisungen in der Dokumentation Ihres Betriebssystems an.

### Vorgehensweise

---

1. Laden Sie die entsprechende Paketdatei von einer der folgenden Websites herunter:
  - Laden Sie das Serverpaket aus Passport Advantage oder Fix Central herunter.
  - Die neuesten Informationen, Aktualisierungen und Fixes finden Sie im IBM Support Portal.
2. Gehen Sie wie folgt vor, wenn Sie das Paket von einer IBM Download-Site heruntergeladen haben:

 Linux-Betriebssysteme

- a. Überprüfen Sie, ob genug Speicherbereich zum Speichern der Installationsdateien nach dem Extrahieren aus dem Produktpaket vorhanden ist. Informationen zum Speicherplatzbedarf finden Sie im Downloaddokument:
  - IBM Spectrum Protect Technote 4042944
  - IBM Spectrum Protect Extended Edition Technote 4042945
  - IBM Spectrum Protect for Data Retention Technote 4042946
- b. Laden Sie die Paketdatei in ein beliebiges Verzeichnis herunter. Der Pfad darf maximal 128 Zeichen enthalten. Sie müssen die Installationsdateien in ein leeres Verzeichnis extrahieren. Verwenden Sie kein Verzeichnis, das bereits extrahierte Dateien oder andere Dateien enthält.
- c. Stellen Sie sicher, dass die Berechtigung zur Ausführung für das Paket definiert ist. Bei Bedarf können Sie die Dateiberechtigungen mit dem folgenden Befehl ändern:

```
chmod a+x Paketname.bin
```

- d. Geben Sie den folgenden Befehl aus, um das Paket zu extrahieren:

```
./Paketname.bin
```

*Paketname* ist der Name der heruntergeladenen Datei. Zum Beispiel:

 Linux-Betriebssysteme

```
8.1.x.000-IBM-SPSRV-Linuxx86_64.bin  
8.1.x.000-IBM-SPSRV-Linuxs390x.bin  
8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
```

3. Wählen Sie eine der folgenden Methoden für die Installation von IBM Spectrum Protect aus:
  - Linux: IBM Spectrum Protect mit dem Installationsassistenten installieren
  - Linux: IBM Spectrum Protect im Konsolenmodus installieren
  - Linux: IBM Spectrum Protect im unbeaufsichtigten Modus installieren
4. Nachdem Sie IBM Spectrum Protect installiert haben und bevor Sie IBM Spectrum Protect für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Support and downloads und legen Sie alle gültigen Fixes an.

## Linux: IBM Spectrum Protect mit dem Installationsassistenten installieren

---

Sie können den Server mit dem grafisch orientierten Assistenten von IBM® Installation Manager installieren.

### Vorbereitende Schritte


---

Führen Sie vor dem Start der Installation die folgenden Schritte aus:


- Überprüfen Sie, ob für das Betriebssystem die erforderliche Sprache definiert ist. Die Sprache des Betriebssystems ist standardmäßig die Sprache des Installationsassistenten.

## Vorgehensweise

Installieren Sie IBM Spectrum Protect mit dem folgenden Verfahren:

| Option  | Bezeichnung  |
|---|--|
| <b>Installation der Software mithilfe eines heruntergeladenen Pakets:</b> | <p>a. Wechseln Sie in das Verzeichnis, in das Sie das Paket heruntergeladen haben.</p> <p>b. Geben Sie den folgenden Befehl aus, um den Installationsassistenten zu starten:  Linux-Betriebssysteme</p> <pre>./install.sh</pre> |

## Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM Installation Manager-Verzeichnis logs gespeichert werden.  
  
Installationsprotokolldateien können Sie anzeigen, indem Sie in Installation Manager auf Datei > Protokoll anzeigen klicken. Um diese Protokolldateien zu erfassen, klicken Sie in Installation Manager auf Hilfe > Daten zur Fehleranalyse exportieren.
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.
-  Linux-Betriebssysteme Nachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.

## Linux: IBM Spectrum Protect im Konsolenmodus installieren

Sie können IBM Spectrum Protect mithilfe der Befehlszeile im Konsolenmodus installieren.



## Vorbereitende Schritte

Führen Sie vor dem Start der Installation die folgenden Schritte aus:


- Überprüfen Sie, ob für das Betriebssystem die erforderliche Sprache definiert ist. Die Sprache des Betriebssystems ist standardmäßig die Sprache des Installationsassistenten.


## Vorgehensweise

Installieren Sie IBM Spectrum Protect mit dem folgenden Verfahren:

| Option  | Bezeichnung  |
|---|--|
| <b>Installation der Software mithilfe eines heruntergeladenen Pakets:</b> | <p>a. Wechseln Sie in das Verzeichnis, in das Sie das Paket heruntergeladen haben.</p> <p>b. Geben Sie den folgenden Befehl aus, um den Installationsassistenten im Konsolenmodus zu starten:  Linux-Betriebssysteme</p> <pre>./install.sh -c</pre> <p>Optional : Generieren Sie während einer Installation im Konsolenmodus eine Antwortdatei. Geben Sie die Optionen für die Installation im Konsolenmodus und in der Anzeige Zusammenfassung  an, um die Antworten zu generieren.</p> |

## Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM® Installation Manager-Verzeichnis logs gespeichert werden. Zum Beispiel:
  -  Linux-Betriebssysteme/var/ibm/InstallationManager/logs
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.

-  Linux-Betriebssysteme Nachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.

## Linux: IBM Spectrum Protect im unbeaufsichtigten Modus installieren

---

Sie können den Server im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlermeldungen in Protokolldateien gespeichert.

### Vorbereitende Schritte

---

Für die Dateneingabe bei Verwendung der unbeaufsichtigten Installation können Sie eine Antwortdatei verwenden. Die folgenden Musterantwortdateien stehen im Verzeichnis `input` zur Verfügung, in dem das Installationspaket extrahiert wird:

`install_response_sample.xml`

Verwenden Sie diese Datei für die Installation der IBM Spectrum Protect-Komponenten.

`update_response_sample.xml`

Verwenden Sie diese Datei für das Upgrade der IBM Spectrum Protect-Komponenten.

Diese Dateien enthalten Standardwerte, die dazu beitragen können, unnötige Warnungen zu vermeiden. Befolgen Sie die in den Dateien enthaltenen Anweisungen zur Verwendung dieser Dateien.

Wenn Sie eine Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

### Vorgehensweise


---

1. Erstellen Sie eine Antwortdatei. Sie können die Musterantwortdatei ändern oder eine eigene Datei erstellen.
2. Wenn Sie den Server und das Operations Center im unbeaufsichtigten Modus installieren, erstellen Sie in der Antwortdatei ein Kennwort für den Truststore des Operations Center.  
Wenn Sie die Datei `install_response_sample.xml` verwenden, fügen Sie das Kennwort in die folgende Zeile der Datei ein. Hierbei ist `mein_Kennwort` das Kennwort:

```
<variable name='ssl.password' value='mein_Kennwort' />
```

Weitere Informationen zu diesem Kennwort finden Sie in Prüfliste für die Installation.



Tipp: Das Truststore-Kennwort ist nicht erforderlich, wenn Sie das Operations Center mit der Datei `update_response_sample.xml` aktualisieren.

3. Geben Sie den folgenden Befehl in dem Verzeichnis, in dem das Installationspaket extrahiert wurde, aus, um die unbeaufsichtigte Installation zu starten. Der Wert *Antwortdatei* gibt den Pfad und den Namen der Antwortdatei an.
  -  Linux-Betriebssysteme

```
./install.sh -s -input Antwortdatei -acceptLicense
```

### Nächste Schritte

---

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM® Installation Manager-Verzeichnis `logs` gespeichert werden. Zum Beispiel:
  -  Linux-Betriebssysteme/`var/ibm/InstallationManager/logs`
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.
-  Linux-Betriebssysteme Nachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.

 Linux-Betriebssysteme

## Linux: Serversprachenpakete installieren

---

Übersetzungen für den Server ermöglichen das Anzeigen von Nachrichten und Hilfetext auf dem Server in verschiedenen Sprachen. Die Übersetzungen gestatten auch die Verwendung länderspezifischer Einstellungen für das Datums-, Uhrzeit- und Zahlenformat.

### Vorbereitende Schritte


---


Anweisungen zur Installation von von Sprachenpaketen für Speicheragenten finden Sie unter `Language pack configuration for Storage Agent`.

- Linux: Spracheinstellungen für den Server  
Verwenden Sie zum Anzeigen von Servernachrichten und Hilfetext entweder das Standardsprachenpaket oder wählen Sie ein anderes Sprachenpaket aus.
- Linux: Sprachenpaket konfigurieren  
Nach der Konfiguration eines Sprachenpakets werden Nachrichten und Hilfetext auf dem Server in der Sprache dieses Sprachenpakets und nicht in Englisch (US) angezeigt. Installationspakete werden mit IBM Spectrum Protect zur Verfügung gestellt.
- Linux: Sprachenpaket aktualisieren  
Sie können ein Sprachenpaket mithilfe von IBM® Installation Manager ändern oder aktualisieren.

## Linux: Spracheinstellungen für den Server

Verwenden Sie zum Anzeigen von Servernachrichten und Hilfetext entweder das Standardsprachenpaket oder wählen Sie ein anderes Sprachenpaket aus.

 Dieses Sprachenpaket wird automatisch für die folgende Standardsprachenoption für IBM Spectrum Protect-Servernachrichten und -Hilfetext installiert:

-  LANGUAGE en\_US


Für vom Standard abweichende Sprachen oder Ländereinstellungen installieren Sie das für Ihre Installation erforderliche Sprachenpaket.

Sie können die aufgeführten Sprachen verwenden:



Tabelle 1. Serversprachen für Linux

| Sprache                        | Wert der Option LANGUAGE |
|--------------------------------|--------------------------|
| Chinesisch, vereinfacht        | zh_CN                    |
|                                | zh_CN.gb18030            |
|                                | zh_CN.utf8               |
| Chinesisch, traditionell       | Big5 / Zh_TW             |
|                                | zh_TW                    |
|                                | zh_TW.utf8               |
| Englisch, Vereinigte Staaten   | en_US                    |
|                                | en_US.utf8               |
| Französisch                    | fr_FR                    |
|                                | fr_FR.utf8               |
| Deutsch                        | de_DE                    |
|                                | de_DE.utf8               |
| Italienisch                    | it_IT                    |
|                                | it_IT.utf8               |
| Japanisch                      | ja_JP                    |
|                                | ja_JP.utf8               |
| Koreanisch                     | ko_KR                    |
|                                | ko_KR.utf8               |
| Portugiesisch, Brasilianisches | pt_BR                    |
|                                | pt_BR.utf8               |
| Russisch                       | ru_RU                    |
|                                | ru_RU.utf8               |
| Spanisch                       | es_ES                    |
|                                | es_ES.utf8               |

 Einschränkung: Bei Verwendung des Operations Center werden einige Zeichen möglicherweise nicht ordnungsgemäß angezeigt, wenn der Web-Browsers und der Server nicht dieselbe Sprache verwenden. Wenn dieses Problem auftritt,



geben Sie im Browser dieselbe Sprache wie im Server an.


## Linux: Sprachenpaket konfigurieren



---

Nach der Konfiguration eines Sprachenpakets werden Nachrichten und Hilfetext auf dem Server in der Sprache dieses Sprachenpakets und nicht in Englisch (US) angezeigt. Installationspakete werden mit IBM Spectrum Protect zur Verfügung gestellt.

### Informationen zu diesem Vorgang

---

 Führen Sie eine der folgenden Tasks aus, um die Unterstützung für eine bestimmte Ländereinstellung zu aktivieren:

- Geben Sie in der Option LANGUAGE in der Serveroptionsdatei den Namen der Ländereinstellung an, die verwendet werden soll.  
Beispiel:
  -  Soll die Ländereinstellung `it_IT` verwendet werden, setzen Sie die Option LANGUAGE auf `it_IT`. Siehe Linux: Spracheinstellungen für den Server.
-  Wenn Sie den Server im Vordergrund starten, definieren Sie die Umgebungsvariable `LC_ALL` gemäß dem in der Serveroptionsdatei definierten Wert. Soll beispielsweise die Umgebungsvariable für Italienisch definiert werden, geben Sie folgenden Wert ein:

```
export LC_ALL=it_IT
```

Wenn die Ländereinstellung erfolgreich initialisiert wird, steuert sie die Datums-, Uhrzeit- und Zahlenformatierung für den Server. Wenn die Ländereinstellung nicht erfolgreich initialisiert wird, verwendet der Server die englischen (US) Nachrichtendateien und das Datums-, Uhrzeit- und Zahlenformat der englischen (US) Ländereinstellung.

## Linux: Sprachenpaket aktualisieren

---

Sie können ein Sprachenpaket mithilfe von IBM® Installation Manager ändern oder aktualisieren.

### Informationen zu diesem Vorgang

---

Sie können ein anderes Sprachenpaket in derselben IBM Spectrum Protect-Instanz installieren.

- Verwenden Sie die Funktion Ändern von IBM Installation Manager, um ein anderes Sprachenpaket zu installieren.
- Verwenden Sie die Funktion Aktualisieren von IBM Installation Manager, um eine Aktualisierung auf neuere Versionen der Sprachenpakete durchzuführen.

Tipp: In IBM Installation Manager bedeutet *aktualisieren* das Erkennen und Installieren von Aktualisierungen und Fixes für installierte Softwarepakete. In diesem Kontext sind *Aktualisierung* und *Upgrade* gleichbedeutend.




## Linux: Die ersten Schritte nach der Installation von IBM Spectrum Protect




---

Nach der Installation von Version 8.1.3 bereiten Sie die Konfiguration vor. Bevorzugte Methode für die Konfiguration der IBM Spectrum Protect-Instanz ist die Verwendung des Konfigurationsassistenten.

### Informationen zu diesem Vorgang

---

1.  Aktualisieren Sie die Kernelparameterwerte.  
 Siehe Linux: Kernelparameter für Linux-Systeme optimieren.
2. Erstellen Sie die Verzeichnisse und die Benutzer-ID für die Serverinstanz. Siehe Linux: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen.
3. Konfigurieren Sie eine Serverinstanz. Wählen Sie eine der folgenden Optionen aus:
  - Verwenden Sie den Konfigurationsassistenten (die bevorzugte Methode). Siehe Linux: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren.
  - Konfigurieren Sie die neue Instanz manuell. Siehe Linux: Serverinstanz manuell konfigurieren. Führen Sie während einer manuellen Konfiguration die folgenden Schritte aus:
    - a. Definieren Sie Ihre Verzeichnisse und erstellen Sie die IBM Spectrum Protect-Instanz. Siehe Linux: Serverinstanz erstellen.
    - b. Erstellen Sie eine neue Serveroptionsdatei, indem Sie die Musterdatei kopieren, um die Datenübertragung zwischen dem Server und den Clients zu definieren. Siehe  Linux: Server- und Clientübertragung konfigurieren.

- c. Geben Sie den Befehl `DSMSERV FORMAT` aus, um die Datenbank zu formatieren. Siehe [Linux: Datenbank und Protokoll formatieren](#).
  - d. Konfigurieren Sie Ihr System für die Datenbanksicherung. Siehe [Linux: Datenbankmanager für die Datenbanksicherung vorbereiten](#).
4. Konfigurieren Sie Optionen, die die Ausführung der Datenbankreorganisation steuern. Siehe [Linux: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren](#).
  5. Starten Sie die Serverinstanz, falls noch nicht gestartet.
    -  [Linux: Serverinstanz starten](#).
  6. Registrieren Sie Ihre Lizenz. Siehe [Linux: Lizenzregistrierung](#).
  7. Bereiten Sie Ihr System auf Datenbanksicherungen vor. Siehe [Linux: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben](#).
  8. Überwachen Sie den Server. Siehe [Linux: Server überwachen](#).
-  [Linux: Kernelparameter für Linux-Systeme optimieren](#)  
Damit IBM Spectrum Protect und DB2 unter Linux ordnungsgemäß installiert und ausgeführt werden, müssen Sie die Kernelkonfigurationsparameter aktualisieren.
  - [Linux: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen](#)  
Erstellen Sie die Benutzer-ID für die IBM Spectrum Protect-Serverinstanz und die Verzeichnisse, die die Serverinstanz für Datenbank- und Wiederherstellungsprotokolle benötigt.
  - [Linux: IBM Spectrum Protect-Server konfigurieren](#)  
Nachdem Sie den Server installiert und für die Konfiguration vorbereitet haben, konfigurieren Sie die Serverinstanz.
  - [Linux: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren](#)  
Um Probleme bezüglich des Datenbankwachstums und der Serverleistung zu vermeiden, überwacht der Server automatisch seine Datenbanktabellen und reorganisiert diese Tabellen, wenn dies erforderlich ist. Bevor der Server für den Produktionseinsatz gestartet wird, definieren Sie Serveroptionen, mit denen gesteuert wird, wann die Reorganisation ausgeführt wird. Ist die Verwendung der Dateneduplizierung geplant, stellen Sie sicher, dass die Option für die Ausführung der Indexreorganisation aktiviert ist.
  -  [Linux: Serverinstanz starten](#)  
Sie können den Server mit der Instanzbenutzer-ID (bevorzugte Methode) oder mit der Rootbenutzer-ID starten.
  - [Linux: Server stoppen](#)  
Sie können den Server bei Bedarf stoppen, um die Steuerung an das Betriebssystem zurückzugeben. Um den Verlust von Verwaltungs- und Clientknotenverbindungen zu vermeiden, stoppen Sie den Server erst nach Beendigung oder Abbruch laufender Sitzungen.
  - [Linux: Lizenzregistrierung](#)  
Registrieren Sie alle lizenzierten IBM Spectrum Protect-Funktionen, die Sie beziehen, sofort, damit Sie nach dem Starten der Serveroperationen (z. B. Datensicherung) keine Daten verlieren.
  - [Linux: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben](#)  
Sie müssen die zu verwendende Einheitenklasse angeben, um das System für automatische oder manuelle Datenbanksicherungen vorzubereiten.
  - [Linux: Mehrere Serverinstanzen auf einem System ausführen](#)  
Sie können mehrere Serverinstanzen auf Ihrem System erstellen. Jede Serverinstanz verfügt über ein eigenes Instanzverzeichnis sowie über Datenbank- und Protokollverzeichnisse.
  - [Linux: Server überwachen](#)  
Wenn Sie den Server im Produktionsbetrieb einsetzen, überwachen Sie den von ihm verwendeten Speicherbereich, um sicherzustellen, dass die Größe des Speicherbereichs angemessen ist. Ändern Sie den Speicherbereich, falls erforderlich.

 [Linux-Betriebssysteme](#)

## Linux: Kernelparameter für Linux-Systeme optimieren



---

Damit IBM Spectrum Protect und DB2 unter Linux ordnungsgemäß installiert und ausgeführt werden, müssen Sie die Kernelkonfigurationsparameter aktualisieren.

### Informationen zu diesem Vorgang

---

Wenn Sie diese Parameter nicht aktualisieren, kann die Installation von DB2 und IBM Spectrum Protect fehlschlagen. Auch wenn die Installation erfolgreich verläuft, können Betriebsfehler auftreten, wenn Sie keine Parameterwerte definieren.

-  [Linux: Kernelparameter unter Linux aktualisieren](#)  
DB2 erhöht IPC-Kernelparameterwerte automatisch auf die bevorzugten Einstellungen (IPC = Interprocess Communication, Interprozesskommunikation).
-  [Linux: Wertvorschläge für Kernelparameter unter Linux](#)  
Stellen Sie sicher, dass die Werte für Kernelparameter ausreichen, um Betriebsfehler während der Ausführung des IBM Spectrum Protect-Servers zu verhindern.

## Linux: Kernelparameter unter Linux aktualisieren

DB2 erhöht IPC-Kernelparameterwerte automatisch auf die bevorzugten Einstellungen (IPC = Interprocess Communication, Interprozesskommunikation).

### Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um die Kernelparameter auf Linux-Servern zu aktualisieren:

### Vorgehensweise

1. Geben Sie den Befehl `ipcs -l` aus, um die Parameterwerte aufzulisten.
2. Analysieren Sie die Ergebnisse, um festzustellen, ob für Ihr System Änderungen erforderlich sind. Wenn Änderungen erforderlich sind, können Sie den Parameter in der Datei `/etc/sysctl.conf` definieren. Der Parameterwert wird beim Systemstart angewendet.

### Nächste Schritte

In Red Hat Enterprise Linux 6 (RHEL6) müssen Sie den Parameter `kernel.shmmax` in der Datei `/etc/sysctl.conf` definieren, bevor der IBM Spectrum Protect-Server beim Systemstart automatisch gestartet wird.

Ausführliche Informationen zur DB2-Datenbank für Linux finden Sie in der Produktinformation zu DB2.

## Linux: Wertvorschläge für Kernelparameter unter Linux

Stellen Sie sicher, dass die Werte für Kernelparameter ausreichen, um Betriebsfehler während der Ausführung des IBM Spectrum Protect-Servers zu verhindern.

### Informationen zu diesem Vorgang

Die folgende Tabelle enthält die Vorschläge für Kernelparametereinstellungen für die Ausführung von IBM Spectrum Protect und DB2.

| Parameter                              | Beschreibung   | Bevorzugter Wert |
|--|--|------------------|
| <code>kernel.randomize_va_space</code> | Der Parameter <code>kernel.randomize_va_space</code> konfiguriert die Verwendung von Speicher-ASLR des Kernels. Wenn Sie den Wert 0 definieren ( <code>kernel.randomize_va_space=0</code> ), wird ASLR inaktiviert. DB2-Datenserver sind für bestimmte Objekte des gemeinsam genutzten Speichers auf festgelegte Adressen angewiesen und ASLR (Address Space Layout Randomization) kann bei einigen Aktivitäten Fehler verursachen. Ausführliche Informationen zu Linux ASLR und DB2 finden Sie in <a href="http://www.ibm.com/support/docview.wss?uid=swg21365583">http://www.ibm.com/support/docview.wss?uid=swg21365583</a> . | 0                |
| <code>vm.swappiness</code>             | Der Parameter <code>vm.swappiness</code> legt fest, ob der Kernel Anwendungsspeicher aus dem physischen Arbeitsspeicher (RAM) auslagern kann. Weitere Informationen zu Kernelparametern finden Sie unter Produktinformation zu DB2.  | 0                |
| <code>vm.overcommit_memory</code>      | Der Parameter <code>vm.overcommit_memory</code> hat Einfluss auf die Größe des virtuellen Speichers, deren Zuordnung der Kernel zulassen kann. Weitere Informationen zu Kernelparametern finden Sie unter Produktinformation zu DB2.   | 0                |

## Linux: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen

Erstellen Sie die Benutzer-ID für die IBM Spectrum Protect-Serverinstanz und die Verzeichnisse, die die Serverinstanz für Datenbank- und Wiederherstellungsprotokolle benötigt.


## Vorbereitende Schritte

Lesen Sie die Informationen zur Planung des Speicherbereichs für den Server, bevor Sie diese Task ausführen. Siehe Linux: Arbeitsblätter für Planungsdetails für den Server.

## Vorgehensweise

1. Erstellen Sie die Benutzer-ID, die Eigner der Serverinstanz sein soll. Diese Benutzer-ID verwenden Sie später bei der Erstellung der Serverinstanz.

### Linux-Betriebssysteme

 Erstellen Sie eine Benutzer-ID und eine Gruppe, die Eigner der Serverinstanz sein sollen.

- a. Die folgenden Befehle können mit einer Verwaltungsbenutzer-ID ausgeführt werden, die den Benutzer und die Gruppe definieren soll. Erstellen Sie die Benutzer-ID und Gruppe im Ausgangsverzeichnis des Benutzers.  
Einschränkung: In der Benutzer-ID dürfen nur Kleinbuchstaben (a-z), Ziffern (0-9) und das Unterstrichungszeichen ( \_ ) verwendet werden. Die Benutzer-ID und der Gruppenname müssen die folgenden Regeln einhalten:
  - Die maximale Länge beträgt 8 Zeichen.
  - Die Benutzer-ID und der Gruppenname dürfen nicht mit *ibm*, *sql*, *sys* oder mit einer Ziffer beginnen.
  - Als Benutzer-ID und Gruppenname dürfen nicht *user*, *admin*, *guest*, *public*, *local* und kein reserviertes SQL-Wort verwendet werden.

Erstellen Sie beispielsweise die Benutzer-ID `tsminst1` in der Gruppe `tsmsrvrs`. Die folgenden Beispiele zeigen, wie diese Benutzer-ID und diese Gruppe mit Betriebssystembefehlen erstellt werden.


### Linux-Betriebssysteme

```
groupadd tsmsrvrs -g 1111
useradd -d /home/tsminst1 -u 2222 -g 1111 -s /bin/bash tsminst1
passwd tsminst1
```

Einschränkung: DB2 unterstützt nicht die direkte Authentifizierung von Betriebssystembenutzern durch LDAP.

- b. Melden Sie sich ab und dann bei Ihrem System an. Wechseln Sie zu dem gerade erstellten Benutzerkonto. Verwenden Sie ein interaktives Anmeldeprogramm, z. B. Telnet, damit Sie zur Eingabe des Kennworts aufgefordert werden und es ggf. ändern können.

2. Erstellen Sie die vom Server benötigten Verzeichnisse.

 Erstellen Sie leere Verzeichnisse für jeden Tabelleneintrag und stellen Sie sicher, dass die neue Benutzer-ID, die Sie gerade erstellt haben, Eigner der Verzeichnisse ist. Hängen Sie den zugeordneten Speicher in jedem der Verzeichnisse für aktive Protokolldateien, für Archivprotokolle und Datenbanken an.

| Element   | Beispielbefehle für die Verzeichniserstellung  | Ihre Verzeichnisse |
|---|--|--------------------|
| Das <i>Instanzverzeichnis</i> für den Server. Dieses Verzeichnis enthält spezielle Dateien für diese Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien). | <code>mkdir /tsminst1</code>   |                    |
| Die Datenbankverzeichnisse  | <code>mkdir /tsmdb001</code><br><code>mkdir /tsmdb002</code><br><code>mkdir /tsmdb003</code><br><code>mkdir /tsmdb004</code> |                    |
| Verzeichnis für aktive Protokolldateien   | <code>mkdir /tsmlog</code>   |                    |
| Verzeichnis für Archivprotokolle  | <code>mkdir /tsmarchlog</code>   |                    |
| Optional: Verzeichnis für den Protokollspiegel für die aktive Protokolldatei  | <code>mkdir /tsmlogmirror</code>   |                    |
| Optional: Sekundäres Verzeichnis für Archivprotokolle (Übernahmeverzeichnis für Archivprotokolle)   | <code>mkdir /tsmarchlogfailover</code>   |                    |

Wenn ein Server anfänglich mit dem Dienstprogramm DSMSERV FORMAT oder mit dem Konfigurationsassistenten erstellt wird, werden eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien zum Speichern von Datenbankinformationen erstellt, die vom Datenbankmanager verwendet werden.

3. Melden Sie die neue Benutzer-ID ab.

## Linux: IBM Spectrum Protect-Server konfigurieren

---

Nachdem Sie den Server installiert und für die Konfiguration vorbereitet haben, konfigurieren Sie die Serverinstanz.

### Informationen zu diesem Vorgang

---

Wählen Sie eine der folgenden Optionen aus, um eine IBM Spectrum Protect-Serverinstanz zu konfigurieren:

- **Linux: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren**  
Der Assistent stellt eine Möglichkeit zur Konfiguration eines Servers mit Anleitung dar. Wenn Sie die grafische Benutzerschnittstelle (GUI) verwenden, können Sie einige komplexe Konfigurationsschritte der manuellen Ausführung vermeiden. Starten Sie den Assistenten auf dem System, auf dem Sie das IBM Spectrum Protect-Serverprogramm installiert haben.
- **Linux: Serverinstanz manuell konfigurieren**  
Nach der Installation von IBM Spectrum Protect Version 8.1.3 können Sie IBM Spectrum Protect auch manuell und nicht mit dem Konfigurationsassistenten konfigurieren.

## Linux: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren

---

Der Assistent stellt eine Möglichkeit zur Konfiguration eines Servers mit Anleitung dar. Wenn Sie die grafische Benutzerschnittstelle (GUI) verwenden, können Sie einige komplexe Konfigurationsschritte der manuellen Ausführung vermeiden. Starten Sie den Assistenten auf dem System, auf dem Sie das IBM Spectrum Protect-Serverprogramm installiert haben.



### Vorbereitende Schritte

---

Bevor Sie den Konfigurationsassistenten starten, müssen Sie alle vorhergehenden Schritte zur Vorbereitung der Konfiguration ausführen. Zu diesen Schritten gehören die Installation von IBM Spectrum Protect, die Erstellung der Datenbank- und Protokollverzeichnisse und die Erstellung der Verzeichnisse und der Benutzer-ID für die Serverinstanz.

### Vorgehensweise

---

1. Stellen Sie sicher, dass folgende Anforderungen erfüllt sind:  Linux-Betriebssysteme
  - Das System, auf dem Sie IBM Spectrum Protect installiert haben, muss über den X Window System-Client verfügen. Außerdem müssen Sie einen X Window System-Server auf Ihrem Desktop ausführen.
  - Im System muss das SSH-Protokoll (Secure Shell) aktiviert sein. Stellen Sie sicher, dass für den Port der Standardwert 22 definiert ist und dass der Port nicht durch eine Firewall blockiert wird. Sie müssen die Kennwortauthentifizierung in der Datei `sshd_config` im Verzeichnis `/etc/ssh/` aktivieren. Stellen Sie außerdem sicher, dass der SSH-Dämons service über Zugriffsberechtigungen zum Herstellen einer Verbindung zum System mithilfe des Werts `localhost` verfügt.
  - Sie müssen sich mit der Benutzer-ID, die Sie für die Serverinstanz erstellt haben, mit dem SSH-Protokoll bei IBM Spectrum Protect anmelden können. Bei Verwendung des Assistenten müssen Sie diese Benutzer-ID und dieses Kennwort für den Zugriff auf dieses System angeben.
  - Starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.
2. Starten Sie die lokale Version des Assistenten:
  -  Linux-Betriebssysteme Öffnen Sie das Programm `dsmi.cfgx` im Verzeichnis `/opt/tivoli/tsm/server/bin`. Dieser Assistent kann nur als Root ausgeführt werden.


Befolgen Sie die Anweisungen zur Ausführung der Konfiguration. Der Assistent kann gestoppt und erneut gestartet werden. Der Server ist jedoch erst betriebsbereit, wenn der gesamte Konfigurationsprozess abgeschlossen ist.

## Linux: Serverinstanz manuell konfigurieren

---

Nach der Installation von IBM Spectrum Protect Version 8.1.3 können Sie IBM Spectrum Protect auch manuell und nicht mit dem Konfigurationsassistenten konfigurieren.

- **Linux: Serverinstanz erstellen**  
Erstellen Sie eine IBM Spectrum Protect-Instanz mit dem Befehl `db2icrt`.


-  Linux-Betriebssysteme Linux: Server- und Clientübertragung konfigurieren  
Eine standardmäßige Beispielserveroptionsdatei mit dem Namen `dsmerv.opt.smp` wird während der IBM Spectrum Protect-Installation im Verzeichnis `/opt/tivoli/tsm/server/bin` erstellt. Sie müssen die Datenübertragung zwischen dem Server und den Clients definieren, indem Sie eine neue Serveroptionsdatei erstellen. Hierfür kopieren Sie die Musterdatei in das Verzeichnis für die Serverinstanz.
- Linux: Datenbank und Protokoll formatieren  
Mit dem Dienstprogramm `DSMSERV FORMAT` können Sie eine Serverinstanz initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls ist keine andere Serveraktivität zulässig.
- Linux: Datenbankmanager für die Datenbanksicherung vorbereiten  
Um die Daten in der Datenbank in IBM Spectrum Protect zu sichern, müssen Sie den Datenbankmanager aktivieren und die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) konfigurieren.

## Linux: Serverinstanz erstellen

Erstellen Sie eine IBM Spectrum Protect-Instanz mit dem Befehl `db2icrt`.


### Informationen zu diesem Vorgang

Auf einer Workstation kann mindestens eine Serverinstanz vorhanden sein.


 Wichtig: Stellen Sie Folgendes sicher, bevor der Befehl `db2icrt` ausgeführt wird:

- Das Ausgangsverzeichnis für den Benutzer (`/home/tsminst1`) ist vorhanden. Ist kein Ausgangsverzeichnis vorhanden, müssen Sie es erstellen.  
Im Instanzverzeichnis sind folgende Kerndateien gespeichert, die vom IBM Spectrum Protect-Server generiert werden:
  - Serveroptionsdatei `dsmerv.opt`
  - Die Serverschlüsseldatenbankdatei `cert.kdb` und die `.arm`-Dateien (werden von Clients und anderen Servern zum Importieren der Secure Sockets Layer-Zertifikate des Servers verwendet)
  - Einheitenkonfigurationsdatei, wenn die Serveroption `DEVCONFIG` keinen vollständig qualifizierten Namen angibt
  - Protokolldatei für Datenträger, wenn die Serveroption `VOLUMEHISTORY` keinen vollständig qualifizierten Namen angibt
  - Datenträger für Speicherpools mit dem Typ `DEVTYPE=FILE`, wenn das Verzeichnis für die Einheitenklasse nicht vollständig angegeben oder nicht vollständig qualifiziert ist
  - Benutzerexits
  - Traceausgabe (wenn nicht vollständig qualifiziert)
- Eine Shellkonfigurationsdatei (z. B. `.profile`) ist im Ausgangsverzeichnis vorhanden. Die Rootbenutzer- und Instanzbenutzer-ID müssen über Schreibberechtigung für diese Datei verfügen. Weitere Informationen finden Sie in Produktinformation zu DB2. Suchen Sie dort nach den Einstellungen für Linux- und UNIX-Umgebungsvariablen.

 Linux-Betriebssysteme

1. Melden Sie sich mit der Root-ID an und erstellen Sie eine IBM Spectrum Protect-Instanz. Der Name der Instanz muss mit dem Namen des Benutzers identisch sein, der Eigner der Instanz ist. Verwenden Sie den Befehl `db2icrt` und geben Sie den Befehl in eine Zeile ein: 

```
/opt/tivoli/tsm/db2/instance/db2icrt -a server -u
Instanzname Instanzname
```

Lautet Ihre Benutzer-ID für diese Instanz z. B. `tsminst1`, verwenden Sie den folgenden Befehl, um die Instanz zu erstellen. Geben Sie den Befehl in eine einzelne Zeile ein. 

```
/opt/tivoli/tsm/db2/instance/db2icrt -a server -u
tsminst1 tsminst1
```

Hinweis: Verwenden Sie ab diesem Punkt diese neue Benutzer-ID für die Konfiguration Ihres IBM Spectrum Protect-Servers. Melden Sie sich mit der Root-ID ab und mit der neuen Instanzbenutzer-ID an.

2. Geben Sie als Standardverzeichnis für die Datenbank das Instanzverzeichnis für den Server an. Sind mehrere Server vorhanden, melden Sie sich mit der Instanz-ID des jeweiligen Servers an. Geben Sie den folgenden Befehl aus:

```
db2 update dbm cfg using dftdbpath Instanzverzeichnis
```

Lautet das Instanzverzeichnis für den Server z. B. `'tsminst1'`, ändern Sie mit dem folgenden Befehl das Standardverzeichnis für die Datenbank in `'tsminst1'`:

```
db2 update dbm cfg using dftdbpath /tsminst1
```

3. Ändern Sie den Bibliothekspfad, so dass die Version von IBM Global Security Kit (GSKit) verwendet wird, die mit dem Server installiert wird. In den folgenden Beispielen ist `server_bin_directory` ein Unterverzeichnis des Serverinstallationsverzeichnisses. Zum Beispiel `/opt/tivoli/tsm/server/bin`.


- Sie müssen die folgenden Dateien aktualisieren, um den Bibliothekspfad zu definieren, wenn DB2 oder der Server gestartet wird:

Bash- oder Korn-Shell-Beispiel:

```
Instanzbenutzer-Ausgangsverzeichnis/sqlllib/userprofile
```


C-Shell-Beispiel:

```
Instanzbenutzer-Ausgangsverzeichnis/sqlllib/usercshrc
```

- Fügen Sie den folgenden Eintrag zur Datei *Instanzbenutzer-Ausgangsverzeichnis/sqlllib/userprofile* (Bash- oder Korn-Shell) in einer einzigen Zeile hinzu:  Linux-Betriebssysteme

```
export LD_LIBRARY_PATH=server_bin_directory/  
dbbkapi:/opt/ibm/lib:/opt/ibm/lib64:/usr/lib64:$LD_LIBRARY_PATH
```

Hinweis: Der Bibliothekspfad muss folgende Einträge enthalten:

- /usr/local/ibm/gsk8\_64/lib64
  - /opt/ibm/lib
  - /opt/ibm/lib64
  - /usr/lib64
- Fügen Sie den folgenden Eintrag zur Datei *Instanzbenutzer-Ausgangsverzeichnis/sqlllib/usercshrc* (C-Shell) in einer einzigen Zeile hinzu:  Linux-Betriebssysteme

```
setenv LD_LIBRARY_PATH server_bin_directory/dbbkapi:  
/opt/ibm/lib:/opt/ibm/lib64:/usr/lib64:$LD_LIBRARY_PATH
```

4. Erstellen Sie eine neue Serveroptionsdatei. Siehe Linux: Server- und Clientübertragung konfigurieren.

 Linux-Betriebssysteme

## Linux: Server- und Clientübertragung konfigurieren

Eine standardmäßige Beispielserveroptionsdatei mit dem Namen *dmserv.opt.smp* wird während der IBM Spectrum Protect-Installation im Verzeichnis */opt/tivoli/tsm/server/bin* erstellt. Sie müssen die Datenübertragung zwischen dem Server und den Clients definieren, indem Sie eine neue Serveroptionsdatei erstellen. Hierfür kopieren Sie die Musterdatei in das Verzeichnis für die Serverinstanz.

### Informationen zu diesem Vorgang

Stellen Sie sicher, dass ein Serverinstanzverzeichnis, z. B. */tsminst1*, vorhanden ist und kopieren Sie die Musterdatei in dieses Verzeichnis. Nennen Sie die neue Datei *dmserv.opt* und editieren Sie die Optionen. Führen Sie diese Konfiguration vor der Initialisierung der Serverdatenbank aus. Jedes Beispiel bzw. jeder Standardeintrag in der Beispieloptionsdatei ist ein Kommentar in einer Zeile, die mit einem Stern (\*) beginnt. Bei Optionen muss die Groß-/Kleinschreibung nicht beachtet werden, und zwischen Schlüsselwörtern und Werten dürfen sich ein oder mehrere Leerzeichen befinden.



Für das Editieren der Optionsdatei gelten folgende Richtlinien:


- Entfernen Sie den Stern am Anfang der Zeile, um eine Option zu aktivieren.
- Beginnen Sie mit der Eingabe der Optionen in einer beliebigen Spalte.
- Geben Sie nur eine Option pro Zeile ein. Die Option muss auf einer Zeile stehen.
- Werden mehrere Einträge für ein Schlüsselwort vorgenommen, verwendet der IBM Spectrum Protect-Server den letzten Eintrag.

Wenn Sie die Serveroptionsdatei ändern, müssen Sie den Server erneut starten, damit die Änderungen wirksam werden.

Sie können mindestens eine der folgenden Übertragungsmethoden angeben:

- TCP/IP Version 4 oder Version 6
  - Shared Memory
  - Secure Sockets Layer (SSL)
- Tipp: Sie können Kennwörter im LDAP-Verzeichnisserver oder im IBM Spectrum Protect-Server authentifizieren. Im LDAP-Verzeichnisserver authentifizierte Kennwörter können erweiterte Systemsicherheit zur Verfügung stellen.

-  Linux-Betriebssysteme Linux: TCP/IP-Optionen definieren  
Wählen Sie aus dem Bereich von TCP/IP-Optionen eine Option für den IBM Spectrum Protect-Server aus oder verwenden Sie den Standardwert.
-  Linux-Betriebssysteme Linux: Shared Memory-Optionen definieren  
Sie können die Shared Memory-Übertragung zwischen Clients und Servern auf demselben System verwenden. Für die Verwendung von Shared Memory muss TCP/IP Version 4 auf dem System installiert sein.

-  Linux-Betriebssysteme Linux: Secure Sockets Layer-Optionen definieren  
Mithilfe von Secure Sockets Layer (SSL) können Sie Ihre Daten und Kennwörter besser schützen.

## Linux: TCP/IP-Optionen definieren

---

Wählen Sie aus dem Bereich von TCP/IP-Optionen eine Option für den IBM Spectrum Protect-Server aus oder verwenden Sie den Standardwert.

### Informationen zu diesem Vorgang

---

Das folgende Beispiel zeigt eine Liste der TCP/IP-Optionen, mit denen Sie Ihr System definieren können.


```
commethod      tcpip
tcpport        1500
tcpwindowsize  0
tcponodelay    yes
```

Tipp: Sie können TCP/IP Version 4 und/oder Version 6 verwenden.

#### TCPPORT

Die Adresse des Server-Ports für TCP/IP- und SSL-Kommunikation. Der Standardwert ist 1500.

#### Linux-Betriebssysteme TCPWINDOWSIZE

 Linux-Betriebssysteme Gibt die Größe des TCP/IP-Puffers an, der beim Senden oder Empfangen von Daten verwendet wird. Die in einer Sitzung verwendete Fenstergröße ist der kleinere Wert der Server- und Clientfenstergröße. Größere Fenstergrößen benötigen zusätzlichen Speicher, können jedoch die Leistung verbessern.

Sie können eine ganze Zahl von 0 bis 2048 angeben. Soll die Standardfenstergröße für das Betriebssystem verwendet werden, geben Sie 0 an.

#### TCPNODELAY

Gibt an, ob der Server kleine Nachrichten sendet oder ob TCP/IP die Nachrichten puffern soll. Das Senden kleiner Nachrichten kann den Durchsatz verbessern, erhöht jedoch die Anzahl der im Netz gesendeten Pakete. Geben Sie YES an, wenn kleine Nachrichten gesendet werden sollen, oder NO, wenn sie TCP/IP puffern soll. Der Standardwert ist YES.

#### TCPADMINPORT

Gibt die Anschlussnummer an, an der der TCP/IP-DFV-Treiber des Servers auf TCP/IP- oder SSL-fähige Kommunikationsanforderungen warten soll, die keine Clientsitzungen sind. Der Standardwert ist der Wert von TCPPORT.

#### SSLTCPPOINT

(Nur SSL) Gibt die SSL-Anschlussnummer (SSL = Secure Sockets Layer) an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen für SSL-fähige Sitzungen des Befehlszeilenclients für Sichern/Archivieren und des Verwaltungsbefehlszeilenclients wartet.

#### SSLTCPADMINPORT

(Nur SSL) Gibt die Anschlussadresse an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen für SSL-fähige Sitzungen für den Verwaltungsbefehlszeilenclient wartet.

## Linux: Shared Memory-Optionen definieren

---

Sie können die Shared Memory-Übertragung zwischen Clients und Servern auf demselben System verwenden. Für die Verwendung von Shared Memory muss TCP/IP Version 4 auf dem System installiert sein.

### Informationen zu diesem Vorgang

---


Das folgende Beispiel zeigt eine Einstellung für Shared Memory:

```
commethod      sharedmem
shmport        1510
```

In diesem Beispiel gibt SHMPORT die TCP/IP-Anschlussadresse eines Servers bei Verwendung von Shared Memory an. Verwenden Sie die Option SHMPORT, um einen anderen TCP/IP-Anschluss anzugeben. Die Standardanschlussadresse ist 1510.

COMMETHOD kann in der IBM Spectrum Protect-Serveroptionsdatei mehrfach mit einem jeweils anderen Wert verwendet werden. Die folgende Angabe ist beispielsweise möglich:


```
commethod tcpip
commethod sharedmem
```

 Linux-Betriebssysteme Bei Verwendung von Shared Memory empfangen Sie möglicherweise die folgende Nachricht vom Server:



ANR9999D shmcomm.c(1598): Thread-ID<39>  
Fehler von msgget (2), Fehlernummer = 28

Die Nachricht bedeutet, dass eine Nachrichtenwarteschlange erstellt werden muss, der Systemgrenzwert für die maximale Anzahl Nachrichtenwarteschlangen (MSGMNI) jedoch überschritten würde.

 Linux-Betriebssysteme Um die maximale Anzahl der Nachrichtenwarteschlangen (MSGMNI) auf Ihrem System zu bestimmen, geben Sie den folgenden Befehl aus:

```
cat /proc/sys/kernel/msgmni
```

Geben Sie folgenden Befehl aus, um den Wert für MSGMNI auf Ihrem System zu erhöhen:

```
sysctl -w kernel.msgmni=n
```

Dabei ist **n** die maximale Anzahl der Nachrichtenwarteschlangen, die auf dem System zulässig sein sollen.

## Linux: Secure Sockets Layer-Optionen definieren

---

Mithilfe von Secure Sockets Layer (SSL) können Sie Ihre Daten und Kennwörter besser schützen.

### Vorbereitende Schritte

---

SSL ist die Standardtechnologie für die Erstellung verschlüsselter Sitzungen zwischen Servern und Clients. SSL stellt einen sicheren Kanal für die Server- und Clientkommunikation über offene Kommunikationspfade zur Verfügung. Bei SSL wird die Identität des Servers durch Verwendung digitaler Zertifikate überprüft.

Verwenden Sie SSL für Sitzungen nur im Bedarfsfall, um eine bessere Systemleistung sicherzustellen. Sie könnten die Prozessorressourcen auf dem IBM Spectrum Protect-Server erweitern, um den erhöhten Anforderungen gerecht zu werden.

## Linux: Datenbank und Protokoll formatieren

---

Mit dem Dienstprogramm DSMSEV FORMAT können Sie eine Serverinstanz initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls ist keine andere Serveraktivität zulässig.

Nach der Konfiguration der Serverübertragung können Sie die Datenbank initialisieren. Sie müssen sich mit der Instanzbenutzer-ID anmelden. Fügen Sie die Verzeichnisse nicht in Dateisysteme ein, deren Speicherplatz nicht ausreichen könnte. Wenn bestimmte Verzeichnisse (z. B. das Archivprotokoll) nicht verfügbar oder voll werden, stoppt der Server.


Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN.

### Exitlistenhandler definieren

---

Geben Sie für jede Serverinstanz ON für die Registry-Variable DB2NOEXITLIST an. Melden Sie sich als Serverinstanzeigner beim System an und geben Sie den folgenden Befehl aus:


```
db2set -i Name_der_Serverinstanz DB2NOEXITLIST=ON
```

Beispiel:  Linux-Betriebssysteme

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```


### Serverinstanz initialisieren

---

Mit dem Dienstprogramm DSMSEV FORMAT können Sie eine Serverinstanz initialisieren. Wenn das Verzeichnis der Serverinstanz z. B. */tsminst1* lautet, geben Sie die folgenden Befehle aus:  Linux-Betriebssysteme

```
cd /tsminst1  
dsmsevr format dbdir=tsmdb001 activelogsiz=32768  
activelogdirectory=/activelog archlogdirectory=/archlog  
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```


Tipp: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zu Grunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank verringert.

 **Linux-Betriebssysteme** Tipp: Wenn DB2 nach Ausgabe des Befehls `DSMSERV FORMAT` nicht startet, müssen Sie möglicherweise die Mounption `NOSUID` des Dateisystems inaktivieren. Wird diese Option in dem Dateisystem definiert, in dem sich das Verzeichnis des DB2-Instanzeigners befindet, oder in einem beliebigen Dateisystem, in dem sich die DB2-Datenbank, aktive Protokolldateien, Archivprotokolle, Übernahmeprotokolle oder Spiegelprotokolle befinden, muss die Option inaktiviert werden, um das System starten zu können.

Nach der Inaktivierung der Option `NOSUID` hängen Sie das Dateisystem erneut an. Dann starten Sie DB2 mit dem folgenden Befehl:

```
db2start
```


#### Zugehörige Informationen:

 [DSMSERV FORMAT \(Datenbank und Protokoll formatieren\)](#)

## Linux: Datenbankmanager für die Datenbanksicherung vorbereiten


Um die Daten in der Datenbank in IBM Spectrum Protect zu sichern, müssen Sie den Datenbankmanager aktivieren und die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) konfigurieren.

### Informationen zu diesem Vorgang

 **Linux-Betriebssysteme** Ab IBM Spectrum Protect Version 7.1 ist es nicht mehr erforderlich, das API-Kennwort während einer manuellen Konfiguration des Servers zu definieren. Wenn Sie das API-Kennwort während des manuellen Konfigurationsprozesses definieren, können Datenbanksicherungsversuche fehlschlagen.

Wenn Sie den Konfigurationsassistenten verwenden, um eine IBM Spectrum Protect-Serverinstanz zu erstellen, müssen Sie diese Schritte nicht ausführen. Wenn Sie eine Instanz manuell konfigurieren, führen Sie die folgenden Schritte aus, bevor Sie den Befehl `BACKUP DB` oder `RESTORE DB` ausgeben.

**Achtung:** Wenn die Datenbank nicht verwendet werden kann, ist der gesamte IBM Spectrum Protect-Server nicht verfügbar. Wenn eine Datenbank verloren geht und nicht wiederhergestellt werden kann, kann die Wiederherstellung der von diesem Server verwalteten Daten schwierig oder unmöglich sein. Daher ist es unbedingt erforderlich, die Datenbank zu sichern.

 **Linux-Betriebssysteme** In den folgenden Befehlen müssen Sie die Beispielwerte durch Ihre tatsächlichen Werte ersetzen. In den Beispielen wird `tsminst1` für die Benutzer-ID der Serverinstanz, `/tsminst1` für das Verzeichnis der Serverinstanz und `/home/tsminst1` als Ausgangsverzeichnis der Serverinstanzbenutzer verwendet.

1. Definieren Sie die Umgebungsvariablenkonfiguration der IBM Spectrum Protect-API für die Datenbankinstanz:

- Melden Sie sich mit der Benutzer-ID `tsminst1` an.
- Wenn der Benutzer `tsminst1` angemeldet ist, stellen Sie sicher, dass die DB2-Umgebung ordnungsgemäß initialisiert wird. Die DB2-Umgebung wird durch Ausführung des Scripts `/home/tsminst1/sqllib/db2profile` initialisiert, das normalerweise automatisch über das Profil der Benutzer-ID ausgeführt wird. Stellen Sie sicher, dass die `.profile`-Datei im Ausgangsverzeichnis der Instanzbenutzer vorhanden ist, z. B. `/home/tsminst1/.profile`. Wenn `.profile` das Script `db2profile` nicht ausführt, fügen Sie folgende Zeilen hinzu:

```
if [ -f /home/tsminst1/sqllib/db2profile ]; then
    . /home/tsminst1/sqllib/db2profile
fi
```

c. Fügen Sie in der Datei `Instanzverzeichnis/sqllib/userprofile` die folgenden Zeilen hinzu:

```
DSMI_CONFIG=Serverinstanzverzeichnis/tsmdbmgr.opt
DSMI_DIR=Serververzeichnis_bin/dbbkapi
DSMI_LOG=Serverinstanzverzeichnis
export DSMI_CONFIG DSMI_DIR DSMI_LOG
```

Hierbei gilt Folgendes:

- `Instanzverzeichnis` ist das Ausgangsverzeichnis des Serverinstanzbenutzers.
- `Serverinstanzverzeichnis` ist das Serverinstanzverzeichnis.
- `Serververzeichnis_bin` ist das Serververzeichnis 'bin'. Die Standardposition ist `/opt/tivoli/tsm/server/bin`.

Fügen Sie in der Datei `Instanzverzeichnis/sqllib/usercshrc` die folgenden Zeilen hinzu:

```
setenv DSMI_CONFIG=Serverinstanzverzeichnis/tsmdbmgr.opt
setenv DSMI_DIR=Serververzeichnis_bin/dbbkapi
setenv DSMI_LOG=Serverinstanzverzeichnis
```

2. Melden Sie sich ab und als `tsminst1` erneut an oder geben Sie den folgenden Befehl aus:

```
. ~/.profile
```

Tipp: Stellen Sie sicher, dass Sie ein Leerzeichen nach dem ersten Punkt (.) eingeben.

- Erstellen Sie eine Datei mit dem Namen `tsmdbmgr.opt` im Verzeichnis *Serverinstanz*, das sich in diesem Beispiel im Verzeichnis `/tsminst1` befindet, und fügen Sie folgende Zeile hinzu:

```
SERVERNAME TSMDBMGR_TSMINST1
```


Hinweis: Der Wert für `SERVERNAME` muss in den Dateien `tsmdbmgr.opt` und `dsm.sys` konsistent sein.

- Fügen Sie als Rootbenutzer die folgenden Zeilen zur Konfigurationsdatei `dsm.sys` der IBM Spectrum Protect-API hinzu. Die Konfigurationsdatei `dsm.sys` befindet sich standardmäßig in folgendem Standardverzeichnis:
  - Serververzeichnis\_bin/dbbkapi/dsm.sys*

```
servername TSMDBMGR_TSMINST1
commmethod tcpip
tcpserveraddr localhost
tcpport 1500
errorlogname /tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

Erläuterungen:

- Servername* stimmt mit dem Wert für `servername` in der Datei `tsmdbmgr.opt` überein.
- Commmethod* gibt die Client-API an, mit der Kontakt zum Server wegen der Datenbanksicherung hergestellt wird. Gültige Werte sind `tcpip` und `sharedmem`. Weitere Informationen zu Shared Memory (gemeinsam genutzter Speicher) finden Sie in Schritt 5.
- Tcpserveraddr* gibt die Serveradresse an, mit der die Client-API Kontakt zum Server wegen der Datenbanksicherung herstellt. Um sicherzustellen, dass die Datenbank gesichert werden kann, muss dieser Wert `localhost` lauten.
- Tcpport* gibt die Anschlussnummer an, mit der die Client-API Kontakt zum Server wegen der Datenbanksicherung herstellt. Sie müssen denselben `tcpport`-Wert wie in der Serveroptionsdatei `dsmerv.opt` angeben.
- Errorlogname* gibt das Fehlerprotokoll an, in dem die Client-API Fehler protokolliert, die während einer Datenbanksicherung auftreten. Dieses Protokoll befindet sich normalerweise im Serverinstanzverzeichnis. Dieses Protokoll kann sich jedoch an jeder beliebigen Position befinden, für die die Instanzbenutzer-ID Schreibberechtigung hat.
- Nodename* gibt den Knotennamen an, mit dem die Client-API während einer Datenbanksicherung eine Verbindung zum Server herstellt. Um sicherzustellen, dass die Datenbank gesichert werden kann, muss dieser Wert `$_TSMDBMGR_` lauten.

 **Achtung:** Fügen Sie nicht die Option `PASSWORDACCESS generate` zur Konfigurationsdatei `dsm.sys` hinzu. Diese Option kann einen Datenbanksicherungsfehler verursachen.

- Optional: Konfigurieren Sie den Server für die Datenbanksicherung mithilfe von Shared Memory. Auf diese Weise könnten Sie die Prozessorauslastung verringern und den Durchsatz verbessern. Führen Sie die folgenden Schritte aus:
  - Überprüfen Sie die Datei `dsmerv.opt`. Fügen Sie die folgenden Zeilen in die Datei ein, falls nicht vorhanden:

```
commmethod sharedmem
shmport Anschlussnummer
```

Hierbei steht *Anschlussnummer* für den Anschluss, der für Shared Memory verwendet werden soll.

- Suchen Sie in der Konfigurationsdatei `dsm.sys` die folgenden Zeilen:

```
commmethod tcpip
tcpserveraddr localhost
tcpport Anschlussnummer
```

Ersetzen Sie die angegebenen Zeilen durch die folgenden Zeilen:

```
commmethod sharedmem
shmport Anschlussnummer
```

Hierbei steht *Anschlussnummer* für den Anschluss, der für Shared Memory verwendet werden soll.

## Linux: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren

---


Um Probleme bezüglich des Datenbankwachstums und der Serverleistung zu vermeiden, überwacht der Server automatisch seine Datenbanktabellen und reorganisiert diese Tabellen, wenn dies erforderlich ist. Bevor der Server für den Produktionseinsatz gestartet wird, definieren Sie Serveroptionen, mit denen gesteuert wird, wann die Reorganisation ausgeführt wird. Ist die Verwendung der Datendeduplizierung geplant, stellen Sie sicher, dass die Option für die Ausführung der Indexreorganisation aktiviert ist.

### Informationen zu diesem Vorgang

---

Die Tabellen- und Indexreorganisation erfordert in hohem Umfang Prozessorressourcen, Speicherbereich für die aktive Protokolldatei und Speicherbereich für das Archivprotokoll. Da die Datenbanksicherung Vorrang vor der Reorganisation hat, wählen Sie den Zeitpunkt

und die Dauer für die Reorganisation aus, um sicherzustellen, dass sich die Prozesse nicht überlappen und die Reorganisation ausgeführt werden kann.


 Sie können die Index- und Tabellenreorganisation für die Serverdatenbank optimieren. Auf diese Weise können Sie die Vermeidung von unerwartetem Datenbankwachstum und Leistungsproblemen verbessern. Anweisungen finden Sie in Technote 1683633.

Wenn Sie diese Serveroptionen aktualisieren, während der Server aktiv ist, müssen Sie den Server stoppen und erneut starten, damit die aktualisierten Werte wirksam werden.

## Vorgehensweise

---

### 1. Ändern Sie die Serveroptionen.

 Bearbeiten Sie die Serveroptionsdatei `dmserv.opt` im Serverinstanzverzeichnis. Beachten Sie bei der Bearbeitung der Serveroptionsdatei die folgenden Richtlinien:

- Entfernen Sie den Stern am Zeilenanfang, um eine Option zu aktivieren.
- Geben Sie eine Option in einer beliebigen Zeile ein.
- Geben Sie nur eine Option pro Zeile ein. Die vollständige Option mit ihrem Wert muss sich in einer Zeile befinden.
- Haben Sie mehrere Einträge für eine Option in der Datei, verwendet der Server den letzten Eintrag.

Die verfügbaren Serveroptionen können Sie mit der Musterdatei `dmserv.opt.smp` im Verzeichnis `/opt/tivoli/tsm/server/bin` anzeigen.

### 2. Ist die Verwendung der Datenduplizierung geplant, aktivieren Sie die Serveroption `ALLOWREORGINDEX`. Fügen Sie der Serveroptionsdatei die folgende Option und den folgenden Wert hinzu:

```
allowreorgindex yes
```

### 3. Definieren Sie die Serveroptionen `REORGBEGINTIME` und `REORGDURATION`, mit denen gesteuert wird, wann die Reorganisation gestartet und wie lange sie ausgeführt wird. Wählen Sie den Zeitpunkt und die Dauer so aus, dass die Reorganisation ausgeführt wird, wenn der Server voraussichtlich am wenigsten ausgelastet ist. Diese Serveroptionen steuern sowohl die Tabellen- als auch die Indexreorganisationsprozesse.

- a. Definieren Sie die Startzeit der Reorganisation mit der Serveroption `REORGBEGINTIME`. Geben Sie die Zeit im 24-Stunden-Format an. Um beispielsweise als Startzeit der Reorganisation 20:30 Uhr festzulegen, geben Sie die folgende Option und den folgenden Wert in der Serveroptionsdatei an:

```
reorgbegintime 20:30
```

- b. Definieren Sie das Intervall, in dem der Server die Reorganisation starten kann. Um beispielsweise anzugeben, dass der Server die Reorganisation innerhalb von 4 Stunden nach dem mit der Serveroption `REORGBEGINTIME` definierten Zeitpunkt starten kann, geben Sie die folgende Option und den folgenden Wert in der Serveroptionsdatei an:


```
reorgduration 4
```

### 4. War der Server aktiv, während Sie die Serveroptionsdatei aktualisiert haben, stoppen Sie den Server und starten Sie ihn erneut.


#### Zugehörige Informationen:

 [ALLOWREORGINDEX](#)

 [ALLOWREORGTABLE](#)

 [REORGBEGINTIME](#)

 [REORGDURATION](#)

 [Linux-Betriebssysteme](#)

## Linux: Serverinstanz starten

---

Sie können den Server mit der Instanzbenutzer-ID (bevorzugte Methode) oder mit der Rootbenutzer-ID starten.

### Vorbereitende Schritte

---

Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden.


 Anweisungen finden Sie in Zugriffsberechtigungen und Benutzergrenzwerte überprüfen.

### Informationen zu diesem Vorgang

---

Wenn Sie den Server unter Verwendung der Instanzbenutzer-ID starten, wird der Konfigurationsprozess vereinfacht und potenzielle Probleme werden vermieden. In einigen Fällen kann jedoch die Verwendung der Rootbenutzer-ID zum Starten des Servers erforderlich

sein. Beispielsweise kann die Rootbenutzer-ID verwendet werden, um sicherzustellen, dass der Server auf bestimmte Einheiten zugreifen kann. Sie können den automatischen Serverstart mit der Instanzbenutzer-ID oder mit der Rootbenutzer-ID konfigurieren.

 Linux-Betriebssysteme Wenn Sie Verwaltungs- oder Rekonfigurationstasks ausführen müssen, starten Sie den Server im Verwaltungsmodus.

## Vorgehensweise

---

Führen Sie einen der folgenden Schritte aus, um den Server zu starten:


- Starten Sie den Server mithilfe der Instanzbenutzer-ID.

 Linux-Betriebssysteme Anweisungen finden Sie in Server mit der Instanzbenutzer-ID starten.

- Starten Sie den Server mithilfe der Rootbenutzer-ID.

Anweisungen zum Berechtigen von Rootbenutzer-IDs zum Starten des Servers finden Sie in Rootbenutzer-IDs zum Starten des Servers berechtigen (Version 7.1.1). Anweisungen zum Starten des Servers mit der Rootbenutzer-ID finden Sie in Server mit der Rootbenutzer-ID starten (Version 7.1.1).

-  Linux-Betriebssysteme Starten Sie den Server automatisch.

 Linux-Betriebssysteme Anweisungen siehe Linux: Server auf Linux-Systemen automatisch starten.

-  Linux-Betriebssysteme Starten Sie den Server im Verwaltungsmodus.

Anweisungen siehe Linux: Server im Verwaltungsmodus starten.

 Linux-Betriebssysteme

## Linux: Zugriffsberechtigungen und Benutzergrenzwerte überprüfen

---

Vor dem Start des Servers überprüfen Sie Zugriffsberechtigungen und Benutzergrenzwerte.

### Informationen zu diesem Vorgang

---

Wenn Sie die Benutzergrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, nicht überprüfen, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann. Die müssen auch den systemweiten Grenzwert für die maximale Anzahl offener Dateien überprüfen. Der systemweite Grenzwert muss größer-gleich dem Benutzergrenzwert sein.

## Vorgehensweise

---

1. Überprüfen Sie, ob die Benutzer-ID der Serverinstanz über Berechtigungen zum Starten des Servers verfügt.
2. Stellen Sie für die Serverinstanz, die Sie starten wollen, sicher, dass Sie über die Berechtigung zum Lesen und Schreiben von Dateien im Serverinstanzverzeichnis verfügen. Stellen Sie sicher, dass die Datei `dsmserv.opt` im Serverinstanzverzeichnis vorhanden ist und dass die Datei Parameter für die Serverinstanz enthält.
3. Wenn der Server mit einem Bandlaufwerk, einem Datenträgerwechsler oder mit einer Einheit für austauschbare Datenträger verbunden ist und Sie den Server mit der Instanzbenutzer-ID starten wollen, erteilen Sie der Instanzbenutzer-ID Schreib-/Lesezugriff für diese Einheiten. Führen Sie einen der folgenden Schritte aus, um Berechtigungen festzulegen:
  - Bei einem für IBM Spectrum Protect dediziertem System, auf das nur der IBM Spectrum Protect-Administrator zugreifen kann, erteilen Sie globale Schreibberechtigung für die Gerätedateien der Einheiten. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

```
chmod +w /dev/rmtX
```

- Verfügt das System über mehrere Benutzer, können Sie den Zugriff einschränken, indem Sie die IBM Spectrum Protect-Instanzbenutzer-ID zum Eigner der Gerätedateien der Einheit machen. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

```
chmod u+w /dev/rmtX
```

- Sind mehrere Benutzerinstanzen auf einem System aktiv, ändern Sie den Gruppennamen (z. B. TAPEUSERS) und fügen Sie jede IBM Spectrum Protect-Instanzbenutzer-ID dieser Gruppe hinzu. Übertragen Sie dann das Eigentumsrecht der Gerätedateien der Einheiten an die Gruppe TAPEUSERS und erteilen Sie Schreibberechtigung für die Gruppe. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

```
chmod g+w /dev/rmtX
```

- Linux-Betriebssysteme Wenn Sie den IBM Spectrum Protect-Einheitentreiber und das Dienstprogramm autoconf verwenden, erteilen Sie der Instanzbenutzer-ID mithilfe der Option `-a` Schreib-/Lesezugriff.
- Linux-Betriebssysteme Um Serverfehler während der Interaktion mit DB2 zu verhindern, optimieren Sie die Kernelparameter.
 

Linux-Betriebssysteme Anweisungen zur Optimierung von Kernelparametern finden Sie in [Linux: Kernelparameter für Linux-Systeme optimieren](#).

- Überprüfen Sie die folgenden Benutzergrenzwerte anhand der Richtlinien in der Tabelle.

Tabelle 1. Benutzergrenzwerte (ulimit-Werte)

| Typ des Benutzergrenzwerts                           | Bevorzugter Wert | Befehl zum Abfragen des Werts |
|--|------------------|-------------------------------|
| Maximale Größe erstellter Kerndateien                | Unlimited        | <code>ulimit -Hc</code>       |
| Maximale Größe eines Datensegments für einen Prozess | Unlimited        | <code>ulimit -Hd</code>       |
| Maximale Dateigröße                                  | Unlimited        | <code>ulimit -Hf</code>       |
| Maximale Anzahl offener Dateien                      | 65536            | <code>ulimit -Hn</code>       |
| Maximale Prozessorzeit in Sekunden                   | Unlimited        | <code>ulimit -Ht</code>       |

Für die Änderung von Benutzergrenzwerten befolgen Sie die Anweisungen in der Dokumentation Ihres Betriebssystems.

Tipp: Wenn Sie den Server mithilfe eines Scripts automatisch starten wollen, können Sie die Benutzergrenzwerte in dem Script definieren.

- Stellen Sie sicher, dass als Benutzergrenzwert für die maximale Anzahl Benutzerprozesse (`nproc`-Einstellung) der empfohlene Mindestwert 16384 festgelegt wird.
  - Geben Sie den Befehl `ulimit -Hu` mithilfe der Instanzbenutzer-ID aus, um den aktuellen Benutzergrenzwert zu überprüfen. Zum Beispiel:

```
[user@Machine ~]$ ulimit -Hu
16384
```

- Lautet der Grenzwert für die maximale Anzahl Benutzerprozesse nicht 16384, geben Sie den Wert 16384 an.

Linux-Betriebssysteme Fügen Sie der Datei `/etc/security/limits.conf` die folgende Zeile hinzu:

```
Instanzbenutzer-ID          -          nproc          16384
```

Hierbei gibt *Instanzbenutzer-ID* die Benutzer-ID der Serverinstanz an.

Linux-Betriebssysteme Wenn der Server im Betriebssystem Red Hat Enterprise Linux 6 installiert ist, legen Sie den Benutzergrenzwert durch Bearbeitung der Datei `/etc/security/limits.d/90-nproc.conf` im Verzeichnis `/etc/security/limits.d` fest. Diese Datei überschreibt die Einstellungen in der Datei `/etc/security/limits.conf`.

Tipp: Der Standardbenutzergrenzwert für die maximale Anzahl der Benutzerprozesse hat sich bei einigen Versionen des Betriebssystems Linux geändert. Der Standardwert ist 1024. Wenn Sie diesen Wert nicht durch den empfohlenen Mindestwert 16384 ersetzen, kann es zu einem Fehler oder einer Blockierung des Servers kommen.

Linux-Betriebssysteme

## Linux: Server mit der Instanzbenutzer-ID starten

Um den Server mit der Instanzbenutzer-ID zu starten, melden Sie sich mit der Instanzbenutzer-ID an und geben Sie im Serverinstanzverzeichnis den entsprechenden Befehl ein.

### Vorbereitende Schritte

Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden. Anweisungen siehe [Linux: Zugriffsberechtigungen und Benutzergrenzwerte überprüfen](#).

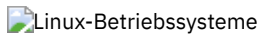
### Vorgehensweise

- Melden Sie sich bei dem System, auf dem IBM Spectrum Protect installiert ist, unter Verwendung der Instanzbenutzer-ID für den Server an.
- Wenn Sie über kein Benutzerprofil zur Ausführung des Scripts `db2profile` verfügen, geben Sie den folgenden Befehl ein:

```
./home/tsminst1/sqllib/db2profile
```

Tipp: Anweisungen zur Aktualisierung des Benutzer-ID-Anmeldescripts zur automatischen Ausführung des Scripts `db2profile` finden Sie in der DB2-Dokumentation.

- Geben Sie den folgenden Befehl in einer Zeile im Verzeichnis der Serverinstanz aus, um den Server zu starten:

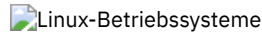


```
usr/bin/dmserv
```

Tipp: Der Befehl wird im Vordergrund ausgeführt, sodass Sie eine Administrator-ID definieren und der Serverinstanz zuordnen können.

Linux-Betriebssysteme hat beispielsweise die Serverinstanz den Namen `tsminst1` und das Serverinstanzverzeichnis den Namen `/tsminst1`, können Sie die Instanz starten, indem Sie die folgenden Befehle ausgeben:

```
cd /tsminst1
. ~/sqllib/db2profile
/usr/bin/dmserv
```



## Linux: Server auf Linux-Systemen automatisch starten

---

Um einen Server unter einem Linux-Betriebssystem automatisch zu starten, verwenden Sie das Script `dmserv.rc`.

### Vorbereitende Schritte

---

Stellen Sie sicher, dass Kernelparameter korrekt definiert werden. Anweisungen finden Sie in Kernelparameter für Linux-Systeme optimieren.

Stellen Sie sicher, dass die Serverinstanz mit der Benutzer-ID des Instanzeigners ausgeführt wird.

Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden. Anweisungen finden Sie in Zugriffsberechtigungen und Benutzergrenzwerte überprüfen.

### Informationen zu diesem Vorgang

---

Das Script `dmserv.rc` befindet sich im Serverinstallationsverzeichnis, z. B. `/opt/tivoli/tsm/server/bin`.

Das Script `dmserv.rc` kann entweder zum manuellen Starten des Servers oder zum automatischen Starten des Servers verwendet werden, indem dem Verzeichnis `/etc/rc.d/init.d` Einträge hinzugefügt werden. Das Script wird zusammen mit Linux-Dienstprogrammen wie `CHKCONFIG` und `SERVICE` eingesetzt.

### Vorgehensweise

---

Führen Sie für jede Serverinstanz, die automatisch gestartet werden soll, die folgenden Schritte aus:

1. Stellen Sie eine Kopie des Scripts `dmserv.rc` in das Verzeichnis `/init.d`, beispielsweise `/etc/rc.d/init.d`.

Achten Sie darauf, dass Änderungen nur in der Kopie des Scripts vorgenommen werden. Ändern Sie nicht das Originalscript.

2. Benennen Sie die Kopie des Scripts so um, dass sie dem Namen des Serverinstanzeigners entspricht, beispielsweise `tsminst1`.

Das Script wurde unter der Voraussetzung erstellt, dass das Serverinstanzverzeichnis `Ausgangsverzeichnis/tsminst1` ist, beispielsweise `/home/tsminst1/tsminst1`.

3. Wenn das Serverinstanzverzeichnis nicht `Ausgangsverzeichnis/tsminst1` ist, suchen Sie in der Kopie des Scripts nach der folgenden Zeile:

```
instance_dir="${Instanzausgangsverzeichnis}/tsminst1"
```

Ändern Sie die Zeile so, dass sie auf Ihr Serverinstanzverzeichnis verweist. Zum Beispiel:

```
instance_dir="/tsminst1"
```

4. Suchen Sie in der Kopie des Scripts nach der folgenden Zeile:

```
# pidfile: /var/run/dmserv_Instanzname.pid
```

Ändern Sie den Wert für den Instanznamen in den Namen des Serverinstanzeigners. Hat beispielsweise der Serverinstanzeigner den Namen `tsminst1`, aktualisieren Sie die Zeile wie folgt:

```
# pidfile: /var/run/dmserv_tsminst1.pid
```

5. Konfigurieren Sie die Ausführungsebene, auf der der Server automatisch gestartet wird. Geben Sie mithilfe von Tools wie z. B. dem Dienstprogramm `CHKCONFIG` einen Wert an, der einem Mehrbenutzermodus mit aktiviertem Netzbetrieb entspricht.

Normalerweise ist der zu verwendende Wert für die Ausführungsebene abhängig vom Betriebssystem und seiner Konfiguration 3 oder 5. Weitere Informationen zum Mehrbenutzermodus und zu Ausführungsebenen enthält die Dokumentation zu Ihrem Betriebssystem.

6. Um den Server zu starten oder zu stoppen, geben Sie einen der folgenden Befehle aus:

- Zum Starten des Servers:

```
service tsminst1 start
```

- Zum Stoppen des Servers:

```
service tsminst1 stop
```

## Beispiel



---

In diesem Beispiel werden die folgenden Werte verwendet:

- Der Instanzeigner ist `tsminst1`.
- Das Serverinstanzverzeichnis lautet `/home/tsminst1/tsminst1`.
- Die Kopie des Scripts `dsmserv.rc` hat den Namen `tsminst1`.
- Das Dienstprogramm `CHKCONFIG` wird verwendet, um das Starten des Scripts auf den Ausführungsebenen 3, 4 und 5 zu konfigurieren.

```
cp /opt/tivoli/tsm/server/bin/dsmserv.rc /etc/rc.d/init.d/tsminst1
sed -i 's/dsmserv_Instanzname.pid/dsmserv_tsminst1.pid/' /etc/rc.d/init.d/tsminst1
chkconfig --list tsminst1
service tsminst1 supports chkconfig, but is not referenced in
any runlevel (run 'chkconfig --add tsminst1')
chkconfig --add tsminst1
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:off 4:off 5:off 6:off
chkconfig --level 345 tsminst1 on
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:on 4:on 5:on 6:off
```

### Zugehörige Verweise:

-  Serverstartscript: `dsmserv.rc`
-  Linux-Betriebssysteme

## Linux: Server im Verwaltungsmodus starten

---

Sie können den Server im Verwaltungsmodus starten, um Unterbrechungen während Verwaltungs- oder Rekonfigurationstasks zu vermeiden.

### Informationen zu diesem Vorgang

---

Führen Sie das Dienstprogramm `DSMSERV` mit dem Parameter `MAINTENANCE` aus, um den Server im Verwaltungsmodus zu starten.

Die folgenden Operationen sind im Verwaltungsmodus inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Wiederherstellung von Speicherbereich auf dem Server
- Bestandsverfall
- Umlagerung von Speicherpools

Außerdem wird verhindert, dass Clients Sitzungen mit dem Server starten.

Tipps:

- Sie müssen die Serveroptionsdatei `dsmserv.opt` nicht bearbeiten, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Prozesse für die Speicherbereichwiederherstellung, den Bestandsverfall und die Speicherpoolumlagerung manuell starten.

### Vorgehensweise

---

Geben Sie den folgenden Befehl aus, um den Server im Verwaltungsmodus zu starten:

```
dsmserv maintenance
```

Tipp: Ein Video zum Starten des Servers im Verwaltungsmodus kann unter [Server im Verwaltungsmodus starten](#) angezeigt werden.



## Nächste Schritte

---

Gehen Sie wie folgt vor, um den Serverbetrieb im Produktionsmodus fortzusetzen:

1. Geben Sie den Befehl HALT aus, um den Server herunterzufahren:

```
halt
```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden.

Die während des Verwaltungsmodus inaktivierten Operationen werden wieder aktiviert.

## Linux: Server stoppen

---


Sie können den Server bei Bedarf stoppen, um die Steuerung an das Betriebssystem zurückzugeben. Um den Verlust von Verwaltungs- und Clientknotenverbindungen zu vermeiden, stoppen Sie den Server erst nach Beendigung oder Abbruch laufender Sitzungen.

### Informationen zu diesem Vorgang

---

Geben Sie den folgenden Befehl in die IBM Spectrum Protect-Befehlszeile ein, um den Server zu stoppen:


```
halt
```

 Wenn Sie keine Verbindung zum Server mit einem Verwaltungsclient herstellen können und wenn der Server gestoppt werden soll, müssen Sie den Prozess mit dem Befehl kill mit der Prozess-ID (PID) abbrechen. Die PID wird bei der Initialisierung angezeigt.

Wichtig: Bevor der Befehl kill eingegeben wird, müssen Sie sicherstellen, dass die korrekte Prozess-ID für den IBM Spectrum Protect-Server bekannt ist.

Die Prozess-ID des mit dem Befehl kill abzubrechenden Prozesses kann mithilfe der Datei `dsmserv.v6lock` in dem Verzeichnis, in dem der Server ausgeführt wird, ermittelt werden. Geben Sie Folgendes ein, um die Datei anzuzeigen:

```
cat /instance_dir/dsmserv.v6lock
```

 Geben Sie den folgenden Befehl aus, um den Server zu stoppen:

```
kill -23 dsmserv_pid
```

Hierbei steht `dsmserv_pid` für die Prozess-ID.

## Linux: Lizenzregistrierung

---

Registrieren Sie alle lizenzierten IBM Spectrum Protect-Funktionen, die Sie beziehen, sofort, damit Sie nach dem Starten der Serveroperationen (z. B. Datensicherung) keine Daten verlieren.

### Informationen zu diesem Vorgang

---

Verwenden Sie hierfür den Befehl REGISTER LICENSE. Weitere Informationen siehe REGISTER LICENSE.

### Beispiel: Lizenz registrieren

---

Die IBM Spectrum Protect-Basislizenz registrieren.

```
register license file=tsmbasic.lic
```

## Linux: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben

---

Sie müssen die zu verwendende Einheitenklasse angeben, um das System für automatische oder manuelle Datenbanksicherungen vorzubereiten.

### Vorbereitende Schritte

---

Stellen Sie sicher, dass eine Bandeneinheitenklasse oder eine Einheitenklasse FILE definiert wurde. Ausführliche Informationen finden Sie in DEFINE DEVCLASS oder suchen Sie nach 'Einheitenklasse definieren'.

### Informationen zu diesem Vorgang

---

Gehen Sie wie folgt vor, um Ihr System für Datenbanksicherungen zu konfigurieren.

## Vorgehensweise

---

1. Wenn Sie den Server nicht mit dem Konfigurationsassistenten (dsmicfgx) konfiguriert haben, müssen Sie sicherstellen, dass die Schritte zur manuellen Konfiguration des Systems für Datenbanksicherungen ausgeführt werden.
2. Wählen Sie die für Datenbanksicherungen zu verwendende Einheitenklasse aus. Geben Sie den folgenden Befehl über eine IBM Spectrum Protect-Verwaltungsbefehlszeile aus.

```
set dbrecovery Einheitenklassenname
```

Die angegebene Einheitenklasse wird vom Datenbankmanager für Datenbanksicherungen verwendet. Wenn Sie keine Einheitenklasse mit dem Befehl SET DBRECOVERY angeben, schlägt die Sicherung fehl.

## Beispiel

---

Geben Sie beispielsweise den folgenden Befehl aus, um anzugeben, dass die Einheitenklasse DBBACK verwendet werden soll:


```
set dbrecovery dbback
```

## Linux: Mehrere Serverinstanzen auf einem System ausführen

---

Sie können mehrere Serverinstanzen auf Ihrem System erstellen. Jede Serverinstanz verfügt über ein eigenes Instanzverzeichnis sowie über Datenbank- und Protokollverzeichnisse.

Multiplizieren Sie den Speicherbedarf und andere Systemvoraussetzungen für einen Server mit der geplanten Instanzzahl für das System.


 Linux-Betriebssysteme Die Gruppe der Dateien für eine Instanz des Servers wird getrennt von den Dateien gespeichert, die von einer anderen Serverinstanz auf demselben System verwendet werden. Gehen Sie wie in Linux: Serverinstanz erstellen beschrieben für jede neue Instanz vor, einschließlich der Erstellung des neuen Instanzbenutzers.

Zur Verwaltung des von jedem Server verwendeten Systemspeichers begrenzen Sie mit der Serveroption DBMEMPERCENT den Prozentsatz des Systemspeichers. Haben alle Server denselben Stellenwert, verwenden Sie für jeden Server denselben Wert. Ist ein Server ein Produktionsserver und andere Server sind Testserver, geben Sie für den Produktionsserver einen höheren Wert an als für die Testserver.

Von Version 7.1 auf Version 8.1 ist ein direktes Upgrade möglich. Weitere Informationen finden Sie im Abschnitt über das Upgrade (Upgrade auf Version 8.1 durchführen). Wenn Sie ein Upgrade durchführen und mehrere Server auf dem System haben, müssen Sie den Installationsassistenten nur einmal ausführen. Der Installationsassistent erfasst die Datenbank- und Variablendaten für alle ursprünglichen Serverinstanzen.

Wenn Sie ein Upgrade von IBM Spectrum Protect Version 6.3 auf Version 8.1.3 durchführen und sich mehrere Server auf Ihrem System befinden, werden alle in DB2 Version 9.7 vorhandenen Instanzen gelöscht und in DB2 Version 11.1 erneut erstellt. Der Assistent gibt den Befehl `db2 upgrade DB DB-Name` für jede Datenbank aus. Die Datenbankumgebungsvariablen für jede Instanz auf Ihrem System werden ebenfalls während des Upgradeprozesses neu konfiguriert.

### Zugehörige Tasks:

 Mehrere Serverinstanzen auf einem einzigen System ausführen (Version 7.1.1)

## Linux: Server überwachen

---

Wenn Sie den Server im Produktionsbetrieb einsetzen, überwachen Sie den von ihm verwendeten Speicherbereich, um sicherzustellen, dass die Größe des Speicherbereichs angemessen ist. Ändern Sie den Speicherbereich, falls erforderlich.

## Vorgehensweise

---

1. Überwachen Sie die aktive Protokolldatei, um sicherzustellen, dass die Größe für die Auslastung der Serverinstanz korrekt ist.

Wenn die Serverauslastung ihren normalen erwarteten Stand erreicht hat, belegt der von der aktiven Protokolldatei verwendete Speicherbereich 80 bis 90 Prozent des Speicherbereichs, der für das Verzeichnis für aktive Protokolldateien zur Verfügung steht. An diesem Punkt müssen Sie den Speicherbereich möglicherweise vergrößern. Die Vergrößerung des Speicherbereichs ist von der Art der Transaktionen in der Serververarbeitung abhängig. Transaktionsmerkmale wirken sich auf die Belegung des Speicherbereichs der aktiven Protokolldateien aus.

Die folgenden Transaktionsmerkmale können sich auf die Speicherbereichsbelegung in der aktiven Protokolldatei auswirken:

- Die Anzahl und Größe der Dateien in Sicherungsoperationen
  - Clients, wie z. B. Dateiserver, die zahlreiche kleine Dateien sichern, können zahlreiche Transaktionen verursachen, die in kurzer Zeit ausgeführt werden. Die Transaktionen können sehr viel Speicherbereich in der aktiven Protokolldatei belegen, jedoch nur für kurze Zeit.
  - Clients, wie z. B. E-Mail-Server oder ein Datenbankserver, die große Datenvolumen in wenigen Transaktionen sichern, können wenige Transaktionen verursachen, deren Ausführung viel Zeit in Anspruch nimmt. Die Transaktionen können wenig Speicherbereich in der aktiven Protokolldatei belegen, jedoch für lange Zeit.
- Netzwerktypen
  - Mit schnellen Netzwerkverbindungen ausgeführte Sicherungsoperationen verursachen Transaktionen, die schneller ausgeführt werden. Die Transaktionen belegen Speicherbereich in der aktiven Protokolldatei über einen kürzeren Zeitraum.
  - Mit langsameren Verbindungen ausgeführte Sicherungsoperationen verursachen Transaktionen, deren Ausführung länger dauert. Die Transaktionen belegen Speicherbereich in der aktiven Protokolldatei über einen längeren Zeitraum.

Wenn der Server Transaktionen mit sehr unterschiedlichen Merkmalen verarbeitet, kann der für die aktive Protokolldatei verwendete Speicherbereich im Lauf der Zeit sehr stark schwanken. Für einen solchen Server müssen Sie unter Umständen dafür sorgen, dass ein niedrigerer Prozentsatz des Speicherbereichs der aktiven Protokolldatei verwendet wird. Der zusätzliche Speicherbereich gestattet eine Vergrößerung der aktiven Protokolldatei für Transaktionen, die viel Zeit in Anspruch nehmen.

## 2. Überwachen Sie das Archivprotokoll, um sicherzustellen, dass immer Speicherbereich verfügbar ist.

Hinweis: Wenn das Archivprotokoll und das Übernahmearchivprotokoll voll werden, kann die aktive Protokolldatei voll werden, so dass der Server stoppt. Für das Archivprotokoll muss so viel Speicherbereich zur Verfügung stehen, dass dieser niemals vollständig belegt wird.

Sie werden wahrscheinlich Folgendes feststellen:

- a. Am Anfang wird das Archivprotokoll schnell größer, wenn normale Clientsicherungsoperationen ausgeführt werden.
- b. Datenbanksicherungen werden regelmäßig ausgeführt, entweder mit einem Zeitplan oder manuell.
- c. Nach mindestens zwei Datenbankgesamtsicherungen wird das Abschneiden des Protokolls automatisch ausgeführt. Der vom Archivprotokoll belegte Speicherbereich verringert sich durch das Abschneiden.
- d. Normale Clientoperationen werden fortgesetzt und das Archivprotokoll wird wieder größer.
- e. Datenbanksicherungen finden regelmäßig statt und die Häufigkeit der Protokollbereinigung ist von der Häufigkeit der Datenbankgesamtsicherungen abhängig.

Nach diesem Muster nimmt die Größe des Archivprotokolls zunächst zu, verringert sich und nimmt dann eventuell wieder zu. Im Laufe der Zeit sollte der vom Archivprotokoll belegte Speicherbereich während der normalen Verarbeitung einen relativ konstanten Stand erreichen.

Wenn die Größe des Archivprotokolls weiter zunimmt, sollten Sie eine oder beide der folgenden Maßnahmen in Betracht ziehen:

- Ordnen Sie dem Archivprotokoll weiteren Speicherbereich zu. Sie müssen unter Umständen das Archivprotokoll in ein anderes Dateisystem versetzen.
  - Erhöhen Sie die Häufigkeit der Datenbankgesamtsicherungen, so dass die Protokollbereinigung häufiger stattfindet.
3. Wenn Sie ein Verzeichnis für das Übernahmearchivprotokoll definiert haben, überprüfen Sie, ob darin Protokolle während der normalen Verarbeitung gespeichert werden. Wenn der Speicherbereich des Übernahmeprotokolls verwendet wird, sollten Sie das Archivprotokoll vergrößern. Das Übernahmearchivprotokoll sollte nur unter außergewöhnlichen Bedingungen verwendet werden, nicht während der normalen Verarbeitung.

## Linux: IBM Spectrum Protect-Server-Fixpack installieren

---

IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe.

### Vorbereitende Schritte

---

Damit ein Fixpack oder ein vorläufiger Fix auf dem Server installiert werden kann, müssen Sie den Server mit der Stufe installieren, auf der er ausgeführt werden soll. Sie müssen die Serverinstallation nicht mit dem Basisrelease beginnen. Wenn momentan beispielsweise Version 8.1.1 installiert ist, können Sie das aktuelle Fixpack für Version 8.1 direkt verwenden. Sie müssen nicht mit der Installation von Version 8.1.0 beginnen, wenn eine Wartungsaktualisierung verfügbar ist.

Das IBM Spectrum Protect-Lizenzpaket muss installiert sein. Das Lizenzpaket wird beim Kauf eines Basisreleases bereitgestellt. Wenn Sie ein Fixpack oder einen vorläufigen Fix von Fix Central herunterladen, installieren Sie die Serverlizenz, die auf der Website von Passport Advantage zur Verfügung steht. Sollen Nachrichten und Hilfetext nicht in Englisch angezeigt werden, installieren Sie das gewünschte Sprachenpaket.

Wenn Sie ein Upgrade des Servers auf Version 8.1.3 oder höher durchführen und den Server dann auf einen Stand vor Version 8.1.3 zurücksetzen, müssen Sie die Datenbank auf einen Zeitpunkt vor dem Upgrade zurückschreiben. Führen Sie während des Upgrades die

erforderlichen Schritte aus, mit denen sichergestellt wird, dass die Datenbank zurückgeschrieben werden kann: Sichern Sie die Datenbank, die Protokolldatei für Datenträger, die Einheitenkonfigurationsdatei und die Serveroptionsdatei. Weitere Informationen finden Sie in Linux: Von Version 8.1.3 auf eine vorherige Serverversion zurücksetzen.

Wenn Sie den Clientverwaltungsservice verwenden, müssen Sie ein Upgrade dieses Service auf dieselbe Version wie beim IBM Spectrum Protect-Server durchführen.

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease des installierten Servers aufbewahrt werden. Wenn Sie IBM Spectrum Protect über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, sind die Installationsmedien für das Basisrelease des Servers für die Neuinstallation der Lizenz erforderlich.

Rufen Sie das IBM® Support Portal auf. Hier finden Sie folgende Informationen:

- Eine Liste der neuesten Wartungs- und Download-Fixes. Klicken Sie auf **Download** und legen Sie alle gültigen Fixes an.
- Informationen zum Erwerb eines Basislizenzpakets. Suchen Sie nach **Downloads > Passport Advantage**.
- Unterstützte Plattformen und Systemvoraussetzungen. Suchen Sie nach **IBM Spectrum Protect supported operating systems**.

Sie müssen ein Upgrade des Servers durchführen, bevor Sie ein Upgrade der Clients für Sichern/Archivieren durchführen. Wenn Sie das Upgrade des Servers nicht zuerst durchführen, könnte die Kommunikation zwischen dem Server und den Clients unterbrochen werden.

Achtung: Sie dürfen die DB2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der DB2-Software und führen Sie kein Upgrade durch, da dies die Datenbank beschädigen kann.

## Vorgehensweise

---

Führen Sie die folgenden Schritte aus, um ein Fixpack oder einen vorläufigen Fix zu installieren:

1. Sichern Sie die Datenbank. Die bevorzugte Methode ist eine Momentaufnahmesicherung. Bei einer Momentaufnahmesicherung handelt es sich um eine Datenbankgesamtsicherung, bei der geplante Datenbanksicherungen nicht unterbrochen werden. Geben Sie beispielsweise den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Sichern Sie die Einheitenkonfigurationsdaten. Geben Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:



```
backup devconfig filenames=Dateiname
```

*Dateiname* gibt den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.

3. Speichern Sie die Protokolldatei für Datenträger in einem anderen Verzeichnis oder benennen Sie die Datei um. Geben Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

```
backup volhistory filenames=Dateiname
```

*Dateiname* gibt den Namen der Datei an, in der Datenträgerhistory-Informationen (Datenträgerprotokolldaten) gespeichert werden sollen.

4. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dsmserv.opt heißt. Die Datei befindet sich im Serverinstanzverzeichnis.
5. Halten Sie den Server vor der Installation eines Fixpacks oder eines vorläufigen Fixes an. Verwenden Sie den Befehl HALT.
6. Stellen Sie sicher, dass im Installationsverzeichnis zusätzlicher Speicherplatz zur Verfügung steht. Für die Installation dieses Fixpacks kann zusätzlicher temporärer Plattenspeicherplatz im Installationsverzeichnis des Servers erforderlich sein. Die Größe des zusätzlichen Plattenspeicherplatzes kann der Größe entsprechen, die für die Installation einer neuen Datenbank während einer IBM Spectrum Protect-Installation benötigt wird. Der IBM Spectrum Protect-Installationsassistent zeigt an, wie viel Speicherplatz für die Installation des Fixpacks benötigt wird und wie viel Platz zur Verfügung steht. Wenn der erforderliche Speicherplatz größer ist als der verfügbare Speicherplatz, stoppt die Installation. Wenn die Installation stoppt, fügen Sie dem Dateisystem den erforderlichen Plattenspeicherplatz hinzu und starten Sie die Installation erneut.
7.  Melden Sie sich als Root an.
8. Laden Sie die Paketdatei für das Fixpack bzw. den vorläufigen Fix, das bzw. der installiert werden soll, über IBM Support Portal, Passport Advantage oder Fix Central herunter.
9.  Wechseln Sie in das Verzeichnis, in dem sich die ausführbare Datei befindet, und führen Sie die folgenden Schritte aus.

Tipp: Die Dateien werden in das aktuelle Verzeichnis extrahiert. Stellen Sie sicher, dass sich die ausführbare Datei in dem Verzeichnis befindet, in dem sich die extrahierten Dateien befinden sollen.

- a. Geben Sie den folgenden Befehl ein, um die Dateiberechtigungen zu ändern:

```
chmod a+x 8.x.x.x-IBM-SPSRV-Plattform.bin
```

Hierbei steht *Plattform* für die Architektur, in der IBM Spectrum Protect installiert werden soll.

b. Geben Sie den folgenden Befehl aus, um die Installationsdateien zu extrahieren:

```
./8.x.x.x-IBM-SPSRV-Plattform.bin
```

10. Wählen Sie eine der folgenden Möglichkeiten für die Installation von IBM Spectrum Protect aus.

Wichtig: Nach der Installation eines Fixpacks muss die Konfiguration nicht wiederholt werden. Sie können nach Beendigung der Installation stoppen, alle Fehler beheben und dann Ihre Server erneut starten.

Installieren Sie die IBM Spectrum Protect-Software mit einer der folgenden Methoden:

Installationsassistent

Befolgen Sie die Anweisungen für Ihr Betriebssystem:

Linux: IBM Spectrum Protect mit dem Installationsassistenten installieren

Tipp: Klicken Sie nach dem Start des Assistenten im Fenster von IBM Installation Manager auf das Symbol Aktualisieren. Klicken Sie nicht auf das Symbol Installieren oder Ändern.

Befehlszeile im Konsolenmodus

Befolgen Sie die Anweisungen für Ihr Betriebssystem:

Linux: IBM Spectrum Protect im Konsolenmodus installieren

Unbeaufsichtigter Modus

Befolgen Sie die Anweisungen für Ihr Betriebssystem:

Linux: IBM Spectrum Protect im unbeaufsichtigten Modus installieren

Tipp: Befinden sich mehrere Serverinstanzen auf Ihrem System, führen Sie den Installationsassistenten nur einmal aus. Der Installationsassistent führt ein Upgrade aller Serverinstanzen durch.

## Ergebnisse

---

Beheben Sie alle Fehler, die während des Installationsprozesses festgestellt werden.

Wenn Sie den Server mithilfe des Installationsassistenten installiert haben, können Sie Installationsprotokolle mithilfe des Tools IBM Installation Manager anzeigen. Klicken Sie auf Datei > Protokoll anzeigen. Um Protokolldateien zu erfassen, klicken Sie in IBM Installation Manager auf Hilfe > Daten zur Fehleranalyse exportieren.

Wenn Sie den Server im Konsolenmodus oder im unbeaufsichtigten Modus installiert haben, können Sie Fehlerprotokolle im IBM Installation Manager-Protokollverzeichnis anzeigen. Zum Beispiel:

-  Linux-Betriebssysteme/var/ibm/InstallationManager/logs

## Linux: Von Version 8.1.3 auf eine vorherige Serverversion zurücksetzen

---

Wenn Sie nach einem Upgrade auf die vorherige Version des Servers zurücksetzen müssen, benötigen Sie eine Datenbankgesamticherung der ursprünglichen Version. Außerdem benötigen Sie die Serverinstallationsmedien für Ihre ursprüngliche Version und Schlüsselkonfigurationsdateien. Führen Sie die Schritte zur Vorbereitung sorgfältig aus, bevor Sie das Upgrade des Servers durchführen. Dadurch könnte das Zurücksetzen auf die vorherige Version des IBM Spectrum Protect-Servers mit minimalem Datenverlust möglich sein.

### Vorbereitende Schritte

---

Sie benötigen die folgenden Elemente aus der früheren Version des Servers:

- Serverdatenbanksicherung
- Protokolldatei für Datenträger
- Einheitenkonfigurationsdatei
- Serveroptionsdatei

### Informationen zu diesem Vorgang

---

Die Anweisungen sind für das Zurücksetzen innerhalb eines Releases oder von einem Release auf ein vorheriges Release identisch, z. B. von 8.1.3 auf 8.1.2 oder von 8.1.3 auf 7.1.2. Die ältere Version muss mit der Version übereinstimmen, die Sie vor dem Upgrade auf Version 8.1 verwendet haben.

Achtung: Geben Sie den Parameter REUSEDELAY an, um den Verlust von Daten des Clients für Sichern/Archivieren verhindern zu helfen, wenn Sie den Server auf eine vorherige Version zurücksetzen.


### Vorgehensweise beim Zurücksetzen auf vorherige Serverversion


---

## Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte auf dem System aus, auf dem sich der Server der Version 8.1 befindet.

### Vorgehensweise

1. Stoppen Sie den Server, um alle Serveroperationen zu beenden. Verwenden Sie hierfür den Befehl `HALT`.
2. Entfernen Sie die Datenbank aus dem Datenbankmanager und löschen Sie anschließend die Datenbank- und Wiederherstellungsprotokollverzeichnisse.
  - a. Entfernen Sie die Datenbank manuell. Eine Möglichkeit zum Entfernen ist der folgende Befehl: Linux-Betriebssysteme

```
dsmserv removedb tsmdb1
```
  - b. Wenn Sie den von den Datenbank- und Wiederherstellungsprotokollverzeichnissen belegten Speicherplatz wiederverwenden müssen, können Sie diese Verzeichnisse jetzt löschen.
3. Deinstallieren Sie den Server der Version 8.1 mit dem Deinstallationsprogramm. Bei der Deinstallation werden der Server und der Datenbankmanager mit den jeweiligen Verzeichnissen entfernt. Ausführliche Informationen siehe [Linux: IBM Spectrum Protect deinstallieren](#).
4. Stoppen Sie den Clusterdienst. Installieren Sie die Version des Serverprogramms, die Sie vor dem Upgrade auf Version 8.1.3 verwendet haben, erneut. Diese Version muss mit der Version übereinstimmen, die auf Ihrem Server verwendet wurde, als Sie die Datenbanksicherung erstellt haben, die Sie zu einem späteren Zeitpunkt wiederherstellen wollen. Wenn der Server vor dem Upgrade z. B. die Version 7.1.7 hatte und wenn Sie die Datenbanksicherung verwenden wollen, die auf diesem Server verwendet wurde, müssen Sie das Fixpack V7.1.7 installieren, damit Sie die Datenbanksicherung zurückschreiben können.
5. Konfigurieren Sie die neue Serverdatenbank mithilfe des Konfigurationsassistenten. Geben Sie den folgenden Befehl aus, um den Assistenten zu starten: Linux-Betriebssysteme

```
. /dsmicfgx
```
6. Stellen Sie sicher, dass keine Server im Hintergrund ausgeführt werden.
7. Schreiben Sie die Datenbank zu einem Zeitpunkt vor dem Upgrade zurück.
8. Kopieren Sie die folgenden Dateien in das Instanzverzeichnis.
  - o Einheitenkonfigurationsdatei
  - o Protokolldatei für Datenträger
  - o Serveroptionsdatei (normalerweise `dsmserv.opt`)
9. Wenn Sie die Datendeduplizierung für Speicherpools des Typs FILE, die vor dem Upgrade vorhanden waren, aktiviert haben oder wenn Sie während der Verwendung des Servers der Version 8.1.3 Daten, die vor dem Upgrade vorhanden waren, in neue Speicherpools verschoben haben, müssen Sie zusätzliche Schritte ausführen. Weitere Informationen finden Sie in [Zusätzliche Wiederherstellungsschritte wegen der Erstellung neuer Speicherpools oder der Aktivierung der Datendeduplizierung](#).
10. Wenn die Einstellung des Parameters `REUSEDELAY` für Speicherpools das Alter der zurückgeschriebenen Datenbank unterschreitet, schreiben Sie Datenträger auf allen Speicherpools mit sequenziellem Zugriff, die nach dieser Datenbanksicherung wiederhergestellt wurden, zurück. Verwenden Sie den Befehl `RESTORE VOLUME`. Wenn keine Sicherung eines Speicherpools vorliegt, prüfen Sie die wiederhergestellten Datenträger mit dem Befehl `AUDIT VOLUME` und dem Parameter `FIX=YES`, um Inkonsistenzen zu beheben. Beispiel:

```
audit volume Datenträgername fix=yes
```
11. Wurden mit dem Server der Version 8.1 Clientsicherungs- oder -archivierungsoperationen ausgeführt, prüfen Sie die Speicherpooldatenträger, auf denen die Daten gespeichert wurden.

## Zusätzliche Wiederherstellungsschritte wegen der Erstellung neuer Speicherpools oder der Aktivierung der Datendeduplizierung

---

Wenn Sie während der Ausführung des Servers mit Version 8.1.3 neue Speicherpools erstellt und/oder die Datendeduplizierung für Speicherpools des Typs FILE aktiviert haben, müssen Sie zusätzliche Schritte ausführen, um die vorherige Serverversion wiederherzustellen.

### Vorbereitende Schritte

Für diese Task benötigen Sie eine Gesamtsicherung des Speicherpools, die vor dem Upgrade auf Version 8.1.3 erstellt wurde.

## Informationen zu diesem Vorgang

Verwenden Sie diese Informationen, wenn Sie einen oder beide der folgenden Schritte ausgeführt haben, während Ihr Server mit Version 8.1.3 ausgeführt wurde:

- Sie haben die Datendeduplizierungsfunktion für beliebige Speicherpools aktiviert, die vor dem Upgrade auf Version 8.1.3 bereits vorhanden waren. Die Datendeduplizierung ist nur für Speicherpools gültig, die den Einheitentyp FILE verwenden.

- Sie haben neue primäre Speicherpools nach dem Upgrade erstellt *und* Daten, die in anderen Speicherpools gespeichert waren, in die neuen Speicherpools versetzt.

Führen Sie diese Schritte aus, nachdem der Server wieder auf Version 7 zurückgesetzt wurde.

## Vorgehensweise

- Schreiben Sie für jeden Speicherpool, für den Sie die Datendeduplizierungsfunktion aktiviert haben, den gesamten Speicherpool mit dem Befehl RESTORE STGPPOOL zurück.
- Bestimmen Sie für Speicherpools, die Sie nach dem Upgrade erstellt haben, welche Maßnahme durchzuführen ist. Daten, die aus vorhandenen Speicherpools der Version 8 in die neuen Speicherpools versetzt wurden, gehen möglicherweise verloren, weil die neuen Speicherpools auf Ihrem auf Version 8 zurückgesetzten Server nicht mehr vorhanden sind. Die Wiederherstellungsmaßnahmen sind vom Typ des Speicherpools abhängig:
  - Wurden Daten aus Speicherpools des Typs DISK der Version 8 in einen neuen Speicherpool versetzt, wurde der von den versetzten Daten belegte Speicherplatz wahrscheinlich wiederverwendet. Daher müssen Sie die ursprünglichen Speicherpools der Version 8 mithilfe der Speicherpoolsicherungen zurückschreiben, die vor dem Upgrade auf Version 8.1.3 erstellt wurden.

Wurden *keine* Daten aus Speicherpools des Typs DISK der Version 8 in einen neuen Speicherpool versetzt, müssen Sie die Speicherpooldatenträger in diesen Speicherpools des Typs DISK prüfen.

  - Wurden Daten aus Speicherpools mit sequenziellem Zugriff der Version 8 in einen neuen Speicherpool versetzt, sind diese Daten möglicherweise noch vorhanden und sie können eventuell auf Speicherpooldatenträgern auf dem wiederhergestellten Server der Version 8 verwendet werden. Die Daten können verwendbar sein, wenn für den Parameter REUSEDELAY des Speicherpools ein Wert definiert wurde, der die Wiederherstellung verhindert hat, während der Server mit der Version 8.1.3 ausgeführt wurde. Wurden Datenträger wiederhergestellt, während der Server mit der Version 8.1.3 ausgeführt wurde, müssen Sie diese Datenträger aus Speicherpoolsicherungen zurückschreiben, die vor dem Upgrade auf Version 8.1.3 erstellt wurden.

## Linux: Referenz: DB2-Befehle für IBM Spectrum Protect-Serverdatenbanken


Verwenden Sie diese Liste als Referenz, wenn der IBM® Support Sie anweist, DB2-Befehle auszugeben.

### Zweck

Nach der Installation und Konfiguration von IBM Spectrum Protect mithilfe der Assistenten müssen Sie DB2-Befehle nur selten verwenden. Eine begrenzte Gruppe von DB2-Befehlen, die Sie verwenden bzw. zu deren Verwendung Sie aufgefordert werden könnten, ist in Tabelle 1 aufgelistet. Diese Liste ist nicht umfassend, es handelt sich lediglich um ergänzende Informationen. Es besteht keine Implikation, dass ein IBM Spectrum Protect-Administrator sie täglich oder regelmäßig verwendet. Beispiele einiger Befehle sind angegeben. Ausgabedaten sind nicht enthalten.

Vollständige Erläuterungen zu den hier beschriebenen Befehlen und zu deren Syntax finden Sie in der Produktinformation zu DB2.

Tabelle 1. DB2-Befehle

| Befehl      | Beschreibung  | Beispiel  |
|-------------|---|---|
| db2i<br>crt | <p>Erstellt DB2-Instanzen im Ausgangsverzeichnis des Instanzeigners.</p> <p>Tipp: Der IBM Spectrum Protect-Konfigurationsassistent erstellt die vom Server und von der Datenbank verwendete Instanz. Nach der Installation und Konfiguration eines Servers mithilfe des Konfigurationsassistenten wird der Befehl db2icrt in der Regel nicht verwendet.</p> <p> Dieses Dienstprogramm befindet sich im Verzeichnis DB2DIR/instance. Hierbei steht DB2DIR für das Installationsverzeichnis, in dem die aktuelle Version des DB2-Datenbanksystems installiert ist.</p> | <p>IBM Spectrum Protect-Instanz manuell erstellen (geben Sie den Befehl in einer einzigen Zeile ein):</p> <pre>/opt/tivoli /tsm/db2/in stance/ db2icrt -a server -u Instanznam e Instanznam e</pre> |

| Befehl                     | Beschreibung  | Beispiel   |
|----------------------------|---|--|
| db2set                     | Zeigt DB2-Variablen an.   | DB2-Variablen auflisten:<br><br>db2set   |
| CATALOG DATABASE TSMDB1    | Speichert Informationen zur Speicherposition der Datenbank im Systemdatenbankverzeichnis. Die Datenbank kann sich auf der lokalen Workstation oder auf einem fernen Datenbankpartitionsserver befinden. Der Serverkonfigurationsassistent kümmert sich um jeden Katalog, der zur Verwendung der Serverdatenbank benötigt wird. Führen Sie diesen Befehl nach der Konfiguration und Aktivierung eines Servers nur dann manuell aus, wenn es eine Änderung oder Beschädigung in der Umgebung gibt.  | Datenbank katalogisieren :<br><br>db2 catalog database tsmdb1  |
| CONNECT TO DATABASE TSMDB1 | Stellt eine Verbindung zu einer angegebenen Datenbank für Befehlszeilenschnittstellenzwecke her.  | Eine Verbindung zur IBM Spectrum Protect-Datenbank über eine DB2-Befehlszeilenschnittstelle herstellen:<br><br>db2 connect to tsmdb1   |
| GET CONFIGURATION          | Gibt die Werte einzelner Einträge in einer bestimmten Datenbankkonfigurationsdatei zurück.<br>Wichtig: Dieser Befehl und seine Parameter werden direkt von DB2 definiert und verwaltet. Sie sind an dieser Stelle für Informationszwecke aufgelistet, um zu zeigen, wie die vorhandenen Einstellungen abgerufen werden können. Eine Änderung dieser Einstellungen könnte durch IBM Support oder Service-Bulletins wie z. B. APARs oder "Technical Guidance"-Dokumente (Technotes) empfohlen werden. Ändern Sie diese Einstellungen nicht manuell. Nehmen Sie eine Änderung nur nach einer entsprechenden Anweisung von IBM und nur mithilfe von IBM Spectrum Protect-Serverbefehlen oder -Prozeduren vor. | Die Konfigurationsdaten für einen Datenbankaliasnamen anzeigen:<br><br>db2 get db cfg for tsmdb1<br><br>Informationen abrufen, um Einstellungen zu überprüfen (z. B. Datenbankkonfiguration, Protokollmodus und Pflege).<br><br>db2 get db config for tsmdb1 show detail |



| Befehl  | Beschreibung  | Beispiel  |
|---|---|---|
| GET<br>DAT<br>ABA<br>SE<br>MAN<br>AGE<br>R<br>CON<br>FIG<br>URA<br>TIO<br>N | <p>Gibt die Werte einzelner Einträge in einer bestimmten Datenbankkonfigurationsdatei zurück.</p> <p>Wichtig: Dieser Befehl und seine Parameter werden direkt von DB2 definiert und verwaltet. Sie sind an dieser Stelle für Informationszwecke aufgelistet, um zu zeigen, wie die vorhandenen Einstellungen abgerufen werden können. Eine Änderung dieser Einstellungen könnte durch IBM Support oder Service-Bulletins wie z. B. APARs oder "Technical Guidance"-Dokumente (Technotes) empfohlen werden. Ändern Sie diese Einstellungen nicht manuell. Nehmen Sie eine Änderung nur nach einer entsprechenden Anweisung von IBM und nur mithilfe von IBM Spectrum Protect-Serverbefehlen oder -Prozeduren vor.</p>  | <p>Konfigurationsdaten für den Datenbankmanager abrufen:</p> <pre>db2 get dbm cfg</pre>   |
| GET<br>HEA<br>LTH<br>SNA<br>PSH<br>OT                                       | <p>Ruft die Informationen zum Allgemeinzustand für den Datenbankmanager und seine Datenbanken ab. Die zurückgegebenen Informationen stellen eine Momentaufnahme des Status zum Zeitpunkt der Befehlsausgabe dar. IBM Spectrum Protect überwacht den Status der Datenbank mithilfe der Diagnosemomentaufnahme und anderer Mechanismen, die von DB2 bereitgestellt werden. Es kann vorkommen, dass die Diagnosemomentaufnahme oder andere DB2-Dokumentation anzeigt, dass sich ein Element bzw. eine Datenbankressource im Alertstatus befindet. In einem solchen Fall müssen entsprechende Schritte zur Behebung der Situation in Betracht gezogen werden. IBM Spectrum Protect überwacht die Bedingung und reagiert entsprechend. Nicht alle deklarierten Alerts der DB2-Datenbank haben Maßnahmen zur Folge.</p>   | <p>Einen Bericht über Anzeiger des DB2-Diagnosemonitors abrufen:</p> <pre>db2 get health snapshot for database on tsmdb1</pre>  |
| GRA<br>NT<br>(Dat<br>enb<br>ank-<br>bere<br>chti<br>gun<br>gen)             | <p>Erteilt Berechtigungen, die sich auf die gesamte Datenbank beziehen, und keine Zugriffsrechte, die sich auf bestimmte Objekte in der Datenbank beziehen.</p>   | <p>Der Benutzer-ID itmuser Zugriffsberechtigung erteilen:</p> <pre>db2 GRANT CONNECT ON DATABASE TO USER itmuser db2 GRANT CREATETAB ON DATABASE TO USER itmuser</pre>          |
| RUN<br>STA<br>TS  | <p>Aktualisiert statistische Daten zu den Merkmalen einer Tabelle und der zugeordneten Indizes oder Statistiksichten. Zu diesen Merkmalen gehören die Anzahl der Datensätze, die Anzahl der Seiten und die durchschnittliche Datensatzlänge.</p> <p>Soll eine Tabelle angezeigt werden, verwenden Sie dieses Dienstprogramm nach dem Aktualisieren oder Reorganisieren der Tabelle.</p> <p>Eine Sicht muss für die Optimierung aktiviert sein, damit ihre statistischen Daten für die Optimierung einer Abfrage verwendet werden können. Eine für die Optimierung aktivierte Sicht wird als Statistiksicht bezeichnet. Sie können eine Sicht mit der DB2-Anweisung ALTER VIEW für die Optimierung aktivieren. Verwenden Sie das Dienstprogramm RUNSTATS, wenn sich Änderungen zugrunde liegender Tabellen auf die von der Sicht zurückgegebenen Zeilen auswirken.</p> <p> Tipp: Der Server konfiguriert DB2 so, dass der Befehl RUNSTATS nach Bedarf ausgeführt wird.</p> | <p>Statistische Daten für eine einzelne Tabelle aktualisieren.</p> <pre>db2 runstats on table SCHEMA_NAME .TABLE_NAME with distributio n and sampled detailed indexes all</pre> |
| SET<br>SCH<br>EMA   | <p>Ändert den Wert des Sonderregisters CURRENT SCHEMA als Vorbereitung für die direkte Ausgabe von SQL-Befehlen über die DB2-Befehlszeilenschnittstelle.</p> <p> Tipp: Ein Sonderregister ist ein Speicherbereich, den der Datenbankmanager für einen Anwendungsprozess definiert. In diesem Bereich werden Informationen gespeichert, auf die in SQL-Anweisungen verwiesen werden kann.</p>  | <p>Das Schema für IBM Spectrum Protect festlegen:</p> <pre>db2 set schema tsmdb1</pre>  |

| Befehl              | Beschreibung   | Beispiel   |
|---------------------|--|--|
| STARTABASEMANAGER   | <p>Startet die Hintergrundprozesse der aktuellen Datenbankmanagerinstanz. Der Server startet und stoppt die Instanz und die Datenbank bei jedem Start und Stopp des Servers.</p> <p>Wichtig: Lassen Sie den Server das Starten und Stoppen der Instanz und der Datenbank steuern, sofern keine anderweitige Anweisung durch IBM Support vorliegt.</p>  | Den Datenbankmanager starten:<br><code>db2start</code>     |
| STOPDATABASEMANAGER | <p>Stoppt die aktuelle Datenbankmanagerinstanz. Der Datenbankmanager bleibt so lange aktiv, bis er explizit gestoppt wird. Dieser Befehl stoppt die Datenbankmanagerinstanz nicht, wenn Anwendungen mit Datenbanken verbunden sind. Liegen keine Datenbankverbindungen, aber Instanzverbindungen vor, erzwingt der Befehl zunächst das Stoppen der Instanzverbindungen. Dann wird der Datenbankmanager gestoppt. Dieser Befehl inaktiviert außerdem alle ausstehenden Datenbankaktivierungen, bevor der Datenbankmanager gestoppt wird.</p> <p>Dieser Befehl ist auf einem Client nicht gültig.</p> <p>Der Server startet und stoppt die Instanz und die Datenbank bei jedem Start und Stopp des Servers.</p> <p>Wichtig: Lassen Sie den Server das Starten und Stoppen der Instanz und der Datenbank steuern, sofern keine anderweitige Anweisung durch IBM Support vorliegt.</p> | Den Datenbankmanager stoppen:<br><code>db2 stop dbm</code> |

## Linux: IBM Spectrum Protect deinstallieren

Sie können IBM Spectrum Protect mit den folgenden Methoden deinstallieren. Vor dem Entfernen von IBM Spectrum Protect müssen Sie sicherstellen, dass Ihre Sicherungs- und Archivierungsdaten nicht verloren gehen.

### Vorbereitende Schritte

Führen Sie folgende Schritte aus, bevor Sie IBM Spectrum Protect deinstallieren:

- Führen Sie eine Gesamtsicherung der Datenbank aus.
- Speichern Sie eine Kopie der Datenträgerhistory- und Einheitenkonfigurationsdateien.
- Bewahren Sie die Ausgabedatenträger an einem sicheren Ort auf.

### Informationen zu diesem Vorgang

Sie können IBM Spectrum Protect mit jeder der folgenden Methoden deinstallieren: grafisch orientierter Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

- Linux: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren  
Sie können IBM Spectrum Protect mit dem Installationsassistenten von IBM® Installation Manager deinstallieren.
- Linux: IBM Spectrum Protect im Konsolenmodus deinstallieren  
Zum Deinstallieren von IBM Spectrum Protect mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.
- Linux: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren  
Zum Deinstallieren von IBM Spectrum Protect im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.
- Linux: IBM Spectrum Protect deinstallieren und erneut installieren  
Wenn Sie IBM Spectrum Protect nicht mit dem Assistenten, sondern manuell erneut installieren wollen, müssen Sie einige Maßnahmen ergreifen, um Ihre Serverinstanznamen und Datenbankverzeichnisse zu bewahren. Während einer Deinstallation werden alle bereits definierten Serverinstanzen entfernt, die Datenbankkataloge für diese Instanzen sind jedoch noch vorhanden.
- Linux: IBM Installation Manager deinstallieren  
Sie können IBM Installation Manager deinstallieren, wenn keine Produkte mehr vorhanden sind, die mit IBM Installation Manager installiert wurden.

### Nächste Schritte

Die Vorgehensweise für die Reinstallation der IBM Spectrum Protect-Komponenten finden Sie in Linux: Serverkomponenten installieren.

# Linux: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren


---

Sie können IBM Spectrum Protect mit dem Installationsassistenten von IBM® Installation Manager deinstallieren.

## Vorgehensweise

---

1. Starten Sie Installation Manager.

 In dem Verzeichnis, in dem Installation Manager installiert ist, wechseln Sie in das Unterverzeichnis eclipse (z. B. /opt/IBM/InstallationManager/eclipse) und geben Sie folgenden Befehl aus:

```
./IBMIM
```

2. Klicken Sie auf Deinstallieren.
3. Wählen Sie IBM Spectrum Protect-Server aus und klicken Sie auf Weiter.
4. Klicken Sie auf Deinstallieren.
5. Klicken Sie auf Fertigstellen.

## Linux: IBM Spectrum Protect im Konsolenmodus deinstallieren


---

Zum Deinstallieren von IBM Spectrum Protect mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.



## Vorgehensweise

---

1. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das folgende Unterverzeichnis:

-  Linux-Betriebssysteme/eclipse/tools

Beispiel:

-  Linux-Betriebssysteme/opt/IBM/InstallationManager/eclipse/tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus:
    -  Linux-Betriebssysteme./imcl -c
  3. Für die Deinstallation geben Sie 5 ein.
  4. Wählen Sie die Deinstallation aus der IBM Spectrum Protect-Paketgruppe aus.
  5. Geben Sie N für 'Next' (Weiter) ein.
  6. Wählen Sie die Deinstallation des IBM Spectrum Protect-Serverpakets aus.
  7. Geben Sie N für 'Next' (Weiter) ein.
  8. Geben Sie U für 'Uninstall' (Deinstallieren) ein.
  9. Geben Sie F für 'Finish' (Fertigstellen) ein.

## Linux: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren

---

Zum Deinstallieren von IBM Spectrum Protect im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.

## Vorbereitende Schritte

---

Sie können die Dateneingabe für eine unbeaufsichtigte Deinstallation der IBM Spectrum Protect-Serverkomponenten mithilfe einer Antwortdatei bereitstellen. IBM Spectrum Protect enthält eine Musterantwortdatei, `uninstall_response_sample.xml`, im Verzeichnis `input`, in dem das Installationspaket extrahiert wird. Diese Datei enthält Standardwerte, durch die Sie unnötige Warnungen vermeiden können.

Wenn Sie alle IBM Spectrum Protect-Komponenten deinstallieren wollen, lassen Sie die Einstellung `modify="false"` für jede Komponente in der Antwortdatei unverändert. Wenn Sie eine Komponente nicht deinstallieren wollen, geben Sie den Wert `modify="true"` an.

Wenn Sie die Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

## Vorgehensweise

---

1. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das folgende Unterverzeichnis:

- o Linux-Betriebssystemeclipse/tools

Beispiel:

- o Linux-Betriebssysteme/opt/IBM/InstallationManager/eclipse/tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus, wobei *Antwortdatei* den Pfad der Antwortdatei einschließlich des Dateinamens angibt:

Linux-Betriebssysteme

```
./imcl -input Antwortdatei -silent
```

Der folgende Befehl ist ein Beispiel:

Linux-Betriebssysteme

```
./imcl -input /tmp/input/uninstall_response.xml -silent
```

## Linux: IBM Spectrum Protect deinstallieren und erneut installieren

Wenn Sie IBM Spectrum Protect nicht mit dem Assistenten, sondern manuell erneut installieren wollen, müssen Sie einige Maßnahmen ergreifen, um Ihre Serverinstanznamen und Datenbankverzeichnisse zu bewahren. Während einer Deinstallation werden alle bereits definierten Serverinstanzen entfernt, die Datenbankkataloge für diese Instanzen sind jedoch noch vorhanden.

### Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um IBM Spectrum Protect manuell zu deinstallieren und erneut zu installieren:

1. Linux-Betriebssysteme Erstellen Sie eine Liste Ihrer aktuellen Serverinstanzen, bevor Sie mit der Deinstallation beginnen. Führen Sie den folgenden Befehl aus:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

2. Führen Sie die folgenden Befehle für jede Serverinstanz aus:

Linux-Betriebssysteme

```
db2 attach to Instanzname
db2 get dbm cfg show detail
db2 detach
```

Notieren Sie den Datenbankpfad für jede Instanz.

3. Deinstallieren Sie IBM Spectrum Protect. Siehe Linux: IBM Spectrum Protect deinstallieren.
4. Wenn Sie eine beliebige unterstützte Version von IBM Spectrum Protect deinstallieren (einschließlich Fixpack), wird eine Instanzdatei erstellt. Die Instanzdatei wird erstellt, um die Reinstallation von IBM Spectrum Protect zu erleichtern. Überprüfen Sie diese Datei und verwenden Sie die Informationen, wenn Sie bei der Reinstallation zur Eingabe der Berechtigungsnachweise der Instanz aufgefordert werden. Bei der unbeaufsichtigten Installation geben Sie diese Berechtigungsnachweise mit der Variablen `INSTANCE_CRED` an.

Sie finden die Instanzdatei an der folgenden Position:

- o Linux-Betriebssysteme/etc/tivoli/tsm/instanceList.obj

5. Installieren Sie IBM Spectrum Protect erneut. Siehe Linux: Serverkomponenten installieren.

Ist die Datei `instanceList.obj` nicht vorhanden, müssen Sie Ihre Serverinstanzen wie folgt erneut erstellen:

- a. Erstellen Sie Ihre Serverinstanzen erneut. Siehe Linux: Serverinstanz erstellen.  
Tipp: Der Installationsassistent konfiguriert die Serverinstanzen, Sie müssen jedoch überprüfen, ob sie vorhanden sind. Wenn sie nicht vorhanden sind, müssen Sie sie manuell konfigurieren.
- b. Katalogisieren Sie die Datenbank. Melden Sie sich bei jeder Serverinstanz nacheinander als Instanzbenutzer an und geben Sie folgende Befehle aus:

Linux-Betriebssysteme

```
db2 catalog database tsmdb1
db2 attach to Instanzname
db2 update dbm cfg using dftdbpath Instanzverzeichnis
db2 detach
```

- c. Linux-Betriebssysteme Überprüfen Sie, ob die Serverinstanz erfolgreich erstellt wurde. Geben Sie den folgenden Befehl aus:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

- d. Überprüfen Sie, ob IBM Spectrum Protect die Serverinstanz erkennt, indem Sie Ihre Verzeichnisse auflisten. Ihr Ausgangsverzeichnis wird angezeigt, wenn Sie es nicht geändert haben. Ihr Instanzverzeichnis wird angezeigt, wenn Sie den Konfigurationsassistenten verwendet haben. Geben Sie den folgenden Befehl aus:

```
db2 list database directory
```

Wenn Sie TS MDB1 in der Liste finden, können Sie den Server starten.

## Linux: IBM Installation Manager deinstallieren


---

Sie können IBM® Installation Manager deinstallieren, wenn keine Produkte mehr vorhanden sind, die mit IBM Installation Manager installiert wurden.

### Vorbereitende Schritte

---

Bevor Sie IBM Installation Manager deinstallieren, müssen Sie sicherstellen, dass alle mit IBM Installation Manager installierten Pakete deinstalliert sind. Schließen Sie IBM Installation Manager, bevor Sie den Deinstallationsprozess starten.

 Geben Sie den folgenden Befehl in eine Befehlszeile ein, um installierte Pakete anzuzeigen:

```
cd /opt/IBM/InstallationManager/eclipse/tools
./imcl listInstalledPackages
```

### Vorgehensweise

---

Gehen Sie wie folgt vor, um IBM Installation Manager zu deinstallieren:

 Geben Sie den folgenden Befehl in eine Befehlszeile ein, um installierte Pakete anzuzeigen:

1. Öffnen Sie eine Befehlszeile und wechseln Sie in das Verzeichnis `/var/ibm/InstallationManager/uninstall`.
2. Geben Sie den folgenden Befehl aus:

```
./uninstall
```

Einschränkung: Sie müssen mit der Benutzer-ID `root` am System angemeldet sein.

## Windows: Server installieren

---


Zur Installation des Servers gehören Planung, Installation und Erstkonfiguration.

- Windows
- Windows: Installation des Servers planen  
Installieren Sie die Server-Software auf dem Computer, der Speichereinheiten verwaltet, und die Client-Software auf jeder Workstation, die Daten an den vom IBM Spectrum Protect-Server verwalteten Speicher überträgt.
- Windows: Serverkomponenten installieren  
Für die Installation der Serverkomponenten der Version 8.1.3 können Sie den Installationsassistenten, die Befehlszeile im Konsolenmodus oder den unbeaufsichtigten Modus verwenden.
- Windows: Die ersten Schritte nach der Installation von IBM Spectrum Protect  
Nach der Installation von Version 8.1.3 bereiten Sie die Konfiguration vor. Bevorzugte Methode für die Konfiguration der IBM Spectrum Protect-Instanz ist die Verwendung des Konfigurationsassistenten.
- Windows: IBM Spectrum Protect-Server-Fixpack installieren  
IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe.
- Windows: Von Version 8.1.3 auf eine vorherige Serverversion zurücksetzen  
Wenn Sie nach einem Upgrade auf die vorherige Version des Servers zurücksetzen müssen, benötigen Sie eine Datenbankgesamticherung der ursprünglichen Version. Außerdem benötigen Sie die Serverinstallationsmedien für Ihre ursprüngliche Version und Schlüsselkonfigurationsdateien. Führen Sie die Schritte zur Vorbereitung sorgfältig aus, bevor Sie das Upgrade des Servers durchführen. Dadurch könnte das Zurücksetzen auf die vorherige Version des IBM Spectrum Protect-Servers mit minimalem Datenverlust möglich sein.
- Windows: Referenz: DB2-Befehle für IBM Spectrum Protect-Serverdatenbanken  
Verwenden Sie diese Liste als Referenz, wenn der IBM® Support Sie anweist, DB2-Befehle auszugeben.
- Windows: IBM Spectrum Protect deinstallieren  
Sie können IBM Spectrum Protect mit den folgenden Methoden deinstallieren. Vor dem Entfernen von IBM Spectrum Protect müssen Sie sicherstellen, dass Ihre Sicherungs- und Archivierungsdaten nicht verloren gehen.

## Windows: Installation des Servers planen

---

Installieren Sie die Server-Software auf dem Computer, der Speichereinheiten verwaltet, und die Client-Software auf jeder Workstation, die Daten an den vom IBM Spectrum Protect-Server verwalteten Speicher überträgt.


- **Windows: Vorausgesetzte Kenntnisse**  
Sie müssen mit Ihren Betriebssystemen, Speichereinheiten, Übertragungsprotokollen und Systemkonfigurationen vertraut sein, bevor Sie IBM Spectrum Protect installieren.
- **Windows: Planung für optimale Leistung**  
Überprüfen Sie vor der Installation des IBM Spectrum Protect-Servers die Merkmale und die Konfiguration des Systems, um sicherzustellen, dass der Server für die optimale Leistung konfiguriert ist.
-  **Windows: Systemmindestvoraussetzungen für Windows-Systeme**  
Für den Server können sehr viel Speicherplatz, eine große Netzbandbreite und viele Prozessorressourcen erforderlich sein. In vielen Fällen ist die Leistung des Servers am besten, wenn andere Anwendungen nicht auf demselben System installiert sind.
- **Windows: IBM Installation Manager**  
IBM Spectrum Protect verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositories installiert oder aktualisiert werden können.
- **Windows: Arbeitsblätter für Planungsdetails für den Server**  
Sie können die Arbeitsblätter für die Planung der Größe und der Position des für den IBM Spectrum Protect-Server benötigten Speichers verwenden. Sie können darauf auch Namen und Benutzer-IDs aufzeichnen.
- **Windows: Kapazitätsplanung**  
Zur Kapazitätsplanung für IBM Spectrum Protect gehört die Verwaltung von Ressourcen wie z. B. die Datenbank, das Wiederherstellungsprotokoll und der Bereich für gemeinsam genutzte Ressourcen. Sie müssen den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll schätzen, um die Ressourcen als Teil der Kapazitätsplanung zu maximieren. Der verfügbare Speicherplatz für den Bereich für gemeinsam genutzte Ressourcen muss für jede Installation bzw. jedes Upgrade ausreichen.
- **Windows: Empfehlungen für die Serverbenennung**  
Verwenden Sie diese Beschreibungen als Referenz bei der Installation oder beim Upgrade eines IBM Spectrum Protect-Servers.
- **Windows: Installationsverzeichnisse**  
Zu den Installationsverzeichnissen für den IBM Spectrum Protect-Server gehören die Verzeichnisse für den Server, DB2, die Einheiten, die Sprache und andere Verzeichnisse. Jedes Verzeichnis enthält mehrere zusätzliche Verzeichnisse.


## Windows: Vorausgesetzte Kenntnisse

---

Sie müssen mit Ihren Betriebssystemen, Speichereinheiten, Übertragungsprotokollen und Systemkonfigurationen vertraut sein, bevor Sie IBM Spectrum Protect installieren.

Wartungsreleases, Client-Software und Veröffentlichungen für den Server stehen im IBM® Support Portal zur Verfügung.

 **Einschränkung:** Sie können den Server der Version 8.1.3 nicht auf einem System installieren und ausführen, auf dem bereits DB2 installiert ist. Das gilt unabhängig davon, ob DB2 separat oder als Teil einer anderen Anwendung installiert wurde. Für den Server der Version 8.1.3 muss die DB2-Version installiert und verwendet werden, die im Paket des Servers der Version 8.1.3 enthalten ist. Es darf keine andere DB2-Version auf dem System vorhanden sein.

 Sie können den IBM Spectrum Protect-Server auf einem Domänencontroller installieren. Auf dem Server kann jedoch eine hohe Prozessorauslastung auftreten, wodurch andere Anwendungen betroffen sein und blockiert werden können.

Erfahrene DB2-Administratoren können erweiterte SQL-Abfragen durchführen und mithilfe von DB2-Tools die Datenbank überwachen. Sie dürfen die DB2-Tools jedoch nicht zur Änderung der von IBM Spectrum Protect vorgegebenen DB2-Konfigurationseinstellungen verwenden oder die DB2-Umgebung für IBM Spectrum Protect auf andere Weise ändern (z. B. mit anderen Produkten). Der Server der Version 8.1.3 wurde mit der Datendefinitionssprache (DDL) und der vom Server implementierten Datenbankkonfiguration erstellt und ausführlich getestet.

**Achtung:** Sie dürfen die DB2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der DB2-Software und führen Sie kein Upgrade durch, da dies die Datenbank beschädigen kann.

## Windows: Planung für optimale Leistung

---

Überprüfen Sie vor der Installation des IBM Spectrum Protect-Servers die Merkmale und die Konfiguration des Systems, um sicherzustellen, dass der Server für die optimale Leistung konfiguriert ist.

## Vorgehensweise

---

1. Lesen Sie den Abschnitt Windows: Vorausgesetzte Kenntnisse.
2. Lesen Sie jeden der folgenden Unterabschnitte.

- Windows: Planung für die Server-Hardware und das Betriebssystem  
Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
- Windows: Planung für Platten für die Serverdatenbank  
Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
- Windows: Planung für Platten für das Serverwiederherstellungsprotokoll  
Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
- Windows: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools  
Überprüfen Sie die Konfiguration Ihrer Verzeichniscontainer- und Cloud-Containerspeicherpools, um eine optimale Leistung zu gewährleisten.
- Windows: Planung für Speicherpools auf DISK- oder FILE-Einheiten  
Überprüfen Sie mithilfe der Prüfliste, wie Ihre Plattenspeicherpools konfiguriert sind. Diese Prüfliste umfasst Tipps für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden.
- Windows: Planung für die Auswahl des korrekten Speichertechnologietyps  
Speichereinheiten haben eine unterschiedliche Kapazität und unterschiedliche Leistungsmerkmale. Diese Merkmale wirken sich darauf aus, welche Einheiten besser für die Verwendung mit IBM Spectrum Protect geeignet sind.
- Windows: Bewährte Verfahren bei der Serverinstallation anwenden  
Normalerweise hat die Konfiguration und Auswahl der Hardware die deutlichsten Auswirkungen auf die Leistung einer IBM Spectrum Protect-Lösung. Weitere Faktoren, die sich auf die Leistung auswirken, sind die Auswahl und Konfiguration des Betriebssystems sowie die Konfiguration von IBM Spectrum Protect.

## Windows: Planung für die Server-Hardware und das Betriebssystem


Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen   |
|---|--|---|
| <p>Werden die Betriebssystem- und Hardwarevoraussetzungen erfüllt oder mehr als erfüllt?</p> <ul style="list-style-type: none"> <li>• Anzahl und Geschwindigkeit der Prozessoren</li> <li>• Systemspeicher</li> <li>• Unterstützte Betriebssystemversion</li> </ul> | <p>Wenn Sie die erforderliche Mindestspeicherkapazität verwenden, können Sie eine minimale Arbeitslast unterstützen.</p> <p>Sie können versuchsweise mehr Systemspeicher hinzufügen, um bestimmen zu können, ob sich die Leistung verbessert. Entscheiden Sie dann, ob der Systemspeicher dem Server zugeordnet bleiben soll. Testen Sie die verschiedenen Speicherkapazitäten jeweils anhand des gesamten Tageszyklus der Serverlast.</p> <p>Wenn Sie mehrere Server auf dem System ausführen, addieren Sie die Voraussetzungen für jeden Server, um die Voraussetzungen für das System zu bestimmen.</p> | <p>Überprüfen Sie die Betriebssystemvoraussetzungen in Technote 1243309.</p> <p>Lesen Sie außerdem die Anweisungen in Tasks für Betriebssysteme und andere Anwendungen optimieren.</p> <p>Weitere Informationen zu Voraussetzungen, wenn die entsprechenden Funktionen verwendet werden, finden Sie in den folgenden Abschnitten:</p> <ul style="list-style-type: none"> <li>• Prüfliste für Datenduplizierung</li> <li>• Prüfliste für Knotenreplikation</li> </ul> <p>Weitere Informationen zu Anforderungen in Bezug auf die Größe des Servers und des Speichers finden Sie im IBM Spectrum Protect-Blueprint.</p> |

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen   |
|--|---|---|
| Sind Platten für die optimale Leistung konfiguriert? | Der Umfang der Optimierung, der für verschiedene Plattensysteme erfolgen kann, variiert. Stellen Sie sicher, dass die Warteschlangenlänge und andere Plattensystemoptionen entsprechend definiert sind.   | <p>Weitere Informationen finden Sie in:</p> <ul style="list-style-type: none"> <li>• "Planung für Platten für die Serverdatenbank"</li> <li>• "Planung für Platten für das Serverwiederherstellungsprotokoll"</li> <li>• "Planung für Speicherpools auf DISK- oder FILE-Einheiten"</li> </ul>             |
| Verfügt der Server über genügend Speicher?           | <p>Höhere Arbeitslasten und erweiterte Funktionen wie beispielsweise Datendeduplizierung und Knotenreplikation erfordern mehr Systempeicher als den Mindestspeicher, der im Dokument mit den Systemvoraussetzungen angegeben ist. Verwenden Sie die folgenden Richtlinien, um den Speicherbedarf für Datenbanken anzugeben, die nicht für die Datendeduplizierung aktiviert sind:</p> <ul style="list-style-type: none"> <li>• Für Datenbanken mit einer Größe unter 500 GB benötigen Sie 16 GB Speicher.</li> <li>• Für Datenbanken mit einer Größe von 500 GB bis 1 TB benötigen Sie 24 GB Speicher.</li> <li>• Für Datenbanken mit einer Größe von 1 TB bis 1,5 TB benötigen Sie 32 GB Speicher.</li> <li>• Für Datenbanken mit einer Größe über 1,5 TB benötigen Sie 40 GB Speicher.</li> </ul> <p>Stellen Sie sicher, dass Sie für die Replikationsverarbeitung zusätzlichen Speicherbereich für die aktive Protokolldatei und das Archivprotokoll zuordnen.</p> | <p>Weitere Informationen zu Voraussetzungen, wenn die entsprechenden Funktionen verwendet werden, finden Sie in den folgenden Abschnitten:</p> <ul style="list-style-type: none"> <li>• Prüfliste für Datendeduplizierung</li> <li>• Prüfliste für Knotenreplikation</li> <li>• Speicherbedarf</li> </ul> |



| Frage   | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen  |
|---|--|--|
| <p>Verfügt das System über genügend Hostbusadapter (HBAs), um die Datenoperationen, die der IBM Spectrum Protect-Server gleichzeitig ausführen muss, handhaben zu können?</p> | <p>Sie müssen wissen, für welche Operationen die gleichzeitige Verwendung von Hostbusadaptern erforderlich ist.</p> <p>Ein Server muss beispielsweise Sicherungsdaten mit 1 GB/s speichern, während er gleichzeitig eine Speicherpoolumlagerung ausführt, für deren Ausführung eine Kapazität von 0,5 GB/s erforderlich ist. Die Hostbusadapter müssen alle Daten mit der erforderlichen Geschwindigkeit handhaben können.</p>         | <p>Siehe HBA-Kapazität optimieren.</p>   |
| <p>Ist die Netzbandbreite größer als der geplante maximale Durchsatz für Sicherungen?</p>   | <p>Die Netzbandbreite muss dem System die Ausführung von Operationen wie Sicherungen innerhalb der zulässigen Zeit oder gemäß den vereinbarten Service-Levels ermöglichen.</p> <p>Bei der Knotenreplikation muss die Netzbandbreite größer als der geplante maximale Durchsatz sein.</p>   | <p>Weitere Informationen finden Sie in:</p> <ul style="list-style-type: none"> <li>• Netzleistung optimieren</li> <li>• Prüfliste für Knotenreplikation</li> </ul> |
| <p>Verwenden Sie ein bevorzugtes Dateisystem für IBM Spectrum Protect-Serverdateien?</p>  | <p>Verwenden Sie ein Dateisystem, das optimale Leistung und Datenverfügbarkeit gewährleistet. Der Server verwendet die direkte E/A mit Dateisystemen, die die Funktion unterstützen. Die Verwendung der direkten E/A kann den Durchsatz verbessern und die Prozessornutzung verringern. Weitere Informationen zum bevorzugten Dateisystem für Ihr Betriebssystem finden Sie in IBM Spectrum Protect server-supported file systems.</p> | <p>Weitere Informationen finden Sie in Betriebssystem für die Plattenleistung konfigurieren.</p>   |

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen |
|--|--|-----------------------|
| Planen Sie, genügend Seitenauslagerungsbereich zu konfigurieren? | <p>Seitenauslagerungsbereich (oder Auslagerungsspeicher) erweitert den Speicher, der für die Verarbeitung verfügbar ist. Wenn der freie Arbeitsspeicher im System knapp wird, werden Programme oder Daten, die nicht im Gebrauch sind, aus dem Speicher in den Seitenauslagerungsbereich versetzt. Mit dieser Aktion wird Speicherbereich für andere Aktivitäten, wie z. B. Datenbankoperationen, freigegeben.</p> <p> Windows-Betriebssysteme<br/>Der Seitenauslagerungsbereich wird automatisch konfiguriert.</p> |                       |

## Windows: Planung für Platten für die Serverdatenbank

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen  |
|--|--|--|
| Befindet sich die Datenbank auf schnellen Platten mit kurzer Latenzzeit? | <p>Verwenden Sie die folgenden Laufwerke nicht für die IBM Spectrum Protect-Datenbank:</p> <ul style="list-style-type: none"> <li>• Nearline SAS (NL-SAS)</li> <li>• Serial Advanced Technology Attachment (SATA)</li> <li>• Parallel Advanced Technology Attachment (PATA)</li> </ul> <p>Verwenden Sie keine internen Platten, die standardmäßig Teil der Hardware der meisten Server ist.</p> <p>Enterprise-Solid-State-Laufwerke mit Fibre Channel- oder SAS-Schnittstellen bieten die beste Leistung.</p> <p>Wenn Sie planen, die Datendeduplizierungsfunktionen von IBM Spectrum Protect zu verwenden, legen Sie den Schwerpunkt auf die Plattenleistung (gemessen in E/A-Operationen pro Sekunde).</p> | Weitere Informationen finden Sie in Prüfliste für Datendeduplizierung. |

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen  |
|--|---|--|
| Ist die Datenbank auf anderen Platten oder LUNs gespeichert als die aktive Protokolldatei, das Archivprotokoll und die Speicherpooldatenträger?                      | Das Trennen der Serverdatenbank von anderen Serverkomponenten trägt zur Reduktion von Konkurrenzsituationen für dieselben Ressourcen durch unterschiedliche Operationen, die gleichzeitig ausgeführt werden müssen, bei.<br>Tipp: Die Datenbank und das Archivprotokoll können ein Array gemeinsam nutzen, wenn Sie die Solid-State-Laufwerk-Technologie (SSD-Technologie) verwenden.   |  |
| Wissen Sie bei Verwendung von RAID, wie die optimale RAID-Stufe für Ihr System ausgewählt wird? Definieren Sie alle LUNs mit derselben Größe und demselben RAID-Typ? | Wenn ein System viele Schreibvorgänge ausführen muss, ist die Leistung bei RAID 10 besser als bei RAID 5. RAID 10 benötigt jedoch mehr Platten als RAID 5, um dieselbe nutzbare Speichermenge bereitzustellen.<br><br>Handelt es sich bei Ihrem Plattensystem um ein RAID-System, definieren Sie alle LUNs mit derselben Größe und demselben RAID-Typ. Verwenden Sie beispielsweise nicht gleichzeitig 4+1 RAID 5 mit 4+2 RAID 6. |  |
| Planen Sie, wenn eine Option zum Definieren der Stripgröße oder der Segmentgröße verfügbar ist, die Größe beim Konfigurieren des Plattensystems zu optimieren?       | Wenn Sie die Stripgröße oder Segmentgröße definieren können, verwenden Sie auf Plattensystemen für die Datenbank Größen von 64 KB oder 128 KB.  | Die Blockgröße, die für die Datenbank verwendet wird, variiert abhängig vom Tabellenbereich. Die meisten Tabellenbereiche verwenden 8-KB-Blöcke; einige verwenden jedoch 32-KB-Blöcke. |

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen   |
|---|---|---|
| <p>Planen Sie, mindestens vier Verzeichnisse, die auch als Speicherpfade bezeichnet werden, auf vier verschiedenen LUNs für die Datenbank zu erstellen?</p> <p>Erstellen Sie exakt ein Verzeichnis pro Array in dem Subsystem. Wenn weniger als drei Arrays vorhanden sind, erstellen Sie in jedem Array einen anderen LUN-Datenträger.</p> | <p>Für größere Arbeitslasten und bei Verwendung einiger Funktionen sind mehr Datenbankspeicherpfade als die Mindestvoraussetzungen erforderlich.</p> <p>Serveroperationen wie die Datenduplizierung verursachen eine hohe Anzahl Ein-/Ausgabeoperationen pro Sekunde (IOPS) für die Datenbank. Die Leistung derartiger Operationen ist besser, wenn die Datenbank über mehr Verzeichnisse verfügt.</p> <p>Verwenden Sie für Serverdatenbanken, die größer als 2 TB sind oder die wahrscheinlich auf diese Größe anwachsen, acht Verzeichnisse.</p> <p>Berücksichtigen Sie das geplante Wachstum des Systems bei der Bestimmung der Anzahl zu erstellender Speicherpfade. Die höhere Anzahl Speicherpfade wird vom Server effizienter genutzt, wenn die Speicherpfade bei der Ersterstellung des Servers bereits vorhanden sind.</p> <p>Verwenden Sie die Variable <i>DB2_PARALLEL_IO</i>, um die parallele E/A für Tabellenbereiche mit einem einzelnen Container zu erzwingen oder für Tabellenbereiche, die über Container auf mehr als einer physischen Platte verfügen. Wenn Sie die Variable <i>DB2_PARALLEL_IO</i> nicht definieren, entspricht die E/A-Parallelität der Anzahl Container, die von dem Tabellenbereich verwendet werden. Wenn ein Tabellenbereich beispielsweise vier Container umfasst, beträgt der verwendete Grad an E/A-Parallelität 4.</p> | <p>Weitere Informationen finden Sie in:</p> <ul style="list-style-type: none"> <li>• Prüfliste für Datenduplizierung</li> <li>• Prüfliste für Knotenreplikation</li> </ul> <p>Hilfreiche Informationen zur Vorhersage des Wachstums beim Duplizieren von Daten durch den Server finden Sie in Technote 1596944.</p> <p>Aktuelle Informationen zur Datenbankgröße, zur Datenbankreorganisation und zu Leistungsaspekten für IBM Spectrum Protect-Server finden Sie in Technote 1683633.</p> <p>Informationen zum Definieren der Variable <i>DB2_PARALLEL_IO</i> finden Sie in Empfohlene Einstellungen für IBM DB2-Registry-Variablen.</p> |
| <p>Haben alle Verzeichnisse für die Datenbank dieselbe Größe?</p>   | <p>Verzeichnisse, die alle dieselbe Größe haben, stellen einen konsistenten Grad an Parallelität für Datenbankoperationen sicher. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als andere sind, verringert sich dadurch das Potenzial für den optimierten parallelen Vorabesezugriff.</p> <p>Diese Richtlinie gilt auch, wenn Sie nach der Erstkonfiguration des Servers Speicherpfade hinzufügen müssen.</p>  |   |
| <p>Planen Sie, die Warteschlangenlänge der Datenbank-LUNs auf AIX-Systemen zu erhöhen?</p>  | <p>Die Standardwarteschlangenlänge ist häufig zu niedrig definiert.</p>   | <p>Siehe AIX-Systeme für die Plattenleistung konfigurieren.</p>   |

## Windows: Planung für Platten für das Serverwiederherstellungsprotokoll

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen  |
|---|---|--|
| Sind die aktive Protokolldatei und das Archivprotokoll auf anderen Platten oder LUNs gespeichert als die Datenbank und die Speicherpooldateiträger? | Stellen Sie sicher, dass die Platten, auf die die aktive Protokolldatei gestellt wird, auf dem Server oder System nicht für andere Zwecke verwendet werden. Stellen Sie die aktive Protokolldatei nicht auf Platten, die die Serverdatenbank, das Archivprotokoll oder Systemdateien, wie Seitenauslagerungsbereich oder Auslagerungsspeicher, enthalten.   | Das Trennen der Serverdatenbank von der aktiven Protokolldatei und dem Archivprotokoll trägt zur Reduktion von Konkurrenzsituationen für dieselben Ressourcen durch unterschiedliche Operationen, die gleichzeitig ausgeführt werden müssen, bei.  |
| Befinden sich die Protokolle auf Platten mit nicht flüchtigem Schreibcache?   | Nicht flüchtiger Schreibcache ermöglicht es, Daten so schnell wie möglich in die Protokolle zu schreiben. Schnellere Schreiboperationen für die Protokolle können die Leistung für Serveroperationen verbessern.  |  |
| Legen Sie für die Protokolle eine Größe fest, die der Arbeitslast entspricht?   | <p>Wenn Sie sich über die Arbeitslast im Unklaren sind, verwenden Sie die größtmögliche Größe.</p> <p><b>Aktive Protokolldatei</b><br/>Die maximale Größe beträgt 512 GB; sie wird über die Serveroption <code>ACTIVELOGSIZE</code> festgelegt.</p> <p>Stellen Sie sicher, dass mindestens 8 GB freier Speicherbereich im Dateisystem für aktive Protokolldateien verfügbar sind, nachdem die aktiven Protokolldateien mit fester Größe erstellt wurden.</p> <p><b>Archivprotokoll</b><br/>Die Größe des Archivprotokolls wird durch die Größe des Dateisystems begrenzt, in dem es sich befindet, und nicht durch eine Serveroption. Das Archivprotokoll muss mindestens so groß wie die aktive Protokolldatei sein.</p> | <ul style="list-style-type: none"> <li>• Ausführliche Informationen zur Festlegung der Protokollgröße enthalten die Informationen zum Wiederherstellungsprotokoll in Technote 1421060.</li> <li>• Informationen zur Festlegung der Größe bei Verwendung der Dateneduplizierung finden Sie in Prüfliste für Dateneduplizierung.</li> </ul>                                  |
| Definieren Sie ein Archivübernahmeprotokoll? Stellen Sie dieses Protokoll auf eine andere Platte als das Archivprotokoll?                           | Das Archivübernahmeprotokoll dient der Verwendung durch den Server im Notfall, wenn das Archivprotokoll voll ist. Für das Archivübernahmeprotokoll können langsamere Platten verwendet werden.  | <p>Geben Sie die Position des Archivübernahmeprotokolls mithilfe der Serveroption <code>ARCHFAILOVERLOGDIRECTORY</code> an.</p> <p>Überwachen Sie die Belegung des Verzeichnisses für das Archivübernahmeprotokoll. Wenn das Archivübernahmeprotokoll vom Server verwendet werden muss, ist der Speicherplatz für das Archivprotokoll möglicherweise nicht groß genug.</p> |
| Verwenden Sie, wenn Sie die aktive Protokolldatei spiegeln, nur einen einzigen Typ von Spiegelung?  | <p>Sie können das Protokoll mithilfe einer der folgenden Methoden spiegeln. Verwenden Sie für das Protokoll nur einen einzigen Typ von Spiegelung.</p> <ul style="list-style-type: none"> <li>• Verwenden Sie die Option <code>MIRRORLOGDIRECTORY</code>, die für den IBM Spectrum Protect-Server verfügbar ist, um eine Position für die Spiegelung anzugeben.</li> <li>• Verwenden Sie die Softwarespiegelung, wie z. B. Logical Volume Manager (LVM) unter AIX.</li> <li>• Verwenden Sie die Spiegelung in der Hardware des Plattensystems.</li> </ul>   | <p>Stellen Sie, wenn Sie die aktive Protokolldatei spiegeln, sicher, dass die Platten für die aktive Protokolldatei und die Spiegelkopie dieselbe Geschwindigkeit und Zuverlässigkeit haben.</p> <p>Weitere Informationen finden Sie in Wiederherstellungsprotokoll konfigurieren und optimieren.</p>  |

## Windows: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools

Überprüfen Sie die Konfiguration Ihrer Verzeichniscontainer- und Cloud-Containerspeicherpools, um eine optimale Leistung zu gewährleisten.

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen   |
|--|--|---|
| <p>Verwenden Sie, gemessen in Anzahl Ein-/Ausgabeoperationen pro Sekunde (IOPS), schnellen Plattenspeicher für die IBM Spectrum Protect-Datenbank?</p> | <p>Verwenden Sie eine Hochleistungsplatte für die Datenbank. Verwenden Sie die Solid-State-Laufwerk-Technologie (SSD-Technologie) für die Datendeduplizierungsverarbeitung.</p> <p>Stellen Sie sicher, dass die Datenbank über eine Mindestkapazität von 3000 E/A-Operationen pro Sekunde (IOPS) verfügt. Addieren Sie zu diesem Mindestwert pro TB Daten, die täglich (vor der Datendeduplizierung) gesichert werden, 1000 E/A-Operationen pro Sekunde.</p> <p>Beispielsweise würde ein IBM Spectrum Protect-Server, der täglich 3 TB Daten aufnimmt, 6000 E/A-Operationen pro Sekunde (IOPS) für die Datenbankplatten benötigen:</p> <p>mindestens 3000 IOPS + 3000 (3 TB x 1000 IOPS) = 6000 IOPS</p>   | <p>Empfehlungen zur Plattenauswahl finden Sie in "Planung für Platten für die Serverdatenbank".</p> <p>Weitere Informationen zu IOPS finden Sie in den IBM Spectrum Protect-Blueprints.</p> |
| <p>Ist genügend Speicherplatz für die Größe Ihrer Datenbank vorhanden?</p>   | <p>Verwenden Sie mindestens 40 GB Systemspeicher für IBM Spectrum Protect-Server, die Daten deduplizieren, mit einer Datenbankgröße von 100 GB. Wenn die Speicherkapazität für Sicherungsdaten wächst, ist unter Umständen ein höherer Speicherbedarf erforderlich.</p> <p>Überwachen Sie regelmäßig die Speicherbelegung, um festzustellen, ob mehr Speicherplatz erforderlich ist.</p> <p>Verwenden Sie weiteren Systemspeicher, um das Caching von Datenbankseiten zu verbessern. Die folgenden Richtlinien für die Speichergröße basieren auf dem Volumen an neuen Daten, das jeden Tag gesichert wird:</p> <ul style="list-style-type: none"> <li>• 128 GB Systemspeicher für tägliche Sicherungen von Daten, wobei die Datenbankgröße zwischen 1 und 2 TB liegt</li> <li>• 192 GB Systemspeicher für tägliche Sicherungen von Daten, wobei die Datenbankgröße zwischen 2 und 4 TB liegt</li> </ul> | <p>Speicherbedarf</p>   |

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen   |
|---|--|---|
| <p>Haben Sie die Speicherkapazität für die die aktive Protokolldatei und das Archivprotokoll der Datenbank korrekt festgelegt?</p>  | <p>Geben Sie in der Konfiguration des Servers eine minimale Größe von 128 GB für die aktive Protokolldatei an, indem Sie die Serveroption ACTIVELOGSIZE auf den Wert 131072 setzen.</p> <p>Als Anfangsgröße für das Archivprotokoll wird eine Größe von 1 TB vorgeschlagen. Die Größe des Archivprotokolls wird durch die Größe des Dateisystems begrenzt, in dem es sich befindet, und nicht durch eine Serveroption. Stellen Sie sicher, dass im Vergleich zur Größe des Archivprotokolls mindestens 10 % zusätzlicher Plattenspeicher für das Dateisystem vorhanden sind.</p> <p>Verwenden Sie für die Datenbankarchivprotokolle ein Verzeichnis mit einer anfänglichen freien Kapazität von mindestens 1 TB. Geben Sie das Verzeichnis mithilfe der Serveroption ARCHLOGDIRECTORY an.</p> <p>Definieren Sie Speicherbereich für das Archivübernahmeprotokoll mithilfe der Serveroption ARCHFAILOVERLOGDIRECTORY.</p> | <p>Weitere Informationen zur Kapazitätsermittlung für Ihr System finden Sie in den IBM Spectrum Protect-Blueprints.</p>   |
| <p>Ist die Komprimierung für die Archivprotokoll- und Datenbanksicherungen aktiviert?</p>   | <p>Aktivieren Sie die Serveroption ARCHLOGCOMPRESS, um Speicherbereich einzusparen.</p> <p>Diese Komprimierungsoption unterscheidet sich von der Inline-Komprimierung. Die Inline-Komprimierung ist ab IBM Spectrum Protect Version 7.1.5 und höher standardmäßig aktiviert.</p> <p>Einschränkung: Sie dürfen diese Option nicht verwenden, wenn das Volumen der pro Tag gesicherten Daten 6 TB überschreitet.</p>   | <p>Weitere Informationen zur Komprimierung für Ihr System finden Sie in den IBM Spectrum Protect-Blueprints.</p>  |
| <p>Befinden sich die Datenbank und Protokolle von IBM Spectrum Protect auf separaten Plattendatenträgern (LUNs)?</p> <p>Ist der Datenträger, der für die Datenbank verwendet wird, gemäß den bewährten Verfahren für eine transaktionsorientierte Datenbank konfiguriert?</p> | <p>Die Datenbank darf keine Plattendatenträger mit IBM Spectrum Protect-Datenbankprotokollen oder -Speicherpools oder mit einer anderen Anwendung oder einem anderen Dateisystem gemeinsam nutzen.</p>   | <p>Weitere Informationen zur Konfiguration der Serverdatenbank und des Wiederherstellungsprotokolls finden Sie in Konfiguration und Optimierung der Serverdatenbank und des Wiederherstellungsprotokolls.</p> |
| <p>Verwenden Sie mindestens acht Prozessorkerne (2,2-GHz-Prozessorkerne oder entsprechende Prozessorkerne) für jeden IBM Spectrum Protect-Server, der mit Datendeduplizierung verwendet werden soll?</p>  | <p>Wenn die clientseitige Datendeduplizierung verwendet werden soll, müssen Sie sicherstellen, dass für Clientsysteme während einer Sicherungsoperation genügend Ressourcen zur Ausführung der Datendeduplizierungsverarbeitung verfügbar sind. Verwenden Sie pro Sicherungsprozess mit clientseitiger Datendeduplizierung einen Prozessor, der mindestens einem 2,2-GHz-Prozessorkern entspricht.</p>   | <ul style="list-style-type: none"> <li>• Effektive Planung und Verwendung der Deduplizierung</li> <li>• IBM Spectrum Protect Blueprints</li> </ul>  |

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen  |
|---|---|--|
| Haben Sie genügend Speicherplatz für die Datenbank zugeordnet?  | <p>Als grobe Schätzung sollten Sie 100 GB Datenbankspeicher für jeweils 50 TB Daten einplanen, die in deduplizierten Speicherpools geschützt werden sollen. <i>Geschützte Daten</i> ist das Datenvolumen vor der Dateneduplizierung, einschließlich aller Versionen gespeicherter Objekte.</p> <p>Als bewährtes Verfahren sollten Sie einen neuen Containerspeicherpool ausschließlich für die Dateneduplizierung definieren. Die Dateneduplizierung erfolgt auf der Speicherpoolebene; mit Ausnahme von verschlüsselten Daten werden alle Daten in einem Speicherpool dedupliziert.</p>  |  |
| Haben Sie die Speicherpoolkapazität geschätzt, um genügend Speicherplatz für die Größe Ihrer Umgebung zu konfigurieren? | <p>Sie können den Kapazitätsbedarf für einen deduplizierten Speicherpool wie folgt schätzen:</p> <ol style="list-style-type: none"> <li>1. Schätzen Sie die Basisgröße der Quelldaten.</li> <li>2. Schätzen Sie die Größe der täglichen Sicherung anhand einer geschätzten Änderungs- und Wachstumsrate.</li> <li>3. Bestimmen Sie die Anforderungen in Bezug auf die Aufbewahrungsdauer.</li> <li>4. Schätzen Sie das Gesamtvolumen an Quelldaten unter Berücksichtigung der Basisgröße, der Größe der täglichen Sicherung und der Anforderungen in Bezug auf die Aufbewahrungsdauer.</li> <li>5. Wenden Sie den Faktor für das Deduplizierungsverhältnis an.</li> <li>6. Wenden Sie den Faktor für das Komprimierungsverhältnis an.</li> <li>7. Runden Sie die Schätzung auf, um die Nutzung transienter Speicherpools zu berücksichtigen.</li> </ol> | Ein Beispiel zur Verwendung dieses Verfahrens finden Sie in Effektive Planung und Verwendung der Deduplizierung. |



| Frage   | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen  |
|---|--|--|
| Haben Sie die Platten-E/A auf viele Platteneinheiten und Controller verteilt?   | <p>Verwenden Sie Arrays, die aus so vielen Platten wie möglich bestehen; dies wird auch als "Wide-Striping" bezeichnet. Stellen Sie sicher, dass Sie exakt ein Datenbankverzeichnis pro Array in dem Subsystem verwenden.</p> <p>Definieren Sie die Registry-Variable <i>DB2_PARALLEL_IO</i>, um die parallele E/A für jeden verwendeten Tabellenbereich zu aktivieren, wenn sich die Container in dem Tabellenbereich über mehrere physische Platten erstrecken.</p> <p>Wenn E/A-Bandbreite verfügbar ist und die Dateien groß sind (beispielsweise 1 MB), kann der Prozess zur Suche nach Duplikaten die Ressourcen eines gesamten Prozessors in Anspruch nehmen. Wenn Dateien kleiner sind, können andere Engpässe auftreten.</p> <p>Geben Sie acht oder mehr Dateisysteme für die Einheitenklasse des deduplizierten Speicherpools an, damit die Ein-/Ausgabe auf so viele LUNs und physische Einheiten wie möglich verteilt wird.</p> | <p>Richtlinien zur Konfiguration von Speicherpools finden Sie in "Planung für Speicherpools auf DISK- oder FILE-Einheiten".</p> <p>Informationen zum Definieren der Variable <i>DB2_PARALLEL_IO</i> finden Sie in Empfohlene Einstellungen für IBM DB2-Registry-Variablen.</p> |
| Haben Sie tägliche Operationen auf der Basis Ihrer Sicherungsstrategie geplant? | <p>Die Operationsfolge sieht gemäß den bewährten Verfahren wie folgt aus:</p> <ol style="list-style-type: none"> <li>1. Clientsicherung</li> <li>2. Speicherpoolschutz</li> <li>3. Knotenreplikation</li> <li>4. Datenbanksicherung</li> <li>5. Bestandsverfall</li> </ol>   | <ul style="list-style-type: none"> <li>• Datendeduplizierungs- und Knotenreplikationsprozesse planen</li> <li>• Tägliche Operation für Verzeichniscontainerspeicherpools</li> </ul>  |
| Ist genügend Speicher zur Verwaltung der DB2-Sperrenliste vorhanden?            | <p>Wenn Sie Daten deduplizieren, die große Dateien oder gleichzeitig eine große Anzahl Dateien umfassen, kann der Prozess zur Speicherknappheit führen. Wenn der Sperrenlistenspeicher nicht ausreichend ist, können Sicherheitsfehler, Datenverwaltungsprozessfehler oder Serverausfälle auftreten.</p> <p>Bei Dateigrößen über 500 GB, die durch die Datendeduplizierung verarbeitet werden, ist es sehr wahrscheinlich, dass der Speicherplatz knapp wird. Wenn jedoch viele Sicherungsoperationen die clientseitige Datendeduplizierung verwenden, kann dieses Problem auch bei Dateien mit geringerer Größe auftreten.</p>  | <p>Informationen zur Optimierung des DB2-Parameters LOCKLIST finden Sie in Serverseitige Datendeduplizierung optimieren.</p>   |

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen  |
|--|---|--|
| Ist genügend Bandbreite verfügbar, um Daten auf einen IBM Spectrum Protect-Server zu übertragen?       | <p>Um Daten auf einen IBM Spectrum Protect-Server zu übertragen, verwenden Sie die clientseitige oder serverseitige Datendeduplizierung und die Komprimierung, um die erforderliche Bandbreite zu verringern.</p> <p>Verwenden Sie einen Server der Version 7.1.5 oder höher, um die Inline-Komprimierung verwenden zu können, und einen Client der Version 7.1.6 oder höher, um die erweiterte Komprimierungsverarbeitung zu aktivieren.</p>   | Weitere Informationen finden Sie in der Beschreibung der Clientoption <code>enablededup</code> . |
| Haben Sie festgelegt, wie viele Speicherpoolverzeichnisse jedem Speicherpool zugeordnet werden sollen? | <p>Ordnen Sie Verzeichnisse einem Speicherpool mithilfe des Befehls <code>DEFINE STGPOOLDIRECTORY</code> zu.</p> <p>Erstellen Sie mehrere Speicherpoolverzeichnisse und stellen Sie sicher, dass jedes Verzeichnis auf einem anderen Plattendatenträger (LUN) gesichert wird.</p>   |  |
| Haben Sie genügend Plattenspeicherplatz in dem Cloud-Containerspeicherpool zugeordnet?                 | <p>Um Sicherheitsfehler zu verhindern, stellen Sie sicher, dass das lokale Verzeichnis über genügend Speicherplatz verfügt. Verwenden Sie die folgende Liste als Leitfaden für optimalen Plattenspeicherplatz:</p> <ul style="list-style-type: none"> <li>• Berechnen Sie für SAS-Platten (SAS = Serial-Attached SCSI) und rotierende Platten das Volumen neuer Daten, das nach der täglichen Datenreduktion (Komprimierung und Datendeduplizierung) erwartet wird. Ordnen Sie bis zu 100 Prozent dieses Volumens (in Terabyte) für den Plattenspeicherplatz zu.</li> <li>• Stellen Sie 3 TB für flash-basierte Speichersysteme mit schnellen Netzverbindungen zu leistungsfähigen On-Premises-Cloudsystemen bereit.</li> <li>• Stellen Sie 5 TB für Systeme mit Solid-State-Laufwerk (SSD) mit schnellen Netzverbindungen zu leistungsfähigen Cloudsystemen bereit.</li> </ul> |  |

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen  | Weitere Informationen |
|---|---|-----------------------|
| <p>Haben Sie den geeigneten Typ des lokalen Speichers ausgewählt?</p> | <p>Stellen Sie sicher, dass Datenübertragungen aus dem lokalen Speicher in die Cloud beendet werden, bevor der nächste Sicherungszyklus beginnt.</p> <p>Tipp: Daten werden kurz nach dem Versetzen in die Cloud aus dem lokalen Speicher entfernt.</p> <p>Verwenden Sie die folgenden Richtlinien:</p> <ul style="list-style-type: none"> <li>• Verwenden Sie Flash- oder SSD-Speicher für große Systeme, die über leistungsfähige Cloudsysteme verfügen. Stellen Sie sicher, dass Sie über eine dedizierte 10-GB-WAN-Verbindung mit einer Hochgeschwindigkeitsverbindung zum Objektspeicher verfügen. Verwenden Sie beispielsweise Flash- oder SSD-Speicher, wenn Sie über eine dedizierte 10-GB-WAN-Verbindung sowie eine Hochgeschwindigkeitsverbindung zu einem IBM® Cloud Object Storage-Speicherort oder zu einem Amazon S3-Datencenter (Amazon S3 = Amazon Simple Storage Service) verfügen.</li> <li>• Verwenden Sie SAS-Platten mit 15000 U/min mit größerer Kapazität für die folgenden Szenarios: <ul style="list-style-type: none"> <li>◦ Systeme mittlerer Größe</li> <li>◦ Langsamere Cloudverbindungen, z. B. 1 GB</li> <li>◦ Bei Verwendung von IBM Cloud Object Storage als Service-Provider in mehreren Regionen</li> </ul> </li> <li>• Berechnen Sie für SAS-Platten oder rotierende Platten das Volumen neuer Daten, das nach der täglichen Datenreduktion (Komprimierung und Datendeduplizierung) erwartet wird. Ordnen Sie bis zu 100 Prozent dieses Volumens (in Terabyte) für den Plattenspeicherplatz zu.</li> </ul> |                       |

## Windows: Planung für Speicherpools auf DISK- oder FILE-Einheiten

Überprüfen Sie mithilfe der Prüfliste, wie Ihre Plattenspeicherpools konfiguriert sind. Diese Prüfliste umfasst Tipps für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden.

| Frage | Tasks, Merkmale, Optionen oder Einstellungen | Weitere Informationen |
|-------|--|-----------------------|
|-------|--|-----------------------|

| Frage   | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen  |
|---|--|--|
| <p>Können die Speicherpool-LUNs Durchsatzraten von 256 KB für sequenzielle Lese- und Schreibvorgänge aufrechterhalten, um die Arbeitslast innerhalb der Zeitvorgaben adäquat handhaben zu können?</p> | <p>Bei der Planung für Spitzenbelastungen müssen Sie alle Daten berücksichtigen, die der Server gleichzeitig aus Plattenspeicherpools lesen oder in Plattenspeicherpools schreiben soll. Berücksichtigen Sie beispielsweise den Spitzenwert für den Datenfluss bei Clientsicherungsoperationen und Serverdatenversetzungsoperationen, wie z. B. Umlagerung, die gleichzeitig ausgeführt werden.</p> <p>Der IBM Spectrum Protect-Server verwendet beim Lesen aus Speicherpools und Schreiben in Speicherpools in erster Linie 256-KB-Blöcke.</p> <p>Wenn das Plattensystem über die entsprechende Funktionalität verfügt, konfigurieren Sie das Plattensystem für die optimale Leistung mit sequenziellen Lese-/Schreiboperationen statt mit wahlfreien Lese-/Schreiboperationen.</p> | <p>Weitere Informationen finden Sie in Basisleistung von Plattensystemen analysieren.</p>  |
| <p>Ist die Platte für die Verwendung von Lese- und Schreibcache konfiguriert?</p>   | <p>Verwenden Sie mehr Cache, um eine bessere Leistung zu erzielen.</p>   |  |
| <p>Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, eine geeignete Größe für die Speicherpooldatenträger festgelegt?</p>  | <p>Lesen Sie die Informationen in Optimale Anzahl und Größe von Datenträgern für Speicherpools, die Platten verwenden. Wenn Sie nicht über die nötigen Informationen zum Schätzen der Größe für Datenträger mit der Einheitenklasse FILE verfügen, beginnen Sie mit einer Datenträgergröße von 50 GB.</p>  | <p>In der Regel treten häufiger Probleme auf, wenn die Datenträger zu klein sind. Wenn Datenträger größer als erforderlich sind, treten nur selten Probleme auf. Wenn Sie die zu verwendende Datenträgergröße festlegen, sollten Sie als Vorsichtsmaßnahme eine größere Größe als erforderlich wählen.</p> |
| <p>Verwenden Sie für Speicherpools, die die Einheitenklasse FILE verwenden, vorab zugeordnete Datenträger?</p>  | <p>Arbeitsdatenträger können eine Dateifragmentierung zur Folge haben.</p> <p>Um sicherzustellen, dass für einen Speicherpool immer genügend Datenträger verfügbar sind, setzen Sie den Parameter MAXSCRATCH auf einen Wert größer als null.</p>   | <p>Ordnen Sie mithilfe des Befehls DEFINE VOLUME Datenträger in dem Speicherpool vorab zu.</p> <p>Verwenden Sie den Serverbefehl DEFINE STGPOOL oder UPDATE STGPOOL, um den Parameter MAXSCRATCH zu definieren.</p>  |
| <p>Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, die maximale Anzahl Clientsitzungen mit der Anzahl definierter Datenträger verglichen?</p>                                    | <p>Es müssen immer genügend verwendbare Datenträger in den Speicherpools vorhanden sein, um die erwartete maximale Anzahl gleichzeitig ausgeführter Clientsitzungen handhaben zu können. Bei den Datenträgern kann es sich um Arbeitsdatenträger, leere Datenträger oder teilweise gefüllte Datenträger handeln.</p>   | <p>Bei Speicherpools, die die Einheitenklasse FILE verwenden, kann jeweils nur eine einzige Sitzung oder ein einziger Prozess auf einen Datenträger schreiben.</p>   |

| Frage  | Tasks, Merkmale, Optionen oder Einstellungen   | Weitere Informationen  |
|--|--|--|
| Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, den Parameter MOUNTLIMIT für die Einheitenklasse auf einen Wert gesetzt, der für die Anzahl Datenträger, die parallel angehängt werden könnten, ausreichend hoch ist? | <p>Für Speicherpools, die die Datendeduplizierung verwenden, liegt der Wert für den Parameter MOUNTLIMIT in der Regel zwischen 500 und 1000. Setzen Sie den Wert für MOUNTLIMIT auf die maximale Anzahl Mountpunkte, die für alle aktiven Sitzungen erforderlich sind. Berücksichtigen Sie Parameter, die sich auf die maximale Anzahl erforderlicher Mountpunkte auswirken:</p> <ul style="list-style-type: none"> <li>Die Serveroption MAXSESSIONS, die die maximal zulässige Anzahl gleichzeitig ablaufender IBM Spectrum Protect-Sitzungen angibt</li> <li>Der Parameter MAXNUMMP, der die maximale Anzahl Mountpunkte definiert, die jeder Clientknoten verwenden kann</li> </ul> <p>Wenn beispielsweise die maximale Anzahl Sicherungssitzungen für Clientknoten normalerweise 100 ist und für jeden der Knoten MAXNUMMP=2 definiert ist, multiplizieren Sie 100 Knoten mit 2 Mountpunkten für jeden Knoten, um den Wert 200 für den Parameter MOUNTLIMIT zu erhalten.</p> | Verwenden Sie den Serverbefehl REGISTER NODE oder UPDATE NODE, um den Parameter MAXNUMMP für Clientknoten zu definieren.   |
| Haben Sie für Speicherpools, die die Einheitenklasse DISK verwenden, festgelegt, wie viele Speicherpooldatenträger in jedes Dateisystem gestellt werden sollen?  | <p>Die Konfiguration des Speichers für einen Speicherpool, der eine Einheitenklasse DISK verwendet, ist davon abhängig, ob Sie RAID für das Plattensystem verwenden.</p> <p>Wenn Sie RAID nicht verwenden, konfigurieren Sie ein einziges Dateisystem pro physischer Platte und definieren Sie exakt einen Speicherpooldatenträger für jedes Dateisystem.</p> <p>Wenn Sie RAID 5 mit <math>n + 1</math> Datenträgern verwenden, konfigurieren Sie den Speicher auf eine der folgenden Arten:</p> <ul style="list-style-type: none"> <li>Konfigurieren Sie <math>n</math> Dateisysteme auf der LUN und definieren Sie exakt einen Speicherpooldatenträger pro Dateisystem.</li> <li>Konfigurieren Sie ein einziges Dateisystem und <math>n</math> Speicherpooldatenträger für die LUN.</li> </ul>   | Ein Beispiellayout, bei dem diese Richtlinie eingehalten wird, zeigt Beispiellayout für Serverspeicherpools.   |
| Haben Sie Ihre Speicherpools für die Verteilung der Ein-/Ausgabe auf mehrere Dateisysteme erstellt?  | <p>Stellen Sie sicher, dass sich jedes Dateisystem auf einer anderen LUN auf dem Plattensystem befindet.</p> <p>Normalerweise sind 10-30 Dateisysteme ein geeigneter Wert, Sie müssen jedoch sicherstellen, dass die Dateisysteme nicht kleiner als etwa 250 GB sind.</p>  | <p>Ausführliche Informationen finden Sie in:</p> <ul style="list-style-type: none"> <li>Plattenspeicher für den Server optimieren</li> <li>Speicherpools und Datenträger optimieren und konfigurieren</li> </ul> |

## Windows: Planung für die Auswahl des korrekten Speichertechnologietyps

Speichereinheiten haben eine unterschiedliche Kapazität und unterschiedliche Leistungsmerkmale. Diese Merkmale wirken sich darauf aus, welche Einheiten besser für die Verwendung mit IBM Spectrum Protect geeignet sind.

### Vorgehensweise

Die folgende Tabelle unterstützt Sie bei der Auswahl des korrekten Speichertechnologietyps für die Speicherressourcen, die der Server erfordert.

Tabelle 1. Speichertechnologietypen für IBM Spectrum Protect-Speicherbedarf

| <b>Speichertechnologietyp</b>   | <b>Datenbank</b>   | <b>Aktive Protokolldatei</b>  | <b>Archivprotokoll und Archivübernahmeprotokoll</b>  | <b>Speicherpools</b>   |
|---|--|---|--|--|
| <b>Solid-State-Laufwerk (SSD)</b>   | <p>Stellen Sie die Datenbank auf ein Solid-State-Laufwerk, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Sie verwenden die IBM Spectrum Protect-Dateneduplizierung.</li> <li>• Sie sichern täglich mehr als 8 TB neuer Daten.</li> </ul>   | <p>Wenn Sie die IBM Spectrum Protect-Datenbank auf ein Solid-State-Laufwerk stellen (dies ist das bewährte Verfahren), stellen Sie auch die aktive Protokolldatei auf ein Solid-State-Laufwerk. Wenn kein Speicherplatz verfügbar ist, verwenden Sie stattdessen eine Hochleistungsplatte.</p>  | <p>Reservieren Sie die Solid-State-Laufwerke für die Verwendung mit der Datenbank und der aktiven Protokolldatei. Das Archivprotokoll und die Archivübernahmeprotokolle können auf langsamere Speichertechnologietypen gestellt werden.</p>                          | <p>Reservieren Sie die Solid-State-Laufwerke für die Verwendung mit der Datenbank und der aktiven Protokolldatei. Speicherpools können auf langsamere Speichertechnologietypen gestellt werden.</p>  |
| <p><b>Hochleistungsplatte mit den folgenden Kenndaten:</b></p> <ul style="list-style-type: none"> <li>• <b>Platte mit 15.000 U/min</b></li> <li>• <b>Fibre Channel - oder Serial-attach und SCSI-Schnittstelle (SAS-Schnittstelle)</b></li> </ul> | <p>Verwenden Sie Hochleistungsplatten, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Der Server führt keine Dateneduplizierung aus.</li> <li>• Der Server führt keine Knotenreplikation aus.</li> </ul> <p>Trennen Sie die Serverdatenbank von den zugehörigen Protokollen und Speicherpools sowie von Daten für andere Anwendungen.</p> | <p>Verwenden Sie Hochleistungsplatten, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Der Server führt keine Dateneduplizierung aus.</li> <li>• Der Server führt keine Knotenreplikation aus.</li> </ul> <p>Trennen Sie aus Gründen der Leistung und Verfügbarkeit die aktive Protokolldatei von der Serverdatenbank, den Archivprotokollen und den Speicherpools.</p> | <p>Sie können Hochleistungsplatten für das Archivprotokoll und die Archivübernahmeprotokolle verwenden. Trennen Sie aus Gründen der Verfügbarkeit diese Protokolle von der Datenbank und der aktiven Protokolldatei.</p>   | <p>Verwenden Sie Hochleistungsplatten für Speicherpools, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Daten werden häufig gelesen.</li> <li>• Daten werden häufig geschrieben.</li> </ul> <p>Trennen Sie aus Gründen der Leistung und Verfügbarkeit die Speicherpooldaten von der Serverdatenbank und den Protokollen sowie von Daten für andere Anwendungen.</p>   |
| <p><b>Platte mit mittlerer Leistung oder Hochleistungsplatte mit den folgenden Kenndaten:</b></p> <ul style="list-style-type: none"> <li>• <b>Platte mit 10.000 U/min</b></li> <li>• <b>Fibre Channel - oder SAS-Schnittstelle</b></li> </ul>     | <p>Wenn das Plattensystem eine Kombination verschiedener Plattentechnologien verwendet, verwenden Sie die schnelleren Platten für die Datenbank und die aktive Protokolldatei. Trennen Sie die Serverdatenbank von den zugehörigen Protokollen und Speicherpools sowie von Daten für andere Anwendungen.</p>   | <p>Wenn das Plattensystem eine Kombination verschiedener Plattentechnologien verwendet, verwenden Sie die schnelleren Platten für die Datenbank und die aktive Protokolldatei. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die aktive Protokolldatei von der Serverdatenbank, den Archivprotokollen und den Speicherpools.</p>   | <p>Sie können eine Platte mit mittlerer Leistung oder eine Hochleistungsplatte für das Archivprotokoll und die Archivübernahmeprotokolle verwenden. Trennen Sie aus Gründen der Verfügbarkeit diese Protokolle von der Datenbank und der aktiven Protokolldatei.</p> | <p>Verwenden Sie eine Platte mit mittlerer Leistung oder eine Hochleistungsplatte für Speicherpools, wenn die folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> <li>• Daten werden häufig gelesen.</li> <li>• Daten werden häufig geschrieben.</li> </ul> <p>Trennen Sie aus Gründen der Leistung und Verfügbarkeit die Speicherpooldaten von der Serverdatenbank und den Protokollen sowie von Daten für andere Anwendungen.</p> |

| Speichertechnologietyp                      | Datenbank   | Aktive Protokolldatei  | Archivprotokoll und Archivübernahmeprotokoll  | Speicherpools  |
|---|---|--|---|--|
| <b>SATA, Network-attached Storage (NAS)</b> | Verwenden Sie diesen Speicher nicht für die Datenbank. Stellen Sie die Datenbank nicht auf XIV-Speichersysteme. | Verwenden Sie diesen Speicher nicht für die aktive Protokolldatei. | Die Verwendung dieser langsameren Speichertechnologie ist akzeptabel, da diese Protokolle einmal geschrieben und nur selten gelesen werden. | Verwenden Sie diese langsamere Speichertechnologie, wenn die folgenden Bedingungen erfüllt sind: <ul style="list-style-type: none"> <li>• Daten werden selten geschrieben, beispielsweise einmal.</li> <li>• Daten werden selten gelesen.</li> </ul> |
| <b>Bänder und virtuelle Bänder</b>          |   |  |   | Verwenden Sie diese Speichermedien für die langfristige Aufbewahrung oder wenn Daten nur selten verwendet werden.  |

## Windows: Bewährte Verfahren bei der Serverinstallation anwenden

Normalerweise hat die Konfiguration und Auswahl der Hardware die deutlichsten Auswirkungen auf die Leistung einer IBM Spectrum Protect-Lösung. Weitere Faktoren, die sich auf die Leistung auswirken, sind die Auswahl und Konfiguration des Betriebssystems sowie die Konfiguration von IBM Spectrum Protect.

### Vorgehensweise

- Nachfolgend sind die wichtigsten bewährten Verfahren für die Erzielung der optimalen Leistung und die Vermeidung von Problemen aufgeführt.
- Bestimmen Sie anhand der Tabelle die bewährten Verfahren, die für Ihre Umgebung gelten.

| Bewährtes Verfahren  | Weitere Informationen  |
|--|--|
| Verwenden Sie schnelle Platten für die Serverdatenbank. Enterprise-Solid-State-Laufwerke mit Fibre Channel- oder SAS-Schnittstellen bieten die beste Leistung. | Verwenden Sie schnelle Platten mit kurzer Latenzzeit für die Datenbank. Die Verwendung von Solid-State-Laufwerken ist von entscheidender Bedeutung, wenn Sie die Datenduplizierung und Knotenreplikation verwenden. Vermeiden Sie die Verwendung von SATA-Laufwerken (SATA = Serial Advanced Technology Attachment) und PATA-Laufwerken (PATA = Parallel Advanced Technology Attachment). Ausführliche Informationen und weitere Tipps finden Sie in: <ul style="list-style-type: none"> <li>◦ "Planung für Platten für die Serverdatenbank"</li> <li>◦ "Planung für die Auswahl des korrekten Speichertechnologietyps"</li> </ul> |
| Stellen Sie sicher, dass das Serversystem über genügend Speicher verfügt.  | Überprüfen Sie die Betriebssystemvoraussetzungen in Technote 1243309. Höhere Arbeitslasten erfordern mehr als die Mindestvoraussetzungen. Erweiterte Funktionen wie beispielsweise Datenduplizierung und Knotenreplikation können mehr Speicher als den Mindestspeicher erfordern, der im Dokument mit den Systemvoraussetzungen angegeben ist. <p>Wenn Sie die Ausführung mehrerer Instanzen planen, ist für jede Instanz der für einen einzelnen Server aufgelistete Speicher erforderlich. Multiplizieren Sie den für einen einzelnen Server erforderlichen Speicher mit der Anzahl der für das System geplanten Instanzen.</p> |

| Bewährtes Verfahren   | Weitere Informationen  |
|---|--|
| Trennen Sie die Serverdatenbank, die aktive Protokolldatei, das Archivprotokoll und die Plattenspeicherpools voneinander.   | <p>Stellen Sie alle IBM Spectrum Protect-Speicherressourcen auf unterschiedliche Platten. Trennen Sie Speicherpoolplatten von den Platten für die Serverdatenbank und die Protokolle.</p> <p>Speicherpooloperationen können Datenbankoperationen beeinträchtigen, wenn sich die Speicherpools und die Datenbank auf denselben Platten befinden. Im Idealfall werden auch die Serverdatenbank und die Protokolle voneinander getrennt.</p> <p>Ausführliche Informationen und weitere Tipps finden Sie in:</p> <ul style="list-style-type: none"> <li>o "Planung für Platten für die Serverdatenbank"</li> <li>o "Planung für Platten für das Serverwiederherstellungsprotokoll"</li> <li>o "Planung für Speicherpools auf DISK- oder FILE-Einheiten"</li> </ul> |
| Verwenden Sie mindestens vier Verzeichnisse für die Serverdatenbank. Verwenden Sie für größere Server oder Server, die erweiterte Funktionen verwenden, acht Verzeichnisse.   | <p>Stellen Sie jedes Verzeichnis auf eine LUN, die von anderen LUNs und von anderen Anwendungen getrennt ist.</p> <p>Ein Server wird als großer Server betrachtet, wenn seine Datenbank größer als 2 TB ist oder wahrscheinlich diese Größe erreichen wird. Verwenden Sie für derartige Server acht Verzeichnisse.</p> <p>Siehe "Planung für Platten für die Serverdatenbank".</p>   |
| Wenn Sie die Datendeduplizierung und/oder die Knotenreplikation verwenden, beachten Sie die Richtlinien für die Datenbankkonfiguration und andere Elemente.   | <p>Konfigurieren Sie den Server gemäß den Richtlinien, da die Datenbank in Bezug darauf, wie gut die Ausführung des Servers bei Verwendung dieser Funktionen ist, extrem wichtig ist. Ausführliche Informationen und weitere Tipps finden Sie in:</p> <ul style="list-style-type: none"> <li>o Prüfliste für Datendeduplizierung</li> <li>o Prüfliste für Knotenreplikation</li> </ul>   |
| Beachten Sie bei Speicherpools, die Einheitenklassen des Typs FILE verwenden, die Richtlinien für die Größe von Speicherpooldatenträgern. In der Regel sind Datenträger mit einer Größe von 50 GB am besten geeignet. | <p>Lesen Sie die Informationen in Optimale Anzahl und Größe von Datenträgern für Speicherpools, die Platten verwenden zur Bestimmung der Datenträgergröße.</p> <p>Konfigurieren Sie Speicherpools und Dateisysteme auf der Basis der Anforderungen in Bezug auf den Durchsatz und nicht nur auf der Basis der Kapazitätsanforderungen.</p> <p>Trennen Sie die Speichereinheiten, die von IBM Spectrum Protect verwendet werden, von anderen Anwendungen mit hoher Ein-/Ausgabe und stellen Sie sicher, dass der Durchsatz für diesen Speicher ausreichend ist.</p> <p>Weitere Informationen finden Sie in Prüfliste für Speicherpools auf FILE- oder DISK-Einheiten.</p>   |
| Planen Sie IBM Spectrum Protect-Clientoperationen und -Serververwaltungsaktivitäten, um eine Überschneidung von Operationen zu verhindern oder auf ein Mindestmaß zu reduzieren.                                      | <p>Weitere ausführliche Informationen liefern die folgenden Themen:</p> <ul style="list-style-type: none"> <li>o Zeitplan für tägliche Operationen optimieren</li> <li>o Prüfliste für Serverkonfiguration</li> </ul>  |
| Überwachen Sie Operationen kontinuierlich.  | <p>Die Überwachung ermöglicht es Ihnen, Probleme frühzeitig erkennen und Ursachen leichter ermitteln zu können. Bewahren Sie Aufzeichnungen von Überwachungsberichten bis zu einem Jahr lang auf, um Trends schneller erkennen und Wachstum besser planen zu können. Siehe Umgebung im Hinblick auf die Leistung überwachen und verwalten.</p>   |

## Windows: Systemmindestvoraussetzungen für Windows-Systeme

Für den Server können sehr viel Speicherplatz, eine große Netzbandbreite und viele Prozessorressourcen erforderlich sein. In vielen Fällen ist die Leistung des Servers am besten, wenn andere Anwendungen nicht auf demselben System installiert sind.



## Hardware- und Softwarevoraussetzungen für die IBM Spectrum Protect-Serverinstallation

Die folgenden Tabellen enthalten die Mindesthardware- und -softwarevoraussetzungen für die Installation eines IBM Spectrum Protect-Servers. Verwenden Sie diese Voraussetzungen als Ausgangspunkt für Systeme ohne Datendeduplizierung. Die optimale IBM Spectrum Protect-Umgebung ist mit Datendeduplizierung mithilfe der IBM Spectrum Protect Blueprints konfiguriert. Die neuesten Informationen zu den Systemvoraussetzungen finden Sie unter Technote 1243309.

### Hardwarevoraussetzungen

In Tabelle 1 sind die Hardwaremindestvoraussetzungen für den Server beschrieben. Wenn der Server die Mindestvoraussetzungen nicht erfüllt, schlägt die Installation fehl. Weitere Informationen zur Planung des Plattenspeicherplatzes finden Sie in Windows: Kapazitätsplanung.

Tabelle 1. Hardwarevoraussetzungen

| Hardwaretyp     | Hardwarevoraussetzungen  |
|-----------------|--|
| Hardware        | Ein AMD64- oder Intel EMT-64-Prozessor   |
| Plattenspeicher | <p>Folgende Mindestwerte für den Plattenspeicher:</p> <ul style="list-style-type: none"><li>• Mindestens 7,5 GB freier Plattenspeicher für eine Standardinstallation</li><li>• 60 MB im temporären Verzeichnisbereich</li><li>• 2 GB Partitionsgröße im Laufwerk C:\</li><li>• 300 MB im Instanzverzeichnis</li><li>• 2 GB für den Bereich der gemeinsam genutzten Ressourcen</li></ul> <p>Für den Fall, dass ein Problem auftritt und eine Diagnose erforderlich ist, wird empfohlen, temporären oder anderen Speicherbereich für ein FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) oder für andere temporäre Verwendungszwecke (z. B. für die Erfassung von Traceprotokollen) auf dem System verfügbar zu haben.</p> <p>Sehr viel zusätzlicher Plattenspeicherplatz ist für Datenbank- und Protokolldateien erforderlich. Die Größe der Datenbank ist von der Anzahl der zu speichernden Clientdateien und von der Methode abhängig, mit der sie vom Server verwaltet werden. Der Standardspeicherbereich der aktiven Protokolldatei beträgt 16 GB, das für die meisten Arbeitslasten und Konfigurationen benötigte Minimum. Wenn Sie die aktive Protokolldatei erstellen, benötigen Sie mindestens 64 GB für die Replikation. Wird sowohl Replikation als auch Datendeduplizierung verwendet, erstellen Sie eine aktive Protokolldatei mit einer Größe von 128 GB. Ordnen Sie mindestens die dreifache Größe des Standardspeicherbereichs der aktiven Protokolldatei für das Archivprotokoll zu (48 GB). Stellen Sie sicher, dass Sie über ausreichende Ressourcen verfügen, wenn Sie die Datendeduplizierung verwenden oder eine hohe Clientauslastung erwarten.</p> <p>Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN.</p> <p>Lesen Sie den Abschnitt zur Windows: Kapazitätsplanung, um weitere Informationen zum Plattenspeicherplatz zu erhalten.</p> |
| Hauptspeicher   | <p>Folgende Mindestwerte für den Hauptspeicher:</p> <ul style="list-style-type: none"><li>• 16 GB für Standardserverbetrieb ohne Datendeduplizierung und Knotenreplikation</li><li>• 24 GB für Datendeduplizierung oder Knotenreplikation</li><li>• 32 GB für Knotenreplikation mit Datendeduplizierung</li></ul> <p>Speziellere Angaben zum Speicherbedarf für große Datenbanken und höhere Aufnahmefähigkeit finden Sie in der Tabelle für die Serverspeicheroptimierung von IBM Spectrum Protect.</p> <p>Ausführliche Informationen zum Speicherbedarf bei Verwendung der Datendeduplizierung finden Sie unter IBM Spectrum Protect Blueprint für Ihr Betriebssystem.</p>   |

### Softwarevoraussetzungen

In Tabelle 2 sind die für einen Server auf einem Windows-System erforderlichen Softwaremindestvoraussetzungen beschrieben.

Tabelle 2. Softwarevoraussetzungen

| Softwaretyp | Softwaremindestvoraussetzungen |
|-------------|--------------------------------|
|-------------|--------------------------------|

| Softwaretyp           | Softwaremindestvoraussetzungen   |
|-----------------------|--|
| Betriebssystem        | <p>Eines der folgenden Betriebssysteme:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows Server 2012: Standard, Enterprise oder Datacenter Edition (64-Bit)</li> <li>• Microsoft Windows Server 2012 R2 (64-Bit)</li> <li>• Microsoft Windows Server 2016</li> </ul>   |
| Übertragungsprotokoll | <p>Mindestens eins der folgenden Übertragungsprotokolle (standardmäßig mit den aktuellen Windows-Betriebssystemen installiert):</p> <ul style="list-style-type: none"> <li>• Benannte Pipes</li> <li>• TCP/IP Version 4 oder Version 6</li> </ul>  |
| Einheitentreiber      | <p>Der für Laufwerke und Bandarchive eines anderen Herstellers erforderliche IBM Spectrum Protect-Durchgriffseinheitentreiber. Der systemeigene Windows-Einheitentreiber wird für Bandlaufwerke und Bandarchive empfohlen. Andernfalls kann der IBM Spectrum Protect-Kerneinheitentreiber verwendet werden.</p> <p>Für die Bandarchive bzw. Bandlaufwerke IBM® 3590, 3592 oder Ultrium sind die IBM Einheitentreiber erforderlich. Installieren Sie die aktuellen Einheitentreiber. IBM-Treiberpakete finden Sie bei Fix Central.</p> <p>Konfigurieren Sie die Einheitentreiber, bevor Sie den Server für Bandeinheiten verwenden.</p>   |
| Sonstige Software     | <p>Für Windows 2012, Windows 2012 R2 und Windows 2016 muss .NET Framework 3.5 installiert und aktiviert sein.</p> <p>Die folgenden Richtlinien für die Benutzerkontensteuerung müssen inaktiviert werden:</p> <ul style="list-style-type: none"> <li>• Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto</li> <li>• Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen</li> </ul> <p>Um IBM Spectrum Protect-Benutzer mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol) zu authentifizieren, müssen Sie einen der folgenden Verzeichnisse verwenden:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server Version 6.3</li> <li>• IBM Security Directory Server Version 6.4</li> </ul> |

## Windows: IBM Installation Manager

IBM Spectrum Protect verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositories installiert oder aktualisiert werden können.

Wenn die erforderliche Version von IBM Installation Manager noch nicht installiert ist, wird sie automatisch installiert oder aktualisiert, wenn Sie IBM Spectrum Protect installieren. Die Software muss auf dem System installiert bleiben, damit IBM Spectrum Protect später nach Bedarf aktualisiert oder deinstalliert werden kann.

Die folgende Liste enthält Erläuterungen einiger Begriffe, die in IBM Installation Manager verwendet werden:

### Angebot

Eine installierbare Einheit eines Softwareprodukts.

Das Angebot 'IBM Spectrum Protect' enthält alle Datenträger, die IBM Installation Manager für die Installation von IBM Spectrum Protect benötigt.

### Paket

Die Gruppe der Softwarekomponenten, die für die Installation eines Angebots benötigt werden.

Das IBM Spectrum Protect-Paket enthält folgende Komponenten:

- Installationsprogramm IBM Installation Manager
- Das Angebot 'IBM Spectrum Protect'

### Paketgruppe

Eine Gruppe von Paketen mit demselben übergeordneten Verzeichnis.

Die Standardpaketgruppe für das IBM Spectrum Protect-Paket ist `IBM Installation Manager`.

**Repository**

Ein ferner oder lokaler Speicherbereich für Daten und andere Anwendungsressourcen.

Das IBM Spectrum Protect-Paket wird in einem Repository in IBM Fix Central gespeichert.


**Verzeichnis für gemeinsam genutzte Ressourcen**

Ein Verzeichnis, das Softwaredateien oder Plug-ins enthält, die von Paketen gemeinsam genutzt werden.

In dem Verzeichnis für gemeinsam genutzte Ressourcen speichert IBM Installation Manager installationsbezogene Dateien, darunter Dateien, die für das Rollback zu einer vorherigen Version von IBM Spectrum Protect verwendet werden.

## Windows: Arbeitsblätter für Planungsdetails für den Server

Sie können die Arbeitsblätter für die Planung der Größe und der Position des für den IBM Spectrum Protect-Server benötigten Speichers verwenden. Sie können darauf auch Namen und Benutzer-IDs aufzeichnen.

 **Windows-Betriebssystemeinschränkung:** Wenn Sie ein FAT- oder FAT32- oder ein NTFS-Dateisystemformat verwenden, können Sie nicht das Stammverzeichnis dieses Systems als Position eines Datenbank- oder Protokollverzeichnisses angeben (FAT = File Allocation Table, NTFS = New Technology File System). Stattdessen müssen Sie mindestens ein Unterverzeichnis in dem Stammverzeichnis erstellen. Dann erstellen Sie die Datenbankverzeichnisse und Protokollverzeichnisse in den Unterverzeichnissen.

| Element  | Erforderlicher Speicherbereich | Anzahl der Verzeichnisse | Position der Verzeichnisse |
|--|--------------------------------|--------------------------|----------------------------|
| Die Datenbank  |                                |                          |                            |
| Aktive Protokolldatei  |                                |                          |                            |
| Archivprotokoll  |                                |                          |                            |
| Optional: Protokollspiegel für die aktive Protokolldatei                         |                                |                          |                            |
| Optional: Sekundäres Archivprotokoll (Übernahmeverzeichnis für Archivprotokolle) |                                |                          |                            |

| Element   | Namen und Benutzer-IDs | Position |
|---|------------------------|----------|
| Die <i>Instanzbenutzer-ID</i> für den Server. Mit dieser ID starten Sie den IBM Spectrum Protect-Server und führen ihn aus.   |                        |          |
| Das <i>Ausgangsverzeichnis</i> des Servers. In diesem Verzeichnis befindet sich die Instanzbenutzer-ID.   |                        |          |
| Der Datenbankinstanzname  |                        |          |
| Das <i>Instanzverzeichnis</i> für den Server. Dieses Verzeichnis enthält spezielle Dateien für diese Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien). |                        |          |
| Der Servername; verwenden Sie einen eindeutigen Namen für jeden Server.   |                        |          |

## Windows: Kapazitätsplanung

Zur Kapazitätsplanung für IBM Spectrum Protect gehört die Verwaltung von Ressourcen wie z. B. die Datenbank, das Wiederherstellungsprotokoll und der Bereich für gemeinsam genutzte Ressourcen. Sie müssen den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll schätzen, um die Ressourcen als Teil der Kapazitätsplanung zu maximieren. Der verfügbare Speicherplatz für den Bereich für gemeinsam genutzte Ressourcen muss für jede Installation bzw. jedes Upgrade ausreichen.

- **Windows: Speicherbedarf für die Datenbank schätzen**  
Sie können den Speicherbedarf für die Datenbank auf der Basis der maximalen Anzahl Dateien schätzen, die sich gleichzeitig im Serverspeicher befinden können, oder auf der Basis der Speicherpoolkapazität.
- **Windows: Speicherplatzbedarf für das Wiederherstellungsprotokoll**  
In IBM Spectrum Protect beinhaltet der Begriff *Wiederherstellungsprotokoll* die aktive Protokolldatei, das Archivprotokoll, den Spiegel der aktiven Protokolldatei und das Archivübernahmeprotokoll. Der für das Wiederherstellungsprotokoll erforderliche Speicherbereich ist von verschiedenen Faktoren, wie z. B. dem Umfang der Clientaktivität mit dem Server, abhängig.
- **Windows: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen**  
Um den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei zu bestimmen, geben Sie den Befehl QUERY LOG ein. Um die Speicherauslastung in der Datenbank und den Wiederherstellungsprotokollen zu überwachen, können Sie auch das Aktivitätenprotokoll auf Nachrichten überprüfen.
- **Windows: Rollbackdateien der Installation löschen**  
Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, löschen, um Speicherplatz im Verzeichnis für gemeinsam genutzte Ressourcen freizugeben. Zu den Dateitypen, die Sie löschen können, gehören z. B. Dateien, die für eine Rollbackoperation benötigt wurden.

## Windows: Speicherbedarf für die Datenbank schätzen

---

Sie können den Speicherbedarf für die Datenbank auf der Basis der maximalen Anzahl Dateien schätzen, die sich gleichzeitig im Serverspeicher befinden können, oder auf der Basis der Speicherpoolkapazität.

### Informationen zu diesem Vorgang

---

Anfänglich sollte mindestens 25 GB Speicherplatz in der Datenbank verwendet werden. Stellen Sie entsprechend Speicherplatz im Dateisystem bereit. Eine Datenbankgröße von 25 GB ist für eine Testumgebung oder eine Umgebung, die nur einen Speicherarchivmanager umfasst, ausreichend. Für einen Produktionsserver, der Clientlasten unterstützt, sollte die Datenbank größer sein. Wenn Sie Plattenspeicherpools (DISK) mit wahlfreiem Zugriff verwenden, ist mehr Datenbank- und Protokollspeicherbereich erforderlich als für Speicherpools mit sequenziellem Zugriff.

Die maximale Größe der IBM Spectrum Protect-Datenbank beträgt 6 TB.

Informationen zur Festlegung der Größe einer Datenbank in einer Produktionsumgebung, die auf der Anzahl Dateien und der Speicherpoolgröße basiert, enthalten die folgenden Abschnitte.

- **Windows: Speicherbedarf für die Datenbank auf der Basis der Anzahl Dateien schätzen**  
Wenn die maximale Anzahl Dateien, die sich zu einem bestimmten Zeitpunkt im Serverspeicher befinden, geschätzt werden kann, können Sie diese Zahl verwenden, um den Speicherbedarf für die Datenbank zu schätzen.
- **Windows: Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität schätzen**  
Um den Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität zu schätzen, verwenden Sie ein Verhältnis von 1-5 %. Sind beispielsweise 200 TB Speicherpoolkapazität erforderlich, sollte die Größe der Datenbank erwartungsgemäß zwischen 2 und 10 TB betragen. Als allgemeine Regel gilt: Wählen Sie die Größe ihrer Datenbank so groß wie möglich, um zu verhindern, dass der Speicherplatz knapp wird. Wenn der Speicherplatz knapp wird, können Serveroperationen und Clientspeicheroperationen fehlschlagen.
- **Windows: Datenbankmanager und temporärer Speicherbereich**  
Der Datenbankmanager des IBM Spectrum Protect-Servers verwaltet System Speicher und Plattenspeicher für die Datenbank und ordnet diesen Speicher zu. Der benötigte Datenbankspeicherbereich ist von der Größe des verfügbaren Systemspeichers und von der Serverauslastung abhängig.

## Windows: Speicherbedarf für die Datenbank auf der Basis der Anzahl Dateien schätzen

---

Wenn die maximale Anzahl Dateien, die sich zu einem bestimmten Zeitpunkt im Serverspeicher befinden, geschätzt werden kann, können Sie diese Zahl verwenden, um den Speicherbedarf für die Datenbank zu schätzen.

### Informationen zu diesem Vorgang

---

Um den Speicherbedarf auf der Basis der maximalen Anzahl Dateien im Serverspeicher zu schätzen, verwenden Sie die folgenden Richtlinien:

- 600-1000 Byte für jede gespeicherte Version einer Datei einschließlich der Imagesicherungen.  
Einschränkung: Diese Richtlinie umfasst nicht den Speicherplatz, der während der Datendeduplizierung verwendet wird.
- 100-200 Byte für jede Datei im Cache, jede Kopierspeicherpooldatei, jede Datei im Pool für aktive Daten und jede deduplizierte Datei.

- Zusätzlicher Speicherbereich ist für die Datenbankoptimierung erforderlich, um variable Datenzugriffsmuster und die Server-Back-End-Verarbeitung von Daten zu unterstützen. Die Größe des zusätzlichen Speicherplatzes entspricht 50 % der Schätzung für die Gesamtanzahl Byte für Dateiobjekte.

In dem folgenden Beispiel für einen einzelnen Client basieren bei Berechnungen auf den Maximalwerten in den vorhergehenden Richtlinien. Bei den Beispielen wird die mögliche Verwendung der Dateiaggregation nicht berücksichtigt. Im Allgemeinen wird durch das Aggregieren kleiner Dateien der erforderliche Speicherplatz in der Datenbank reduziert. Die Dateiaggregation betrifft keine speicherwarteten Dateien.

## Vorgehensweise

1. Berechnen Sie die Anzahl Dateiversionen. Addieren Sie alle folgenden Werte, um die Anzahl Dateiversionen zu erhalten:
  - a. Berechnen Sie die Anzahl gesicherter Dateien. Beispiel: Möglicherweise werden bis zu 500.000 Clientdateien gleichzeitig gesichert. In diesem Beispiel sind die Speichermaßnahmen so definiert, dass maximal drei Kopien gesicherter Dateien aufbewahrt werden:
 
$$500.000 \text{ Dateien} * 3 \text{ Kopien} = 1.500.000 \text{ Dateien}$$
  - b. Berechnen Sie die Anzahl Archivierungsdateien. Beispiel: Bis zu 100.000 Clientdateien können archivierte Kopien sein.
  - c. Berechnen Sie die Anzahl speicherwarteter Dateien. Beispiel: Bis zu 200.000 Clientdateien können von Client-Workstations umgelagert werden.

Bei Verwendung von 1000 Byte pro Datei beträgt der Gesamtspeicherplatz in der Datenbank, der für die zu dem Client gehörigen Dateien erforderlich ist, 1,8 GB:

$$(1.500.000 + 100.000 + 200.000) * 1000 = 1,8 \text{ GB}$$

2. Berechnen Sie die Anzahl Dateien im Cache, Kopierspeicherpooldateien, Dateien im Pool für aktive Daten und deduplizierter Dateien:
  - a. Berechnen Sie die Anzahl der Cachekopien. Beispiel: In einem Plattenspeicherpool mit 5 GB Kapazität ist Caching aktiviert. Die obere Umlagerungsschwelle des Pools ist 90 % und die untere Umlagerungsschwelle ist 70 %. Das heißt 20 % des Plattenpools (oder 1 GB) wird von Cachedateien belegt. Wenn die durchschnittliche Dateigröße ungefähr 10 KB beträgt, enthält der Cache zu jedem beliebigen Zeitpunkt etwa 100.000 Dateien:
 
$$100.000 \text{ Dateien} * 200 \text{ Byte} = 19 \text{ MB}$$
  - b. Berechnen Sie die Anzahl Kopierspeicherpooldateien. Alle primären Speicherpools werden im Kopierspeicherpool gesichert:
 
$$(1.500.000 + 100.000 + 200.000) * 200 \text{ Byte} = 343 \text{ MB}$$
  - c. Berechnen Sie die Anzahl Dateien im Speicherpool für aktive Daten. Alle aktiven Clientsicherungsdaten in primären Speicherpools werden in den Speicherpool für aktive Daten kopiert. Angenommen, es sind 500.000 Versionen der 1.500.000 Sicherungsdateien im primären Speicherpool aktiv:
 
$$500.000 * 200 \text{ Byte} = 95 \text{ MB}$$
  - d. Berechnen Sie die Anzahl deduplizierter Dateien. Angenommen, ein deduplizierter Speicherpool enthält 50.000 Dateien:
 
$$50.000 * 200 \text{ Byte} = 10 \text{ MB}$$

Auf der Basis der vorhergehenden Berechnungen sind etwa 0,5 GB zusätzlicher Speicherplatz in der Datenbank für die Cachedateien, die Kopierspeicherpooldateien, die Dateien im Pool für aktive Daten und die deduplizierten Dateien des Clients erforderlich.

3. Berechnen Sie den zusätzlichen Speicherplatz, der für die Datenbankoptimierung benötigt wird. Um optimalen Datenzugriff und optimale Verwaltung durch den Server bereitzustellen, ist zusätzlicher Speicherplatz in der Datenbank erforderlich. Die Größe des zusätzlichen Speicherplatzes in der Datenbank beträgt 50 % des Gesamtspeicherbedarfs für Dateiobjekte.

$$(1,8 + 0,5) * 50 \% = 1,2 \text{ GB}$$

4. Die Gesamtgröße des für den Client erforderlichen Datenbankspeicherbereichs berechnen. Die Gesamtgröße beträgt ca. 3,5 GB:

$$1,8 + 0,5 + 1,2 = 3,5 \text{ GB}$$

5. Berechnen Sie den Gesamtspeicherplatz in der Datenbank, der für alle Clients erforderlich ist. Wenn der Client, der in den vorhergehenden Berechnungen verwendet wurde, ein typischer Client ist und Sie beispielsweise über 500 Clients verfügen, können Sie den Gesamtspeicherplatz in der Datenbank, der für alle Clients erforderlich ist, mithilfe der folgenden Berechnung schätzen:

$$500 * 3,5 = 1,7 \text{ TB}$$

## Ergebnisse

Tipp: In den Beispielen oben handelt es sich bei den Ergebnissen um Schätzungen. Die tatsächliche Größe der Datenbank kann aufgrund von Faktoren wie beispielsweise der Anzahl Verzeichnisse und der Länge der Pfad- und Dateinamen von der geschätzten Größe abweichen. Sie sollten die Datenbank regelmäßig überwachen und die Größe wie erforderlich anpassen.

## Nächste Schritte

Während des normalen Betriebs erfordert der IBM Spectrum Protect-Server möglicherweise temporären Speicherplatz in der Datenbank. Dieser Speicherplatz wird aus den folgenden Gründen benötigt:

- Zum Speichern der Ergebnisse der Sortierung oder Änderung der Reihenfolge, die noch nicht in der Datenbank aufbewahrt und in der Datenbank nicht unmittelbar optimiert werden. Die Ergebnisse werden vorübergehend in der Datenbank zur Verarbeitung gespeichert.
- Zum Erteilen des Verwaltungszugriffs auf die Datenbank über eine der folgenden Methoden:
  - Ein DB2-ODBC-Client (ODBC = Open Database Connectivity)
  - Ein Oracle-JDBC-Client (JDBC = Java™ Database Connectivity)
  - SQL (Structured Query Language) für den Server über die Befehlszeile eines Verwaltungsclients

Erwägen Sie die Verwendung von zusätzlichen 50 GB an temporärem Speicherplatz pro 500 GB Speicherbereich für Dateiobjekte und Optimierung. Siehe die Richtlinien in der folgenden Tabelle. In dem Beispiel, das im vorhergehenden Schritt verwendet wurde, sind insgesamt 1,7 TB Speicherplatz in der Datenbank für Dateiobjekte und die Optimierung für 500 Clients erforderlich. Auf der Basis dieser Berechnung sind 200 GB für temporären Speicherplatz erforderlich. Der erforderliche Gesamt Speicherplatz in der Datenbank beträgt 1,9 TB.

| Datenbankgröße      | Mindestens erforderlicher temporärer Speicherplatz |
|---------------------|--|
| < 500 GB            | 50 GB  |
| ≥ 500 GB und < 1 TB | 100 GB   |
| ≥ 1 TB und < 1,5 TB | 150 GB   |
| ≥ 1,5 und < 2 TB    | 200 GB   |
| ≥ 2 und < 3 TB      | 250-300 GB   |
| ≥ 3 und < 4 TB      | 350-400 GB   |

## Windows: Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität schätzen

Um den Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität zu schätzen, verwenden Sie ein Verhältnis von 1-5 %. Sind beispielsweise 200 TB Speicherpoolkapazität erforderlich, sollte die Größe der Datenbank erwartungsgemäß zwischen 2 und 10 TB betragen. Als allgemeine Regel gilt: Wählen Sie die Größe ihrer Datenbank so groß wie möglich, um zu verhindern, dass der Speicherplatz knapp wird. Wenn der Speicherplatz knapp wird, können Serveroperationen und Clientspeicheroperationen fehlschlagen.

## Windows: Datenbankmanager und temporärer Speicherbereich

Der Datenbankmanager des IBM Spectrum Protect-Servers verwaltet Systemspeicher und Plattenspeicher für die Datenbank und ordnet diesen Speicher zu. Der benötigte Datenbankspeicherbereich ist von der Größe des verfügbaren Systemspeichers und von der Serverauslastung abhängig.

Der Datenbankmanager sortiert Daten in einer bestimmten Reihenfolge, gemäß der SQL-Anweisung, mit der Sie die Daten anfordern. Je nach Auslastung des Servers und wenn es mehr Daten gibt, als der Datenbankmanager verwalten kann, werden die (der Reihenfolge nach sortierten) Daten temporärem Plattenspeicher zugeordnet. Daten werden temporärem Plattenspeicher zugeordnet, wenn die Ergebnismenge sehr umfangreich ist. Der Datenbankmanager verwaltet den verwendeten Speicher dynamisch, wenn Daten temporärem Plattenspeicher zugeordnet werden.

Bei der Verfallsverarbeitung kann beispielsweise eine umfangreiche Ergebnismenge generiert werden. Wenn der Systemspeicher in der Datenbank zur Speicherung der Ergebnismenge nicht ausreicht, wird ein Teil der Daten temporärem Plattenspeicher zugeordnet. Wenn während der Verfallsverarbeitung ein Knoten oder ein Dateibereich ausgewählt wird, der für die Verarbeitung zu groß ist, kann der Datenbankmanager die Daten im Speicher nicht sortieren. Der Datenbankmanager muss temporären Speicherbereich zum Sortieren der Daten verwenden.

Bei der Ausführung von Datenbankoperationen sollten Sie in den folgenden Szenarios eine Erweiterung des Speicherplatzes in der Datenbank vornehmen:

- Der Speicherbereich der Datenbank ist klein und die Serveroperation, die temporären Speicherbereich benötigt, belegt den verbleibenden freien Speicherbereich.
- Die Dateibereiche sind groß oder den Dateibereichen ist eine Maßnahme zugeordnet, durch die viele Dateiversionen erstellt werden.
- Der IBM Spectrum Protect-Server muss mit begrenztem Speicher ausgeführt werden. Die Datenbank verwendet den Hauptspeicher des IBM Spectrum Protect-Servers für Datenbankoperationen. Ist der verfügbare Speicher jedoch nicht ausreichend, ordnet der IBM Spectrum Protect-Server der Datenbank temporären Speicherbereich auf Platte zu. Wenn beispielsweise 10G Speicher zur Verfügung stehen und Datenbankoperationen 12G Speicher benötigen, verwendet die Datenbank temporären Speicherbereich.
- Bei der Implementierung eines IBM Spectrum Protect-Servers wird ein Fehler aufgrund fehlenden Datenbankspeicherbereichs (*out of database space*) angezeigt. Überwachen Sie das Serveraktivitätenprotokoll auf Nachrichten, die sich auf den Datenbankspeicherbereich beziehen.

Wichtig: Sie dürfen die DB2-Software, die mit IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht verändern. Führen Sie keine Installation bzw. kein Upgrade auf eine andere Version, ein anderes Release oder ein anderes Fixpack der DB2-Software durch, um eine Beschädigung der Datenbank zu vermeiden.

## Windows: Speicherplatzbedarf für das Wiederherstellungsprotokoll

---

In IBM Spectrum Protect beinhaltet der Begriff *Wiederherstellungsprotokoll* die aktive Protokolldatei, das Archivprotokoll, den Spiegel der aktiven Protokolldatei und das Archivübernahmeprotokoll. Der für das Wiederherstellungsprotokoll erforderliche Speicherbereich ist von verschiedenen Faktoren, wie z. B. dem Umfang der Clientaktivität mit dem Server, abhängig.

- Windows: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll  
Wenn Sie den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll schätzen, müssen Sie einigen zusätzlichen Speicherbereich für gelegentlich auftretende hohe Lasten und Übernahmesituationen einkalkulieren.
- Windows: Speicherbereich des Spiegels für aktive Protokolldateien  
Die aktive Protokolldatei kann gespiegelt werden, sodass die gespiegelte Kopie verwendet werden kann, falls die aktiven Protokolldateien nicht gelesen werden können. Es kann nur ein einziger Spiegel der aktiven Protokolldatei vorhanden sein.
- Windows: Speicherbereich des Übernahmeverzeichnisses für Archivprotokolle  
Das Übernahmeverzeichnis für Archivprotokolle wird vom Server verwendet, wenn der Speicherbereich des Verzeichnisses für Archivprotokolle nicht mehr ausreicht.

## Windows: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll

---

Wenn Sie den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll schätzen, müssen Sie einigen zusätzlichen Speicherbereich für gelegentlich auftretende hohe Lasten und Übernahmesituationen einkalkulieren.

In IBM Spectrum Protect-Servern der Version 7.1 und höher kann die aktive Protokolldatei eine maximale Größe von 512 GB haben. Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist.

Berücksichtigen Sie bei der Schätzung der Größe der aktiven Protokolldatei die folgenden allgemeinen Richtlinien:

- Die empfohlene Anfangsgröße für die aktive Protokolldatei ist 16 GB.
- Stellen Sie sicher, dass die aktive Protokolldatei mindestens groß genug ist, um die gleichzeitig ablaufende Aktivität handhaben zu können, die der Server in der Regel handhabt. Versuchen Sie als Vorsichtsmaßnahme das größte Arbeitsvolumen zu schätzen, das der Server jeweils handhabt. Stellen Sie für die aktive Protokolldatei zusätzlichen Speicherbereich bereit, der, falls erforderlich, verwendet werden kann. Ziehen Sie 20 % zusätzlichen Speicherbereich in Betracht.
- Überwachen Sie den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei. Passen Sie die Größe der aktiven Protokolldatei wie erforderlich abhängig von Faktoren wie Clientaktivität und Ebene der Serveroperationen an.
- Stellen Sie sicher, dass das Verzeichnis, das die aktive Protokolldatei enthält, mindestens genauso groß wie die aktive Protokolldatei ist. Ein Verzeichnis, das größer als die aktive Protokolldatei ist, kann Übernahmesituationen handhaben, sollten diese auftreten.
- Stellen Sie sicher, dass das Dateisystem, das das Verzeichnis für aktive Protokolldateien enthält, über mindestens 8 GB freien Speicherbereich für Anforderungen zum Versetzen temporärer Protokolle verfügt.

Die vorgeschlagene Anfangsgröße für das Archivprotokoll beträgt 48 GB.

Das Archivprotokollverzeichnis muss groß genug sein, um die Protokolldateien aufnehmen zu können, die seit der vorherigen Gesamtsicherung generiert wurden. Wenn Sie beispielsweise täglich eine Gesamtsicherung der Datenbank ausführen, muss das Archivprotokollverzeichnis groß genug sein, um die Protokolldateien für die gesamte Clientaktivität aufnehmen zu können, die während

24 Stunden stattfindet. Um Speicherbereich wiederherzustellen, löscht der Server veraltete Archivprotokolldateien nach einer Gesamtsicherung der Datenbank. Wenn das Archivprotokollverzeichnis voll wird und kein Verzeichnis für Archivübernahmeprotokolle vorhanden ist, verbleiben Protokolldateien im Verzeichnis für aktive Protokolldateien. Diese Bedingung kann zur Folge haben, dass das Verzeichnis für aktive Protokolldateien vollständig gefüllt und der Server gestoppt wird. Bei einem Serverneustart wird ein Teil des vorhandenen Speicherbereichs für die aktive Protokolldatei freigegeben wird.

Nach der Installation des Servers können Sie die Archivprotokollauslastung und den Speicherbereich im Archivprotokollverzeichnis überwachen. Wenn sich der Speicherbereich im Archivprotokollverzeichnis füllt, können die folgenden Probleme auftreten:

- Der Server kann keine Datenbankgesamtsicherungen ausführen. Untersuchen und beheben Sie dieses Problem.
- Andere Anwendungen schreiben in das Archivprotokollverzeichnis und belegen den für das Archivprotokoll erforderlichen Speicherbereich. Nutzen Sie den Speicherbereich für das Archivprotokoll nicht gemeinsam mit anderen Anwendungen, einschließlich anderer IBM Spectrum Protect-Server. Stellen Sie sicher, dass jeder Server über eine separate Speicherposition verfügt, dessen Eigner dieser spezifische Server ist und der von diesem spezifischen Server verwaltet wird.
- Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen schätzen  
Grundlegende Clientspeicheroperationen umfassen Sicherung, Archivierung und Speicherbereichsverwaltung. Der Protokollspeicherbereich muss groß genug sein, um alle Speichertransaktionen handhaben zu können, die gleichzeitig aktiv sind.
- Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, schätzen  
Wenn Sie Clientoption RESOURCEUTILIZATION auf einen größeren Wert als den Standardwert gesetzt ist, erhöht sich die gleichzeitige Last für den Server.
- Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Operationen für gleichzeitiges Schreiben schätzen  
Wenn Clientsicherungsoperationen Speicherpools verwenden, die für gleichzeitiges Schreiben konfiguriert sind, erhöht sich der Protokollspeicherbedarf, der für jede Datei erforderlich ist.
- Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen und Serveroperationen schätzen  
Die Umlagerung von Daten in Serverspeicher, Identifikationsprozesse für die Datenduplizierung, Wiederherstellung und Verfallsverarbeitung werden möglicherweise gleichzeitig mit Clientspeicheroperationen ausgeführt. Verwaltungstasks wie Verwaltungsbefehle oder SQL-Abfragen von Verwaltungsclients können ebenfalls gleichzeitig mit Clientspeicheroperationen ausgeführt werden. Serveroperationen und Verwaltungstasks, die gleichzeitig ausgeführt werden, können den erforderlichen Speicherbereich für die aktive Protokolldatei erhöhen.
- Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls unter Bedingungen mit extremen Abweichungen schätzen  
Probleme in Bezug auf knapp werdenden Speicherbereich für die aktive Protokolldatei können auftreten, wenn viele Transaktionen, die sehr schnell ausgeführt werden, zusammen mit einigen Transaktionen vorhanden sind, deren Ausführung sehr viel länger dauern kann. Ein typischer Fall sind viele aktive Workstation- oder Dateiserversicherungssitzungen und wenige aktive Serversicherungssitzungen für sehr große Datenbanken. Trifft diese Situation für Ihre Umgebung zu, müssen Sie möglicherweise die Größe der aktiven Protokolldatei erhöhen, damit die Arbeit erfolgreich ausgeführt werden kann.
- Windows: Beispiel: Größe des Archivprotokolls bei Datenbankgesamtsicherungen schätzen  
Der IBM Spectrum Protect-Server löscht nicht benötigte Dateien nur dann aus dem Archivprotokoll, wenn eine Datenbankgesamtsicherung ausgeführt wird. Demzufolge müssen Sie beim Schätzen des für das Archivprotokoll erforderlichen Speicherbereichs auch die Häufigkeit, mit der Datenbankgesamtsicherungen ausgeführt werden, berücksichtigen.
- Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Datenduplizierungsoperationen schätzen  
Wenn Sie Daten deduplizieren, müssen Sie die Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll berücksichtigen.

## Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen schätzen

Grundlegende Clientspeicheroperationen umfassen Sicherung, Archivierung und Speicherbereichsverwaltung. Der Protokollspeicherbereich muss groß genug sein, um alle Speichertransaktionen handhaben zu können, die gleichzeitig aktiv sind.

Um die Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen zu bestimmen, führen Sie die folgende Berechnung aus:

Anzahl Clients x In jeder Transaktion gespeicherte Dateien  
x Für jede Datei benötigter Protokollspeicherbereich

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Grundlegende Clientspeicheroperationen

| Element | Beispielwerte | Beschreibung |
|---------|---------------|--------------|
|---------|---------------|--------------|



| Element  | Beispielwerte        | Beschreibung   |
|--|----------------------|--|
| Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern  | 300                  | Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.  |
| Anzahl während jeder Transaktion gespeicherter Dateien   | 4096                 | Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.  |
| Für jede Datei erforderlicher Protokollspeicherbereich   | 3053 Byte            | Der Wert von 3053 Byte für jede Datei in einer Transaktion gibt die Protokollbyte an, die erforderlich sind, wenn Dateien von einem Windows-Client gesichert werden, auf dem Dateinamen eine Länge von 12-120 Byte haben.<br><br>Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients für Sichern/Archivieren gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet. |
| Aktive Protokolldatei: vorgeschlagene Größe  | 19,5 GB <sup>1</sup> | Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.<br><br>(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 Byte = 3,5 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>3,5 + 16 = 19,5 GB  |
| Archivprotokoll: vorgeschlagene Größe  | 58,5 GB <sup>1</sup> | Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen.<br><br>3,5 x 3 = 10,5 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:<br><br>10,5 + 48 = 58,5 GB  |
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |                      |  |

## Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, schätzen

Wenn Sie Clientoption RESOURCEUTILIZATION auf einen größeren Wert als den Standardwert gesetzt ist, erhöht sich die gleichzeitige Last für den Server.

Um die Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, zu bestimmen, führen Sie die folgende Berechnung aus:

Anzahl Clients x Anzahl Sitzungen pro Client x Anzahl während jeder Transaktion gespeicherter Dateien x pro Datei erforderlicher Protokollspeicherbereich

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Mehrere Clientsitzungen

| Element   | Beispielwerte        |                     | Beschreibung  |
|---|----------------------|---------------------|---|
| Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern | 300                  | 1000                | Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.   |
| Mögliche Sitzungen für jeden Client   | 3                    | 3                   | Die Einstellung der Clientoption RESOURCEUTILIZATION ist größer als der Standardwert. Jede Clientsitzung führt maximal drei Sitzungen parallel aus.   |
| Anzahl während jeder Transaktion gespeicherter Dateien  | 4096                 | 4096                | Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.   |
| Für jede Datei erforderlicher Protokollspeicherbereich  | 3053                 | 3053                | <p>Der Wert von 3053 Byte für jede Datei in einer Transaktion gibt die Protokollbyte an, die erforderlich sind, wenn Dateien von einem Windows-Client gesichert werden, auf dem Dateinamen eine Länge von 12-120 Byte haben.</p> <p>Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.</p>   |
| Aktive Protokolldatei: vorgeschlagene Größe   | 26,5 GB <sup>1</sup> | 51 GB <sup>1</sup>  | <p>Die folgende Berechnung wurde für 300 Clients ausgeführt. 1 Gigabyte entspricht 1.073.741.824 Byte.</p> <p><math>(300 \text{ Clients} \times 3 \text{ Sitzungen pro Client} \times 4096 \text{ während jeder Transaktion gespeicherte Dateien} \times 3053 \text{ Byte pro Datei}) \div 1.073.741.824 = 10,5 \text{ GB}</math></p> <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:</p> <p><math>10,5 + 16 = 26,5 \text{ GB}</math></p> <p>Die folgende Berechnung wurde für 1000 Clients ausgeführt. 1 Gigabyte entspricht 1.073.741.824 Byte.</p> <p><math>(1000 \text{ Clients} \times 3 \text{ Sitzungen pro Client} \times 4096 \text{ während jeder Transaktion gespeicherte Dateien} \times 3053 \text{ Byte pro Datei}) \div 1.073.741.824 = 35 \text{ GB}</math></p> <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:</p> <p><math>35 + 16 = 51 \text{ GB}</math></p> |
| Archivprotokoll: vorgeschlagene Größe   | 79,5 GB <sup>1</sup> | 153 GB <sup>1</sup> | <p>Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, wird die Schätzung für die aktive Protokolldatei mit 3 multipliziert:</p> <p><math>10,5 \times 3 = 31,5 \text{ GB}</math></p> <p><math>35 \times 3 = 105 \text{ GB}</math></p> <p>Erhöhen Sie diese Werte um die vorgeschlagene Anfangsgröße von 48 GB:</p> <p><math>31,5 + 48 = 79,5 \text{ GB}</math></p> <p><math>105 + 48 = 153 \text{ GB}</math></p>  |

| Element   | Beispielwerte | Beschreibung |
|---|---------------|--------------|
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre aktive Protokolldatei und passen Sie die Größe, falls erforderlich, an.</p> |               |              |

## Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Operationen für gleichzeitiges Schreiben schätzen

Wenn Clientsicherungsoperationen Speicherpools verwenden, die für gleichzeitiges Schreiben konfiguriert sind, erhöht sich der Protokollspeicherbedarf, der für jede Datei erforderlich ist.

Der Protokollspeicherbereich, der für jede Datei erforderlich ist, erhöht sich um ungefähr 200 Byte für jeden Kopienspeicherpool, der für eine Operation für gleichzeitiges Schreiben verwendet wird. In dem Beispiel in der folgenden Tabelle werden Daten in einem primären Speicherpool und darüber hinaus in zwei Kopienspeicherpools gespeichert. Die geschätzte Protokollgröße erhöht sich für jede Datei um 400 Byte. Wenn Sie den vorgeschlagenen Wert von 3053 Byte Protokollspeicherbereich pro Datei verwenden, sind insgesamt 3453 Byte erforderlich.

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Operationen für gleichzeitiges Schreiben

| Element   | Beispielwerte      | Beschreibung  |
|---|--------------------|---|
| Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern | 300                | Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.   |
| Anzahl während jeder Transaktion gespeicherter Dateien  | 4096               | Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.   |
| Für jede Datei erforderlicher Protokollspeicherbereich  | 3453 Byte          | <p>3053 Byte plus 200 Byte für jeden Kopienspeicherpool.</p> <p>Der Wert von 3053 Byte für jede Datei in einer Transaktion stellt die Anzahl der Protokollbyte dar, die bei der Sicherung von Dateien auf einem Windows-Client benötigt werden, wo die Dateinamen 12 - 120 Byte haben.</p> <p>Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients für Sichern/Archivieren gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.</p> |
| Aktive Protokolldatei: vorgeschlagene Größe   | 20 GB <sup>1</sup> | <p>Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.</p> <p><math>(300 \text{ Clients} \times 4096 \text{ während jeder Transaktion gespeicherte Dateien} \times 3453 \text{ Byte pro Datei}) \div 1.073.741.824 \text{ Byte} = 4,0 \text{ GB}</math></p> <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>   |

| Element  | Beispielwerte      | Beschreibung   |
|--|--------------------|--|
| Archivprotokoll: vorgeschlagene Größe  | 60 GB <sup>1</sup> | <p>Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Speicherbedarf für das Archivprotokoll zu schätzen:</p> $4 \text{ GB} \times 3 = 12 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $12 + 48 = 60 \text{ GB}$ |
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |                    |  |

## Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen und Serveroperationen schätzen

Die Umlagerung von Daten in Serverspeicher, Identifikationsprozesse für die Datendeduplizierung, Wiederherstellung und Verfallsverarbeitung werden möglicherweise gleichzeitig mit Clientspeicheroperationen ausgeführt. Verwaltungstasks wie Verwaltungsbefehle oder SQL-Abfragen von Verwaltungsclients können ebenfalls gleichzeitig mit Clientspeicheroperationen ausgeführt werden. Serveroperationen und Verwaltungstasks, die gleichzeitig ausgeführt werden, können den erforderlichen Speicherbereich für die aktive Protokolldatei erhöhen.

Beispielsweise wird bei der Umlagerung von Dateien aus dem Speicherpool mit wahlfreiem Zugriff (DISK) in einem Plattenspeicherpool mit sequenziellem Zugriff (FILE) für jede Datei, die umgelagert wird, ungefähr 110 Byte Protokollspeicherbereich verwendet. Beispiel: Angenommen, es sind 300 Clients für Sichern/Archivieren vorhanden, von denen jeder 100.000 Dateien jede Nacht sichert. Die Dateien sind anfänglich in einem DISK-Speicherpool gespeichert und werden dann in einen FILE-Speicherpool umgelagert. Um die Größe des Speicherbereichs für die aktive Protokolldatei zu schätzen, die für die Datenumlagerung erforderlich ist, verwenden Sie die folgende Berechnung. Die Anzahl Clients in der Berechnung stellt die maximale Anzahl zu einem beliebigen Zeitpunkt dar, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern.

$300 \text{ Clients} \times 100.000 \text{ Dateien pro Client} \times 110 \text{ Byte} = 3,1 \text{ GB}$

Addieren Sie diesen Wert zu der Schätzung für die Größe der aktiven Protokolldatei, die für grundlegende Clientspeicheroperationen berechnet wurde.

## Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls unter Bedingungen mit extremen Abweichungen schätzen

Probleme in Bezug auf knapp werdenden Speicherbereich für die aktive Protokolldatei können auftreten, wenn viele Transaktionen, die sehr schnell ausgeführt werden, zusammen mit einigen Transaktionen vorhanden sind, deren Ausführung sehr viel länger dauern kann. Ein typischer Fall sind viele aktive Workstation- oder Dateiserversicherungssitzungen und wenige aktive Serversicherungssitzungen für sehr große Datenbanken. Trifft diese Situation für Ihre Umgebung zu, müssen Sie möglicherweise die Größe der aktiven Protokolldatei erhöhen, damit die Arbeit erfolgreich ausgeführt werden kann.

## Windows: Beispiel: Größe des Archivprotokolls bei Datenbankgesamticherungen schätzen

Der IBM Spectrum Protect-Server löscht nicht benötigte Dateien nur dann aus dem Archivprotokoll, wenn eine Datenbankgesamticherung ausgeführt wird. Demzufolge müssen Sie beim Schätzen des für das Archivprotokoll erforderlichen Speicherbereichs auch die Häufigkeit, mit der Datenbankgesamticherungen ausgeführt werden, berücksichtigen.

Wenn beispielsweise einmal pro Woche eine Datenbankgesamtssicherung ausgeführt wird, muss der Speicherbereich für das Archivprotokoll groß genug sein, um die Informationen einer vollständigen Woche im Archivprotokoll aufnehmen zu können.

Die unterschiedliche Größe des Archivprotokolls für täglich ausgeführte Datenbankgesamtssicherungen wird in dem Beispiel in der folgenden Tabelle gezeigt.

Tabelle 1. Datenbankgesamtssicherungen

| Element   | Beispielwerte       | Beschreibung  |
|---|---------------------|---|
| Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern | 300                 | Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.   |
| Anzahl während jeder Transaktion gespeicherter Dateien  | 4096                | Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.   |
| Für jede Datei erforderlicher Protokollspeicherbereich  | 3453 Byte           | 3053 Byte für jede Datei plus 200 Byte für jeden Kopierspeicherpool.<br><br>Der Wert von 3053 Byte für jede Datei in einer Transaktion stellt die Anzahl der Protokollbyte dar, die bei der Sicherung von Dateien auf einem Windows-Client benötigt werden, wo die Dateinamen 12 - 120 Byte haben.<br><br>Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet. |
| Aktive Protokolldatei: vorgeschlagene Größe   | 20 GB <sup>1</sup>  | Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.<br><br>(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3453 Byte pro Datei) ÷ 1.073.741.824 Byte = 4,0 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>4 + 16 = 20 GB   |
| Archivprotokoll: vorgeschlagene Größe bei einer Datenbankgesamtssicherung pro Tag                                       | 60 GB <sup>1</sup>  | Aufgrund der Voraussetzung, dass Archivprotokolle über drei Sicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen:<br><br>4 GB x 3 = 12 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:<br><br>12 + 48 = 60 GB   |
| Archivprotokoll: vorgeschlagene Größe bei einer Datenbankgesamtssicherung pro Woche                                     | 132 GB <sup>1</sup> | Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen. Multiplizieren Sie das Ergebnis mit der Anzahl Tage, die zwischen Datenbankgesamtssicherungen liegen.<br><br>(4 GB x 3 ) x 7 = 84 GB<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:<br><br>84 + 48 = 132 GB  |

| Element  | Beispielwerte | Beschreibung |
|--|---------------|--------------|
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Anfangsgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |               |              |

## Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Dateneduplizierungsoperationen schätzen

Wenn Sie Daten deduplizieren, müssen Sie die Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll berücksichtigen.

Die folgenden Faktoren haben Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll:

### Volumen der deduplizierten Daten

Welche Auswirkungen die Dateneduplizierung auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll hat, ist von dem Prozentsatz an Daten abhängig, der für die Deduplizierung auswählbar ist. Ist der Prozentsatz an Daten, die dedupliziert werden können, relativ hoch, ist mehr Protokollspeicherbereich erforderlich.

### Größe und Anzahl Speicherbereiche

Für jeden Speicherbereich, der durch einen Prozess zum Identifizieren doppelter Daten identifiziert wird, sind ungefähr 1.500 Byte Speicherbereich für die aktive Protokolldatei erforderlich. Werden beispielsweise 250.000 Speicherbereiche durch einen erkennen identifiziert, beträgt die geschätzte Größe der aktiven Protokolldatei 358 MB:

```
250.000 während jedes Prozesses ermittelte Speicherbereiche x 1.500 Byte
für jeden Speicherbereich = 358 MB
```

Betrachten Sie das folgende Szenario. 300 Clients für Sichern/Archivieren sichern jede Nacht bis zu 100.000 Dateien. Diese Aktivität hat eine Last von 30.000.000 Dateien zur Folge. Die durchschnittliche Anzahl Speicherbereiche für jede Datei ist 2. Demzufolge beträgt die Gesamtzahl Speicherbereiche 60.000.000 und der Speicherbedarf für das Archivprotokoll 84 GB:

```
60.000.000 Speicherbereiche x 1.500 Byte pro Speicherbereich = 84 GB
```

Ein Prozess zum Identifizieren doppelter Daten wird für Aggregate von Dateien ausgeführt. Ein Aggregat besteht aus Dateien, die in einer bestimmten Transaktion gespeichert sind, wie durch die Serveroption TXNGROUPMAX angegeben. Angenommen, die Serveroption TXNGROUPMAX ist auf den Standardwert 4096 gesetzt. Wenn die durchschnittliche Anzahl Speicherbereiche für jede Datei 2 beträgt, ist die Gesamtzahl Speicherbereiche in jedem Aggregat 8192 und der für die aktive Protokolldatei erforderliche Speicherbedarf 12 MB:

```
8192 Speicherbereiche in jedem Aggregat x 1500 Byte pro Speicherbereich =
12 MB
```

### Timing und Anzahl der Prozesse zum Identifizieren doppelter Daten

Das Timing und die Anzahl Prozesse zum Identifizieren doppelter Daten haben ebenfalls Auswirkungen auf die Größe der aktiven Protokolldatei. Bei Verwendung der in dem vorhergehenden Beispiel berechneten Größe der aktiven Protokolldatei von 12 MB beträgt die gleichzeitige Last für die aktive Protokolldatei 120 MB, wenn 10 Prozesse zum Identifizieren doppelter Daten parallel ausgeführt werden:

```
12 MB pro Prozess x 10 Prozesse = 120 MB
```

### Dateigröße

Große Dateien, die für die Identifizierung doppelter Daten verarbeitet werden, können ebenfalls Auswirkungen auf die Größe der aktiven Protokolldatei haben. Beispiel: Angenommen, ein Client für Sichern/Archivieren sichert ein Dateisystemimage mit einer Größe von 80 GB. Die Anzahl doppelter Speicherbereiche für dieses Objekt kann groß sein, wenn beispielsweise die in das Dateisystemimage eingeschlossenen Dateien mit Teilsicherungen gesichert wurden. Beispiel: Angenommen, ein Dateisystemimage hat 1,2 Millionen doppelte Speicherbereiche. Die 1,2 Millionen Speicherbereiche in dieser großen Datei stellen eine einzige Transaktion für einen Prozess zum Identifizieren doppelter Daten dar. Der Gesamtspeicherbereich in der aktiven Protokolldatei, der für dieses einzelne Objekt erforderlich ist, beträgt 1,7 GB:

```
1.200.000 Speicherbereich x 1.500 Byte pro Speicherbereich = 1,7 GB
```

Wenn andere, kleinere Prozesse zum Identifizieren doppelter Daten zu demselben Zeitpunkt ausgeführt werden wie der Prozess zum Identifizieren doppelter Daten für ein einzelnes großes Objekt, ist in der aktiven Protokolldatei möglicherweise nicht genügend Speicherbereich verfügbar. Beispiel: Angenommen, ein Speicherpool ist für die Deduplizierung aktiviert. Der Speicherpool enthält gemischte Daten, einschließlich vieler relativ kleiner Dateien mit einer Größe von 10 KB bis zu mehreren

hundert KB. Der Speicherpool enthält außerdem einige wenige große Objekte mit einem hohen Prozentsatz an doppelten Speicherbereichen.

Um nicht nur den Speicherbedarf zu berücksichtigen, sondern auch das Timing und die Dauer gleichzeitig ablaufender Transaktionen, erhöhen Sie die geschätzte Größe der aktiven Protokolldatei um den Faktor 2. Beispiel: Angenommen, das Ergebnis Ihrer Berechnungen für den Speicherbedarf lautet 25 GB (23,3 GB + 1,7 GB für die Deduplizierung eines großen Objekts). Wenn Deduplizierungsverarbeitung gleichzeitig ausgeführt werden, beträgt die vorgeschlagene Größe der aktiven Protokolldatei 50 GB. Die vorgeschlagene Größe des Archivprotokolls ist 150 GB.

Die Beispiele in den folgenden Tabellen zeigen Berechnungen für aktive Protokolldateien und Archivprotokolle. In dem Beispiel in der ersten Tabelle wird eine durchschnittliche Größe von 700 KB für Speicherbereiche verwendet. In dem Beispiel in der zweiten Tabelle wird eine durchschnittliche Größe von 256 KB verwendet. Wie den Beispielen zu entnehmen ist, zeigt die durchschnittliche Größe doppelter Speicherbereiche von 256 KB eine größere geschätzte Größe für die aktive Protokolldatei an. Um betriebsbezogene Probleme für den Server auf ein Mindestmaß reduzieren oder zu verhindern, verwenden Sie 256 KB für die Schätzung der Größe der aktiven Protokolldatei in Ihrer Produktionsumgebung.

Tabelle 1. Durchschnittliche Größe doppelter Speicherbereiche von 700 KB

| Element  | Beispielwerte |               | Beschreibung   |
|--|---------------|---------------|--|
| Größe des größten zu deduplizierenden Objekts  | 800 GB        | 4 TB          | Die Granularität der Verarbeitung für die Deduplizierung bezieht sich auf die Dateiebene. Demzufolge stellt die größte einzelne zu deduplizierende Datei die umfangreichste Transaktion und eine entsprechend hohe Last für die aktive Protokolldatei und das Archivprotokoll dar.   |
| Durchschnittliche Größe der Speicherbereiche   | 700 KB        | 700 KB        | Die Deduplizierungsalgorithmen verwenden eine variable Blockmethode. Nicht alle deduplizierten Speicherbereiche für eine bestimmte Datei haben dieselbe Größe, daher wird bei dieser Berechnung eine durchschnittliche Speicherbereichsgröße vorausgesetzt.  |
| Speicherbereiche für eine bestimmte Datei  | 1.198.372 Bit | 6.135.667 Bit | Bei Verwendung der durchschnittlichen Speicherbereichsgröße (700 KB), geben diese Berechnungen die Gesamtzahl Speicherbereiche für ein bestimmtes Objekt an.<br><br>Die folgende Berechnung wurde für ein Objekt mit einer Größe von 800 GB ausgeführt: $(800 \text{ GB} \div 700 \text{ KB}) = 1.198.372 \text{ Bit}$<br><br>Die folgende Berechnung wurde für ein Objekt mit einer Größe von 4 TB ausgeführt: $(4 \text{ TB} \div 700 \text{ KB}) = 6.135.667 \text{ Bit}$ |
| Aktive Protokolldatei: vorgeschlagene Größe, die für die Deduplizierung eines einzelnen großen Objekts während eines einzelnen Prozesses zum Identifizieren doppelter Daten erforderlich ist | 1,7 GB        | 8,6 GB        | Der geschätzte Speicherbereich für die aktive Protokolldatei, der für diese Transaktion benötigt wird.   |

| Element  | Beispielwerte       |                       | Beschreibung  |
|--|---------------------|-----------------------|---|
| Aktive Protokolldatei:<br>vorgeschlagene<br>Gesamtgröße  | 66 GB <sup>1</sup>  | 79,8 GB <sup>1</sup>  | <p>Multiplizieren Sie, nachdem zusätzlich zur Deduplizierung andere Aspekte der Last auf dem Server berücksichtigt wurden, die vorhandene Schätzung mit dem Faktor 2. In diesen Beispielen wird der zum Deduplizieren eines einzelnen großen Objekts erforderliche Speicherbereich für die aktive Protokolldatei im Zusammenhang mit den vorherigen Schätzungen für die erforderliche Größe der aktiven Protokolldatei betrachtet.</p> <p>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:</p> $(23,3 \text{ GB} + 1,7 \text{ GB}) \times 2 = 50 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:</p> $50 + 16 = 66 \text{ GB}$ <p>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:</p> $(23,3 \text{ GB} + 8,6 \text{ GB}) \times 2 = 63,8 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:</p> $63,8 + 16 = 79,8 \text{ GB}$ |
| Archivprotokoll:<br>vorgeschlagene<br>Größe  | 198 GB <sup>1</sup> | 239,4 GB <sup>1</sup> | <p>Multiplizieren Sie die geschätzte Größe der aktiven Protokolldatei mit dem Faktor 3.</p> <p>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:</p> $50 \text{ GB} \times 3 = 150 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $150 + 48 = 198 \text{ GB}$ <p>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:</p> $63,8 \text{ GB} \times 3 = 191,4 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $191,4 + 48 = 239,4 \text{ GB}$  |
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die die Deduplizierung verwendet, ist 32 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die die Deduplizierung verwendet, ist 96 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 32 GB bzw. 96 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |                     |                       |   |

Tabelle 2. Durchschnittliche Größe doppelter Speicherbereiche von 256 KB

| Element                                       | Beispielwerte |      | Beschreibung   |
|---|---------------|------|--|
| Größe des größten zu deduplizierenden Objekts | 800 GB        | 4 TB | Die Granularität der Verarbeitung für die Deduplizierung bezieht sich auf die Dateiebene. Demzufolge stellt die größte einzelne zu deduplizierende Datei die umfangreichste Transaktion und eine entsprechend hohe Last für die aktive Protokolldatei und das Archivprotokoll dar. |



| Element  | Beispielwerte        |                       | Beschreibung   |
|--|----------------------|-----------------------|--|
| Durchschnittliche Größe der Speicherbereiche   | 256 KB               | 256 KB                | Die Deduplizierungsalgorithmen verwenden eine variable Blockmethode. Nicht alle deduplizierten Speicherbereiche für eine bestimmte Datei haben dieselbe Größe, daher wird bei dieser Berechnung eine durchschnittliche Speicherbereichsgröße vorausgesetzt.  |
| Speicherbereiche für eine bestimmte Datei  | 3.276.800 Bit        | 16.777.216 Bit        | Bei Verwendung der durchschnittlichen Speicherbereichsgröße, geben diese Berechnungen die Gesamtzahl Speicherbereiche für ein bestimmtes Objekt an.<br><br>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:<br><br>$(800 \text{ GB} \div 256 \text{ KB}) = 3.276.800 \text{ Bit}$<br><br>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:<br><br>$(4 \text{ TB} \div 256 \text{ KB}) = 16.777.216 \text{ Bit}$  |
| Aktive Protokolldatei: vorgeschlagene Größe, die für die Deduplizierung eines einzelnen großen Objekts während eines einzelnen Prozesses zum Identifizieren doppelter Daten erforderlich ist | 4,5 GB               | 23,4 GB               | Die geschätzte Größe des Speicherbereichs für die aktive Protokolldatei, die für diese Transaktion erforderlich ist.   |
| Aktive Protokolldatei: vorgeschlagene Gesamtgröße  | 71,6 GB <sup>1</sup> | 109,4 GB <sup>1</sup> | Nachdem Sie neben der Deduplizierung andere Aspekte der Serverauslastung mit berücksichtigt haben, multiplizieren Sie die vorhandene Schätzung mit dem Faktor 2. In diesen Beispielen wird der zum Deduplizieren eines einzelnen großen Objekts erforderliche Speicherbereich für die aktive Protokolldatei im Zusammenhang mit den vorherigen Schätzungen für die erforderliche Größe der aktiven Protokolldatei betrachtet.<br><br>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:<br><br>$(23,3 \text{ GB} + 4,5 \text{ GB}) \times 2 = 55,6 \text{ GB}$<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>$55,6 + 16 = 71,6 \text{ GB}$<br><br>Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:<br><br>$(23,3 \text{ GB} + 23,4 \text{ GB}) \times 2 = 93,4 \text{ GB}$<br><br>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:<br><br>$93,4 + 16 = 109,4 \text{ GB}$ |

| Element  | Beispielwerte         |                       | Beschreibung   |
|--|-----------------------|-----------------------|--|
| Archivprotokoll:<br>vorgeschlagene<br>Größe  | 214,8 GB <sup>1</sup> | 328,2 GB <sup>1</sup> | <p>Die geschätzte Größe der aktiven Protokolldatei multipliziert mit dem Faktor 3.</p> <p>Die folgende Berechnung wurde für ein Objekt mit einer Größe von 800 GB ausgeführt:</p> $55,6 \text{ GB} \times 3 = 166,8 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $166,8 + 48 = 214,8 \text{ GB}$ <p>Die folgende Berechnung wurde für ein Objekt mit einer Größe von 4 TB ausgeführt:</p> $93,4 \text{ GB} \times 3 = 280,2 \text{ GB}$ <p>Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:</p> $280,2 + 48 = 328,2 \text{ GB}$ |
| <p><sup>1</sup> Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die die Deduplizierung verwendet, ist 32 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die die Deduplizierung verwendet, ist 96 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 32 GB bzw. 96 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.</p> <p>Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.</p> |                       |                       |  |

## Windows: Speicherbereich des Spiegels für aktive Protokolldateien

Die aktive Protokolldatei kann gespiegelt werden, sodass die gespiegelte Kopie verwendet werden kann, falls die aktiven Protokolldateien nicht gelesen werden können. Es kann nur ein einziger Spiegel der aktiven Protokolldatei vorhanden sein.

Die Erstellung einer Protokollspiegel ist eine vorgeschlagene Option. Wenn Sie die aktive Protokolldatei vergrößern, wird der Protokollspiegel automatisch vergrößert. Die Spiegelung des Protokolls kann sich negativ auf die Leistung auswirken, da die doppelte E/A-Aktivität erforderlich ist, um den Spiegel zu verwalten. Der zusätzliche Speicherbereich, den der Protokollspiegel benötigt, ist ein weiterer Faktor, der bei der Entscheidung über die Erstellung eines Protokollspiegels berücksichtigt werden muss.

Wenn das Spiegelprotokollverzeichnis voll wird, gibt der Server Fehlernachrichten in das Aktivitätenprotokoll und in die Datei db2diag.log aus. Die Serveraktivität wird fortgesetzt.

## Windows: Speicherbereich des Übernahmeverzeichnis für Archivprotokolle

Das Übernahmeverzeichnis für Archivprotokolle wird vom Server verwendet, wenn der Speicherbereich des Verzeichnisses für Archivprotokolle nicht mehr ausreicht.

Durch Angabe eines Übernahmezeichnisses für Archivprotokolle können Probleme verhindert werden, die auftreten, wenn der Speicherbereich der Archivprotokolldatei nicht mehr ausreicht. Wenn sowohl das Verzeichnis für Archivprotokolle als auch das Laufwerk oder das Dateisystem, in dem sich das Übernahmeverzeichnis für Archivprotokolle befindet, voll wird, bleiben die Daten im Verzeichnis für aktive Protokolldateien. Dadurch kann die aktive Protokolldatei vollständig ausgefüllt werden, was einen Serverhalt verursacht.

## Windows: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen

Um den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei zu bestimmen, geben Sie den Befehl QUERY LOG ein. Um die Speicherauslastung in der Datenbank und den Wiederherstellungsprotokollen zu überwachen, können Sie auch das Aktivitätenprotokoll auf Nachrichten überprüfen.

## Aktive Protokolldatei

---

Wenn der verfügbare Speicherbereich für die aktive Protokolldatei zu gering ist, werden die folgenden Nachrichten im Aktivitätenprotokoll angezeigt:

### ANR4531I: IC\_AUTOBACKUP\_LOG\_USED\_SINCE\_LAST\_BACKUP\_TRIGGER

Diese Nachricht wird angezeigt, wenn der Speicherbereich für die aktive Protokolldatei die angegebene maximale Größe überschreitet. Der IBM Spectrum Protect-Server startet eine Datenbankgesamtsicherung.

Um die maximale Protokollgröße zu ändern, stoppen Sie den Server. Öffnen Sie die Datei dmserv.opt und geben Sie für die Option ACTIVELOGSIZE einen neuen Wert an. Starten Sie anschließend den Server erneut.

### ANR0297I: IC\_BACKUP\_NEEDED\_LOG\_USED\_SINCE\_LAST\_BACKUP

Diese Nachricht wird angezeigt, wenn der Speicherbereich für die aktive Protokolldatei die angegebene maximale Größe überschreitet. Sie müssen die Datenbank manuell sichern.

Um die maximale Protokollgröße zu ändern, stoppen Sie den Server. Öffnen Sie die Datei dmserv.opt und geben Sie für die Option ACTIVELOGSIZE einen neuen Wert an. Starten Sie anschließend den Server erneut.

### ANR4529I: IC\_AUTOBACKUP\_LOG\_UTILIZATION\_TRIGGER

Das Verhältnis des belegten Speicherbereichs für die aktive Protokolldatei zum verfügbaren Speicherbereich für die aktive Protokolldatei überschreitet den Schwellenwert für die Protokollauslastung. Wenn mindestens eine einzige Datenbankgesamtsicherung ausgeführt wurde, startet der IBM Spectrum Protect-Server eine Teilsicherung der Datenbank. Andernfalls startet der Server eine Datenbankgesamtsicherung.

### ANR0295I: IC\_BACKUP\_NEEDED\_LOG\_UTILIZATION

Das Verhältnis des belegten Speicherbereichs für die aktive Protokolldatei zum verfügbaren Speicherbereich für die aktive Protokolldatei überschreitet den Schwellenwert für die Protokollauslastung. Sie müssen die Datenbank manuell sichern.

## Archivprotokoll

---

Wenn der verfügbare Speicherbereich für das Archivprotokoll zu gering ist, wird die folgende Nachricht im Aktivitätenprotokoll angezeigt:

### ANR0299I: IC\_BACKUP\_NEEDED\_ARCHLOG\_USED

Das Verhältnis des belegten Speicherbereichs für das Archivprotokoll zum verfügbaren Speicherbereich für das Archivprotokoll überschreitet den Schwellenwert für die Protokollauslastung. Der IBM Spectrum Protect-Server startet eine automatische Datenbankgesamtsicherung.

## Datenbank

---

Wenn der verfügbare Speicherbereich für Datenbankaktivitäten zu gering ist, wird die folgende Nachricht im Aktivitätenprotokoll angezeigt:

### ANR2992W: IC\_LOG\_FILE\_SYSTEM\_UTILIZATION\_WARNING\_2

Der belegte Speicherplatz in der Datenbank überschreitet den Schwellenwert für die Belegung des Speicherplatzes in der Datenbank. Um den Speicherplatz für die Datenbank zu vergrößern, verwenden Sie den Befehl EXTEND DBSPACE oder das Dienstprogramm DSMSEV FORMAT mit dem Parameter DBDIR.

### ANR1546W: FILESYSTEM\_DBPATH\_LESS\_1GB

Der verfügbare Speicherbereich in dem Verzeichnis, in dem sich die Serverdatenbankdateien befinden, beträgt weniger als 1 GB.

Wenn ein IBM Spectrum Protect-Server mit dem Dienstprogramm DSMSEV FORMAT oder dem Konfigurationsassistenten erstellt wird, werden auch eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien erstellt, in denen Datenbankinformationen gespeichert werden sollen, die vom Datenbankmanager verwendet werden. Der in dieser Nachricht angegebene Pfad gibt die Speicherposition der Datenbankinformationen an, die vom Datenbankmanager verwendet werden. Ist in dem Pfad kein Speicherbereich verfügbar, ist der Server nicht mehr funktionsfähig.

Sie müssen dem Dateisystem Speicherbereich hinzufügen oder in dem Dateisystem oder auf der Platte Speicherbereich freigeben.

## Windows: Rollbackdateien der Installation löschen

---

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, löschen, um Speicherplatz im Verzeichnis für gemeinsam genutzte Ressourcen freizugeben. Zu den Dateitypen, die Sie löschen können, gehören z. B. Dateien, die für eine Rollbackoperation benötigt wurden.

## Informationen zu diesem Vorgang

---

Zum Löschen der nicht mehr benötigten Dateien verwenden Sie den grafisch orientierten Installationsassistenten oder die Befehlszeile im Konsolenmodus.

- **Windows: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen**  
Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der IBM® Installation Manager-Benutzerschnittstelle löschen.
- **Windows: Rollbackdateien für die Installation mit der Befehlszeile löschen**  
Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der Befehlszeile löschen.

## Windows: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen

---

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der IBM® Installation Manager-Benutzerschnittstelle löschen.

### Vorgehensweise

---

1. Öffnen Sie IBM Installation Manager.
2. Klicken Sie auf Datei > Benutzervorgaben.
3. Wählen Sie Dateien für Rollback aus.
4. Klicken Sie auf Gespeicherte Dateien löschen und dann auf OK.

## Windows: Rollbackdateien für die Installation mit der Befehlszeile löschen

---

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der Befehlszeile löschen.

### Vorgehensweise

---

1. In dem Verzeichnis, in dem IBM® Installation Manager installiert ist, wechseln Sie in das folgende Unterverzeichnis:
  -  Windows-Betriebssystemeclipse\tools
- Beispiel:
  -  Windows-BetriebssystemeC:\Programme\IBM\Installation Manager\eclipse\tools
2. Geben Sie im Verzeichnis tools den folgenden Befehl aus, um eine IBM Installation Manager-Befehlszeile zu starten:
  -  Windows-Betriebssystemeimcl.exe -c
3. Geben Sie **P** ein, um Benutzervorgaben auszuwählen.
4. Geben Sie **3** ein, um Dateien für Rollback auszuwählen.
5. Geben Sie **D** ein, um die Dateien für Rollback zu löschen.
6. Geben Sie **A** ein, um die Änderungen anzuwenden und zum Benutzervorgabenmenü zurückzukehren.
7. Geben Sie **C** ein, um das Benutzervorgabenmenü zu verlassen.
8. Geben Sie **X** ein, um Installation Manager zu beenden.

## Windows: Empfehlungen für die Serverbenennung

---

Verwenden Sie diese Beschreibungen als Referenz bei der Installation oder beim Upgrade eines IBM Spectrum Protect-Servers.

### Instanzenutzer-ID

---

Die Instanzbenutzer-ID wird als Basis für andere Namen verwendet, die sich auf die Serverinstanz beziehen. Die Instanzbenutzer-ID wird auch als Instanzeigner bezeichnet.

Zum Beispiel: tsminst1

Die Instanzbenutzer-ID ist die Benutzer-ID, die über das Eigentumsrecht oder über Schreib-/Lesezugriffsberechtigung für alle Verzeichnisse verfügen muss, die Sie für die Datenbank und das Wiederherstellungsprotokoll erstellen. Der Server wird standardmäßig mit der Instanzbenutzer-ID ausgeführt. Diese Benutzer-ID benötigt außerdem Schreib-/Lesezugriff für die Verzeichnisse, die für die Einheitenklasse FILE verwendet werden.

 Windows-Betriebssysteme

## Datenbankinstanzname

---

Der Datenbankinstanzname ist der Name der Serverinstanz in der Registrierung.

Zum Beispiel: Server1

 Windows-Betriebssysteme

## Instanzenverzeichnis

---

Das Instanzverzeichnis enthält spezielle Dateien für eine Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien). Es kann einen beliebigen Namen haben. Um die Identifizierung zu erleichtern, sollten Sie einen Namen verwenden, der das Verzeichnis mit dem Instanznamen verknüpft.

Sie können einen Namen verwenden, der den Namen der Serverinstanz enthält, der in der Registrierung angezeigt wird. Standardnamen für die Serverinstanz haben das Format **Serverx**.

Zum Beispiel: C:\tsm\server1

Im Instanzverzeichnis sind folgende Dateien für die Serverinstanz gespeichert:

- Serveroptionsdatei dsmserv.opt
- Die Serverschlüsseldatenbankdatei `cert.kdb` und die `.arm`-Dateien (werden von Clients und anderen Servern zum Importieren der Secure Sockets Layer-Zertifikate des Servers verwendet)
- Einheitenkonfigurationsdatei, wenn die Serveroption DEVCONFIG keinen vollständig qualifizierten Namen angibt
- Protokolldatei für Datenträger, wenn die Serveroption VOLUMEHISTORY keinen vollständig qualifizierten Namen angibt
- Datenträger für Speicherpools mit dem Typ DEVTYPE=FILE, wenn das Verzeichnis für die Einheitenklasse nicht vollständig angegeben oder nicht vollständig qualifiziert ist
- Benutzerexits
- Traceausgabe (wenn nicht vollständig qualifiziert)

## Datenbankname


---

Der Datenbankname lautet für jede Serverinstanz immer TSMDB1. Dieser Name kann nicht geändert werden.

## Servername

---

Der Servername ist ein interner Name für IBM Spectrum Protect und wird für Operationen verwendet, bei denen eine Datenübertragung zwischen mehreren IBM Spectrum Protect-Servern auftritt. Zum Beispiel bei der Kommunikation zwischen Servern und bei der gemeinsamen Nutzung von Speicherarchiven.

 Windows-Betriebssysteme Der Servername wird auch verwendet, wenn Sie den Server dem Operations Center hinzufügen, so dass er mit dieser Schnittstelle verwaltet werden kann. Verwenden Sie einen eindeutigen Namen für jeden Server. Verwenden Sie einen Namen, der die Position oder den Zweck des Servers angibt, um die Identifikation im Operations Center (oder mit einem Befehl QUERY SERVER) zu erleichtern. Nachdem ein IBM Spectrum Protect-Server als Hub- oder Peripherieserver konfiguriert wurde, dürfen Sie seinen Namen nicht mehr ändern.

Wenn Sie den Assistenten verwenden, wird als Standardname der Hostname des von Ihnen verwendeten Systems vorgeschlagen. Sie können einen anderen, für Ihre Umgebung aussagekräftigen Namen verwenden. Befinden sich mehrere Server auf dem System, können Sie bei Verwendung des Assistenten den Standardnamen nur für einen der Server angeben. Sie müssen einen eindeutigen Namen für jeden Server eingeben.

 Windows-Betriebssysteme Zum Beispiel:

- TUCSON\_SERVER1
- TUCSON\_SERVER2

## Verzeichnisse für Datenbankbereich und Wiederherstellungsprotokoll

---

Die Verzeichnisse können gemäß den lokalen Vorgaben benannt werden. Sie sollten Namen verwenden, die die Verzeichnisse mit der Serverinstanz verknüpfen, um die Identifikation zu erleichtern.

Beispiel für das Archivprotokoll:

-  Windows-Betriebssystemef:\server1\archlog

## Windows: Installationsverzeichnisse

---

Zu den Installationsverzeichnissen für den IBM Spectrum Protect-Server gehören die Verzeichnisse für den Server, DB2, die Einheiten, die Sprache und andere Verzeichnisse. Jedes Verzeichnis enthält mehrere zusätzliche Verzeichnisse.

Das Verzeichnis `/opt/tivoli/tsm/server/bin` ist das Standardverzeichnis, das den Servercode und die Lizenzierung enthält.

Das während der Installation des IBM Spectrum Protect-Servers installierte DB2-Produkt hat die in den DB2-Informationsquellen dokumentierte Verzeichnisstruktur. Schützen Sie diese Verzeichnisse und Dateien wie die Serververzeichnisse. Das Standardverzeichnis heißt `/opt/tivoli/tsm/db2`.

Sie können folgende Sprachen verwenden: Englisch (US), Deutsch, Französisch, Italienisch, Spanisch, Portugiesisch (Brasilien), Koreanisch, Japanisch, traditionelles Chinesisch, vereinfachtes Chinesisch, Chinesisch GBK, Chinesisch Big5 und Russisch.

## Windows: Serverkomponenten installieren

---


Für die Installation der Serverkomponenten der Version 8.1.3 können Sie den Installationsassistenten, die Befehlszeile im Konsolenmodus oder den unbeaufsichtigten Modus verwenden.

### Informationen zu diesem Vorgang

---

Mithilfe der IBM Spectrum Protect-Installationssoftware können Sie die folgenden Komponenten installieren:

- Server  
Tipp: Die Datenbank (DB2), Global Security Kit (GSKit) und IBM® Java™ Runtime Environment (JRE) werden automatisch installiert, wenn Sie die Serverkomponente auswählen.
- Sprachen des Servers
- Lizenz
- Einheiten
- IBM Spectrum Protect for SAN
- Operations Center

 Für die Installation eines Servers der Version 8.1.3 anhand dieses Leitfadens müssen Sie 15 - 30 Minuten einplanen.

- Windows: Installationspaket abrufen  
Das Installationspaket für IBM Spectrum Protect kann von einer IBM Download-Site heruntergeladen werden, z. B. von Passport Advantage oder IBM Fix Central.
- Windows: IBM Spectrum Protect mit dem Installationsassistenten installieren  
Sie können den Server mit dem grafisch orientierten Assistenten von IBM Installation Manager installieren.
- Windows: IBM Spectrum Protect im Konsolenmodus installieren  
Sie können IBM Spectrum Protect mithilfe der Befehlszeile im Konsolenmodus installieren.
- Windows: IBM Spectrum Protect im unbeaufsichtigten Modus installieren  
Sie können den Server im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlermeldungen in Protokolldateien gespeichert.
- Windows: Serversprachenpakete installieren  
Übersetzungen für den Server ermöglichen das Anzeigen von Nachrichten und Hilfetext auf dem Server in verschiedenen Sprachen. Die Übersetzungen gestatten auch die Verwendung länderspezifischer Einstellungen für das Datums-, Uhrzeit- und Zahlenformat.

## Windows: Installationspaket abrufen


---

Das Installationspaket für IBM Spectrum Protect kann von einer IBM® Download-Site heruntergeladen werden, z. B. von Passport Advantage oder IBM Fix Central.

### Vorgehensweise

---

1. Laden Sie die entsprechende Paketdatei von einer der folgenden Websites herunter:
  - Laden Sie das Serverpaket aus Passport Advantage oder Fix Central herunter.
  - Die neuesten Informationen, Aktualisierungen und Fixes finden Sie im IBM Support Portal.
2. Gehen Sie wie folgt vor, wenn Sie das Paket von einer IBM Download-Site heruntergeladen haben:

 Windows-Betriebssysteme

- a. Überprüfen Sie, ob genug Speicherbereich zum Speichern der Installationsdateien nach dem Extrahieren aus dem Produktpaket vorhanden ist. Informationen zum Speicherplatzbedarf finden Sie im Downloadaddokument:
  - IBM Spectrum Protect Technote 4042944
  - IBM Spectrum Protect Extended Edition Technote 4042945
  - IBM Spectrum Protect for Data Retention Technote 4042946
- b. Wechseln Sie in das Verzeichnis, in dem sich die ausführbare Datei befindet.  
Wichtig: Im nächsten Schritt werden die Dateien in das aktuelle Verzeichnis extrahiert. Der Pfad darf maximal 128 Zeichen enthalten. Sie müssen die Installationsdateien in ein leeres Verzeichnis extrahieren. Verwenden Sie kein Verzeichnis, das bereits extrahierte Dateien oder andere Dateien enthält.
- c. Klicken Sie entweder doppelt auf die ausführbare Datei oder geben Sie den folgenden Befehl in die Befehlszeile ein, um die Installationsdateien zu extrahieren. Die Dateien werden in das aktuelle Verzeichnis extrahiert.

*Paketname.exe*

*Paketname* sieht wie in dem folgenden Beispiel aus: *8.1.x.000-IBM-SPSRV-WindowsX64.exe*


3. Wählen Sie eine der folgenden Methoden für die Installation von IBM Spectrum Protect aus:
  - Windows: IBM Spectrum Protect mit dem Installationsassistenten installieren
  - Windows: IBM Spectrum Protect im Konsolenmodus installieren
  - Windows: IBM Spectrum Protect im unbeaufsichtigten Modus installieren
4. Nachdem Sie IBM Spectrum Protect installiert haben und bevor Sie IBM Spectrum Protect für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Support and downloads und legen Sie alle gültigen Fixes an.

## Windows: IBM Spectrum Protect mit dem Installationsassistenten installieren

Sie können den Server mit dem grafisch orientierten Assistenten von IBM® Installation Manager installieren.



### Vorbereitende Schritte

Führen Sie vor dem Start der Installation die folgenden Schritte aus:

- Überprüfen Sie, ob für das Betriebssystem die erforderliche Sprache definiert ist. Die Sprache des Betriebssystems ist standardmäßig die Sprache des Installationsassistenten.
-  Windows-Betriebssysteme Stellen Sie sicher, dass die Benutzer-ID, die Sie während der Installation verwenden wollen, ein Benutzer mit der Berechtigung eines lokalen Administrators ist.

### Vorgehensweise


Installieren Sie IBM Spectrum Protect mit dem folgenden Verfahren:


| Option  | Bezeichnung   |
|---|---|
| <b>Installation der Software mithilfe eines heruntergeladenen Pakets:</b> | <p>a. Wechseln Sie in das Verzeichnis, in das Sie das Paket heruntergeladen haben.</p> <p>b. Geben Sie den folgenden Befehl aus, um den Installationsassistenten zu starten:</p> <p> Windows-Betriebssysteme</p> <p style="padding-left: 40px;">install.bat</p> <p> Windows-Betriebssysteme Sie können auch in dem Verzeichnis, in dem die Installationsdateien extrahiert wurden, doppelt auf die Datei install.bat klicken.</p> |

### Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM Installation Manager-Verzeichnis logs gespeichert werden.

Installationsprotokolldateien können Sie anzeigen, indem Sie in Installation Manager auf Datei > Protokoll anzeigen klicken. Um diese Protokolldateien zu erfassen, klicken Sie in Installation Manager auf Hilfe > Daten zur Fehleranalyse exportieren.

- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.
-  Windows-Betriebssysteme Nachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.


-  Windows-Betriebssysteme Ist unter Windows ein nativer Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, verwenden Sie den nativen Einheitentreiber. Ist unter Windows kein nativer Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, installieren Sie den IBM Spectrum Protect-Einheitentreiber mithilfe des Befehls `dpinst.exe /a`. Die Datei `dpinst.exe` befindet sich im Verzeichnis des Einheitentreibers. Das Standardverzeichnis ist `C:\Programme\Tivoli\TSM\device\drivers`.

## Windows: IBM Spectrum Protect im Konsolenmodus installieren

Sie können IBM Spectrum Protect mithilfe der Befehlszeile im Konsolenmodus installieren.


### Vorbereitende Schritte

Führen Sie vor dem Start der Installation die folgenden Schritte aus:




- Überprüfen Sie, ob für das Betriebssystem die erforderliche Sprache definiert ist. Die Sprache des Betriebssystems ist standardmäßig die Sprache des Installationsassistenten.
-  Windows-Betriebssysteme Stellen Sie sicher, dass die Benutzer-ID, die Sie während der Installation verwenden wollen, ein Benutzer mit der Berechtigung eines lokalen Administrators ist.

### Vorgehensweise

Installieren Sie IBM Spectrum Protect mit dem folgenden Verfahren:

| Option  | Bezeichnung  |
|---|--|
| <b>Installation der Software mithilfe eines heruntergeladenen Pakets:</b> | <p>a. Wechseln Sie in das Verzeichnis, in das Sie das Paket heruntergeladen haben.</p> <p>b. Geben Sie den folgenden Befehl aus, um den Installationsassistenten im Konsolenmodus zu starten:  Windows-Betriebssysteme</p> <pre>install.bat -c</pre> <p>Optional : Generieren Sie während einer Installation im Konsolenmodus eine Antwortdatei. Geben Sie die Optionen für die Installation im Konsolenmodus und in der Anzeige Zusammenfassung <code>c</code> an, um die Antworten zu generieren.</p> |

### Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM® Installation Manager-Verzeichnis logs gespeichert werden. Zum Beispiel:
  -  Windows-Betriebssysteme `C:\Programme\IBM\Installation Manager\logs`
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.
-  Windows-Betriebssysteme Nachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.
-  Windows-Betriebssysteme Ist unter Windows ein nativer Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, verwenden Sie den nativen Einheitentreiber. Ist unter Windows kein nativer Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, installieren Sie den IBM Spectrum Protect-Einheitentreiber mithilfe des Befehls `dpinst.exe /a`. Die Datei `dpinst.exe` befindet sich im Verzeichnis des Einheitentreibers. Das Standardverzeichnis ist `C:\Programme\Tivoli\TSM\device\drivers`.

## Windows: IBM Spectrum Protect im unbeaufsichtigten Modus installieren

Sie können den Server im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlernachrichten in Protokolldateien gespeichert.

### Vorbereitende Schritte

Für die Dateneingabe bei Verwendung der unbeaufsichtigten Installation können Sie eine Antwortdatei verwenden. Die folgenden Musterantwortdateien stehen im Verzeichnis `input` zur Verfügung, in dem das Installationspaket extrahiert wird:

`install_response_sample.xml`

Verwenden Sie diese Datei für die Installation der IBM Spectrum Protect-Komponenten.

`update_response_sample.xml`

Verwenden Sie diese Datei für das Upgrade der IBM Spectrum Protect-Komponenten.



Diese Dateien enthalten Standardwerte, die dazu beitragen können, unnötige Warnungen zu vermeiden. Befolgen Sie die in den Dateien enthaltenen Anweisungen zur Verwendung dieser Dateien.

Wenn Sie eine Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

## Vorgehensweise

---


1. Erstellen Sie eine Antwortdatei. Sie können die Musterantwortdatei ändern oder eine eigene Datei erstellen.
2. Wenn Sie den Server und das Operations Center im unbeaufsichtigten Modus installieren, erstellen Sie in der Antwortdatei ein Kennwort für den Truststore des Operations Center.  
Wenn Sie die Datei `install_response_sample.xml` verwenden, fügen Sie das Kennwort in die folgende Zeile der Datei ein. Hierbei ist `mein_Kennwort` das Kennwort:

```
<variable name='ssl.password' value='mein_Kennwort' />
```

Weitere Informationen zu diesem Kennwort finden Sie in Prüfliste für die Installation.

Tipp: Das Truststore-Kennwort ist nicht erforderlich, wenn Sie das Operations Center mit der Datei `update_response_sample.xml` aktualisieren.




3. Geben Sie den folgenden Befehl in dem Verzeichnis, in dem das Installationspaket extrahiert wurde, aus, um die unbeaufsichtigte Installation zu starten. Der Wert *Antwortdatei* gibt den Pfad und den Namen der Antwortdatei an.

- o  Windows-Betriebssysteme

```
install.bat -s -input Antwortdatei -acceptLicense
```

## Nächste Schritte

---

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM® Installation Manager-Verzeichnis logs gespeichert werden. Zum Beispiel:
  - o  Windows-Betriebssysteme: C:\Programme\IBM\Installation Manager\logs
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.
-  Windows-Betriebssysteme: Nachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.
-  Windows-Betriebssysteme: Ist unter Windows ein nativer Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, verwenden Sie den nativen Einheitentreiber. Ist unter Windows kein nativer Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, installieren Sie den IBM Spectrum Protect-Einheitentreiber mithilfe des Befehls `dpinst.exe /a`. Die Datei `dpinst.exe` befindet sich im Verzeichnis des Einheitentreibers. Das Standardverzeichnis ist `C:\Programme\Tivoli\TSM\device\drivers`.

 Windows-Betriebssysteme

## Windows: Serversprachenpakete installieren

---

Übersetzungen für den Server ermöglichen das Anzeigen von Nachrichten und Hilfetext auf dem Server in verschiedenen Sprachen. Die Übersetzungen gestatten auch die Verwendung länderspezifischer Einstellungen für das Datums-, Uhrzeit- und Zahlenformat.

## Vorbereitende Schritte

---


Anweisungen zur Installation von von Sprachenpaketen für Speicheragenten finden Sie unter Language pack configuration for Storage Agent.

- Windows: Spracheinstellungen für den Server  
Verwenden Sie zum Anzeigen von Servernachrichten und Hilfetext entweder das Standardsprachenpaket oder wählen Sie ein anderes Sprachenpaket aus.
- Windows: Sprachenpaket konfigurieren  
Nach der Konfiguration eines Sprachenpakets werden Nachrichten und Hilfetext auf dem Server in der Sprache dieses Sprachenpakets und nicht in Englisch (US) angezeigt. Installationspakete werden mit IBM Spectrum Protect zur Verfügung gestellt.
- Windows: Sprachenpaket aktualisieren  
Sie können ein Sprachenpaket mithilfe von IBM® Installation Manager ändern oder aktualisieren.

## Windows: Spracheinstellungen für den Server

---

Verwenden Sie zum Anzeigen von Servernachrichten und Hilfetext entweder das Standardsprachenpaket oder wählen Sie ein anderes Sprachenpaket aus.

 Windows-Betriebssysteme Dieses Sprachenpaket wird automatisch für die folgende Standardsprachenoption für Servernachrichten und Hilfetext installiert: LANGUAGE AMENG.


Für vom Standard abweichende Sprachen oder Ländereinstellungen installieren Sie das für Ihre Installation erforderliche Sprachenpaket.

Sie können die aufgeführten Sprachen verwenden:

 Windows-Betriebssysteme

Tabelle 1. Serversprachen für Windows

| Sprache                        | Wert der Option LANGUAGE |
|--------------------------------|--------------------------|
| Chinesisch, vereinfacht        | chs                      |
| Chinesisch, traditionell       | cht                      |
| Englisch                       | ameng                    |
| Französisch                    | fra                      |
| Deutsch                        | deu                      |
| Italienisch                    | ita                      |
| Japanisch (Shift-JIS)          | jpn                      |
| Koreanisch                     | kor                      |
| Portugiesisch, Brasilianisches | ptb                      |
| Russisch                       | rus                      |
| Spanisch                       | esp                      |

 Windows-Betriebssysteme Einschränkung: Bei Verwendung des Operations Center werden einige Zeichen möglicherweise nicht ordnungsgemäß angezeigt, wenn der Web-Browsers und der Server nicht dieselbe Sprache verwenden. Wenn dieses Problem auftritt, geben Sie im Browser dieselbe Sprache wie im Server an.


## Windows: Sprachenpaket konfigurieren

---

Nach der Konfiguration eines Sprachenpakets werden Nachrichten und Hilfetext auf dem Server in der Sprache dieses Sprachenpakets und nicht in Englisch (US) angezeigt. Installationspakete werden mit IBM Spectrum Protect zur Verfügung gestellt.

### Informationen zu diesem Vorgang

---

 Windows-Betriebssysteme Geben Sie in der Option LANGUAGE in der Serveroptionsdatei den Namen der Ländereinstellung an, die verwendet werden soll. Soll beispielsweise die Ländereinstellung `ita` verwendet werden, setzen Sie die Option LANGUAGE auf `ita`. Siehe Windows: Spracheinstellungen für den Server.

Wenn die Ländereinstellung erfolgreich initialisiert wird, steuert sie die Datums-, Uhrzeit- und Zahlenformatierung für den Server. Wenn die Ländereinstellung nicht erfolgreich initialisiert wird, verwendet der Server die englischen (US) Nachrichtendateien und das Datums-, Uhrzeit- und Zahlenformat der englischen (US) Ländereinstellung.

## Windows: Sprachenpaket aktualisieren

---

Sie können ein Sprachenpaket mithilfe von IBM® Installation Manager ändern oder aktualisieren.

### Informationen zu diesem Vorgang

---

Sie können ein anderes Sprachenpaket in derselben IBM Spectrum Protect-Instanz installieren.

- Verwenden Sie die Funktion Ändern von IBM Installation Manager, um ein anderes Sprachenpaket zu installieren.
- Verwenden Sie die Funktion Aktualisieren von IBM Installation Manager, um eine Aktualisierung auf neuere Versionen der Sprachenpakete durchzuführen.

Tipp: In IBM Installation Manager bedeutet *aktualisieren* das Erkennen und Installieren von Aktualisierungen und Fixes für installierte Softwarepakete. In diesem Kontext sind *Aktualisierung* und *Upgrade* gleichbedeutend.

# Windows: Die ersten Schritte nach der Installation von IBM Spectrum Protect

Nach der Installation von Version 8.1.3 bereiten Sie die Konfiguration vor. Bevorzugte Methode für die Konfiguration der IBM Spectrum Protect-Instanz ist die Verwendung des Konfigurationsassistenten.

## Informationen zu diesem Vorgang

1. Erstellen Sie die Verzeichnisse und die Benutzer-ID für die Serverinstanz. Siehe [Windows: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen](#).
  2. Konfigurieren Sie eine Serverinstanz. Wählen Sie eine der folgenden Optionen aus:
    - Verwenden Sie den Konfigurationsassistenten (die bevorzugte Methode). Siehe [Windows: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren](#).
    - Konfigurieren Sie die neue Instanz manuell. Siehe [Windows: Serverinstanz manuell konfigurieren](#). Führen Sie während einer manuellen Konfiguration die folgenden Schritte aus:
      - a. Definieren Sie Ihre Verzeichnisse und erstellen Sie die IBM Spectrum Protect-Instanz. Siehe [Windows: Serverinstanz erstellen](#).
      - b. Erstellen Sie eine neue Serveroptionsdatei, indem Sie die Musterdatei kopieren, um die Datenübertragung zwischen dem Server und den Clients zu definieren. Siehe [Windows-Betriebssysteme/Windows: Server- und Clientübertragung konfigurieren](#).
      - c. Geben Sie den Befehl `DSMSERV FORMAT` aus, um die Datenbank zu formatieren. Siehe [Windows: Datenbank und Protokoll formatieren](#).
      - d. Konfigurieren Sie Ihr System für die Datenbanksicherung. Siehe [Windows: Datenbankmanager für die Datenbanksicherung vorbereiten](#).
  3. Konfigurieren Sie Optionen, die die Ausführung der Datenbankreorganisation steuern. Siehe [Windows: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren](#).
  4. Starten Sie die Serverinstanz, falls noch nicht gestartet.
    - [Windows-Betriebssysteme/Windows: Serverinstanz auf Windows-Systemen starten](#).
  5. Registrieren Sie Ihre Lizenz. Siehe [Windows: Lizenzregistrierung](#).
  6. Bereiten Sie Ihr System auf Datenbanksicherungen vor. Siehe [Windows: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben](#).
  7. Überwachen Sie den Server. Siehe [Windows: Server überwachen](#).
- [Windows: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen](#)  
Erstellen Sie die Benutzer-ID für die IBM Spectrum Protect-Serverinstanz und die Verzeichnisse, die die Serverinstanz für Datenbank- und Wiederherstellungsprotokolle benötigt.
  - [Windows: IBM Spectrum Protect-Server konfigurieren](#)  
Nachdem Sie den Server installiert und für die Konfiguration vorbereitet haben, konfigurieren Sie die Serverinstanz.
  - [Windows: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren](#)  
Um Probleme bezüglich des Datenbankwachstums und der Serverleistung zu vermeiden, überwacht der Server automatisch seine Datenbanktabellen und reorganisiert diese Tabellen, wenn dies erforderlich ist. Bevor der Server für den Produktionseinsatz gestartet wird, definieren Sie Serveroptionen, mit denen gesteuert wird, wann die Reorganisation ausgeführt wird. Ist die Verwendung der Datendeduplizierung geplant, stellen Sie sicher, dass die Option für die Ausführung der Indexreorganisation aktiviert ist.
  - [Windows-Betriebssysteme/Windows: Serverinstanz auf Windows-Systemen starten](#)  
In einer Produktionsumgebung ist die bevorzugte Methode zum Starten des Servers der Start als Windows-Dienst. In einer Umgebung, in der Sie rekonfigurieren, testen oder Verwaltungstasks ausführen, starten Sie den Server im Vordergrund oder verwenden Sie den Verwaltungsmodus.
  - [Windows: Server stoppen](#)  
Sie können den Server bei Bedarf stoppen, um die Steuerung an das Betriebssystem zurückzugeben. Um den Verlust von Verwaltungs- und Clientknotenverbindungen zu vermeiden, stoppen Sie den Server erst nach Beendigung oder Abbruch laufender Sitzungen.
  - [Windows: Lizenzregistrierung](#)  
Registrieren Sie alle lizenzierten IBM Spectrum Protect-Funktionen, die Sie beziehen, sofort, damit Sie nach dem Starten der Serveroperationen (z. B. Datensicherung) keine Daten verlieren.
  - [Windows: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben](#)  
Sie müssen die zu verwendende Einheitenklasse angeben, um das System für automatische oder manuelle Datenbanksicherungen vorzubereiten.
  - [Windows: Mehrere Serverinstanzen auf einem System ausführen](#)  
Sie können mehrere Serverinstanzen auf Ihrem System erstellen. Jede Serverinstanz verfügt über ein eigenes Instanzverzeichnis sowie über Datenbank- und Protokollverzeichnisse.
  - [Windows: Server überwachen](#)  
Wenn Sie den Server im Produktionsbetrieb einsetzen, überwachen Sie den von ihm verwendeten Speicherbereich, um

sicherzustellen, dass die Größe des Speicherbereichs angemessen ist. Ändern Sie den Speicherbereich, falls erforderlich.

## Windows: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen

Erstellen Sie die Benutzer-ID für die IBM Spectrum Protect-Serverinstanz und die Verzeichnisse, die die Serverinstanz für Datenbank- und Wiederherstellungsprotokolle benötigt.


### Vorbereitende Schritte

Lesen Sie die Informationen zur Planung des Speicherbereichs für den Server, bevor Sie diese Task ausführen. Siehe Windows: Arbeitsblätter für Planungsdetails für den Server.

### Vorgehensweise

1. Erstellen Sie die Benutzer-ID, die Eigner der Serverinstanz sein soll. Diese Benutzer-ID verwenden Sie später bei der Erstellung der Serverinstanz.

#### Windows-Betriebssysteme

 Erstellen Sie eine Benutzer-ID, die Eigner der IBM Spectrum Protect-Serverinstanz sein soll. Eine Benutzer-ID kann Eigner mehrerer IBM Spectrum Protect-Serverinstanzen sein. Geben Sie das Benutzerkonto an, das Eigner der Serverinstanz sein soll.

Wenn der Server als Windows-Dienst gestartet wird, ist dies das Konto, bei dem sich der Dienst anmeldet. Das Benutzerkonto benötigt Administratorberechtigung auf dem System. Ein Benutzerkonto kann Eigner mehrerer Serverinstanzen sein.

Befinden sich mehrere Server auf einem System und möchten Sie jeden Server mit einem anderen Benutzerkonto ausführen, erstellen Sie ein neues Benutzerkonto in diesem Schritt.

Erstellen Sie die Benutzer-ID.

Einschränkung: Die Benutzer-ID muss die folgende Regel einhalten:

In der Benutzer-ID dürfen nur Kleinbuchstaben (a-z), Ziffern (0-9) und das Unterstrichszeichen ( \_ ) verwendet werden. Die Benutzer-ID darf maximal 30 Zeichen lang sein und sie darf nicht mit *ibm*, *sql*, *sys* oder mit einer Ziffer beginnen. Als Benutzer-ID und Gruppenname dürfen nicht *user*, *admin*, *guest*, *public*, *local* und kein reserviertes SQL-Wort verwendet werden.

- a. Erstellen Sie die Benutzer-ID mit dem folgenden Betriebssystembefehl:


```
net user Benutzer-ID */add
```

Sie werden zur Erstellung und Überprüfung eines Kennworts für die neue Benutzer-ID aufgefordert.

- b. Geben Sie die folgenden Betriebssystembefehle aus, um die neue Benutzer-ID den Administratorgruppen hinzuzufügen:

```
net localgroup Administrators Benutzer-ID /add  
net localgroup DB2ADMNS Benutzer-ID /add
```

2. Erstellen Sie die vom Server benötigten Verzeichnisse.

 Erstellen Sie leere Verzeichnisse für jeden Tabelleneintrag und stellen Sie sicher, dass die neue Benutzer-ID, die Sie gerade erstellt haben, über Schreib-/Leseberechtigung für die Verzeichnisse verfügt. Die Datenbank, das Archivprotokoll und die aktive Protokolldatei müssen sich auf verschiedenen physischen Datenträgern befinden.

| Element   | Beispielbefehle für die Verzeichniserstellung  | Ihre Verzeichnisse |
|---|--|--------------------|
| Das <i>Instanzverzeichnis</i> für den Server. Dieses Verzeichnis enthält spezielle Dateien für diese Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien). | <pre>mkdir d:\tsm\server1</pre>  |                    |
| Die Datenbankverzeichnisse  | <pre>mkdir d:\tsm\db001<br/>mkdir e:\tsm\db002<br/>mkdir f:\tsm\db003<br/>mkdir g:\tsm\db004</pre> |                    |

| Element   | Beispielbefehle für die Verzeichniserstellung | Ihre Verzeichnisse |
|---|---|--------------------|
| Verzeichnis für aktive Protokolldateien   | <code>mkdir h:\tsm\log</code>                 |                    |
| Verzeichnis für Archivprotokolle  | <code>mkdir i:\tsm\archlog</code>             |                    |
| Optional: Verzeichnis für den Protokollspiegel für die aktive Protokolldatei                      | <code>mkdir j:\tsm\logmirror</code>           |                    |
| Optional: Sekundäres Verzeichnis für Archivprotokolle (Übernahmeverzeichnis für Archivprotokolle) | <code>mkdir k:\tsm\archlogfailover</code>     |                    |


Wenn ein Server anfänglich mit dem Dienstprogramm DSMSEV FORMAT oder mit dem Konfigurationsassistenten erstellt wird, werden eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien zum Speichern von Datenbankinformationen erstellt, die vom Datenbankmanager verwendet werden.

3. Melden Sie die neue Benutzer-ID ab.

## Windows: IBM Spectrum Protect-Server konfigurieren

Nachdem Sie den Server installiert und für die Konfiguration vorbereitet haben, konfigurieren Sie die Serverinstanz.

### Informationen zu diesem Vorgang

 Windows-BetriebssystemeTipp: Die IBM Spectrum Protect-Verwaltungskonsole, bei der es sich um ein Microsoft Management Console-Snap-in (MMC-Snap-in) handelt, wird nicht mehr mit IBM Spectrum Protect bereitgestellt. Die bevorzugte Methode für die Konfiguration des Servers ist der Konfigurationsassistent. Mit dem Assistenten können Sie mehrere Serverkonfigurationstasks ausführen. Sie können mit dem Assistenten jedoch nicht das Active Directory-Schema erweitern, so dass Clients Server automatisch erkennen können.

Wählen Sie eine der folgenden Optionen aus, um eine IBM Spectrum Protect-Serverinstanz zu konfigurieren:


- **Windows: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren**  
Der Assistent stellt eine Möglichkeit zur Konfiguration eines Servers mit Anleitung dar. Wenn Sie die grafische Benutzerschnittstelle (GUI) verwenden, können Sie einige komplexe Konfigurationsschritte der manuellen Ausführung vermeiden. Starten Sie den Assistenten auf dem System, auf dem Sie das IBM Spectrum Protect-Serverprogramm installiert haben.
- **Windows: Serverinstanz manuell konfigurieren**  
Nach der Installation von IBM Spectrum Protect Version 8.1.3 können Sie IBM Spectrum Protect auch manuell und nicht mit dem Konfigurationsassistenten konfigurieren.

## Windows: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren


Der Assistent stellt eine Möglichkeit zur Konfiguration eines Servers mit Anleitung dar. Wenn Sie die grafische Benutzerschnittstelle (GUI) verwenden, können Sie einige komplexe Konfigurationsschritte der manuellen Ausführung vermeiden. Starten Sie den Assistenten auf dem System, auf dem Sie das IBM Spectrum Protect-Serverprogramm installiert haben.

### Vorbereitende Schritte

Bevor Sie den Konfigurationsassistenten starten, müssen Sie alle vorhergehenden Schritte zur Vorbereitung der Konfiguration ausführen. Zu diesen Schritten gehören die Installation von IBM Spectrum Protect, die Erstellung der Datenbank- und Protokollverzeichnisse und die Erstellung der Verzeichnisse und der Benutzer-ID für die Serverinstanz.


 Windows-Betriebssysteme

### Informationen zu diesem Vorgang


 Windows-BetriebssystemeTipp: Die IBM Spectrum Protect-Konsole, bei der es sich um ein Microsoft Management Console-Snap-in (MMC-Snap-in) handelt, wird nicht mehr mit IBM Spectrum Protect bereitgestellt. Die bevorzugte Methode für die Konfiguration der Serverinstanz ist der Konfigurationsassistent. Mit dem Assistenten können Sie mehrere Konfigurationstasks ausführen.

## Vorgehensweise


---

1. Stellen Sie sicher, dass folgende Anforderungen erfüllt sind:  Windows-Betriebssysteme
  - Stellen Sie sicher, dass folgende Anforderungen erfüllt sind:
    - a. Klicken Sie auf Start > Verwaltung > Dienste.
    - b. Wählen Sie im Fenster Dienste den Dienst Remoteregistrierung aus, wenn er nicht gestartet wurde, und klicken Sie auf Starten.
  - Stellen Sie sicher, dass die Anschlüsse 137, 139 und 445 nicht durch eine Firewall blockiert sind:
    - a. Klicken Sie auf Start > Systemsteuerung > Windows-Firewall.
    - b. Wählen Sie Erweiterte Einstellungen aus.
    - c. Wählen Sie Eingehende Regeln im linken Teilfenster aus.
    - d. Wählen Sie Neue Regel im rechten Teilfenster aus.
    - e. Erstellen Sie eine Anschlussregel für die TCP-Anschlüsse 137, 139 und 445, die Verbindungen für Domänen und private Netze zulässt.
  - Konfigurieren Sie die Benutzerkontensteuerung:

Greifen Sie auf alle drei der Konfigurationseinstellungen für die Benutzerkontensteuerung zu, indem Sie zunächst wie folgt auf die Optionen für die Lokale Sicherheitsrichtlinie zugreifen:

- a. Aktivieren Sie das integrierte Administratorkonto:
    - Wählen Sie Konten: Administratorkontostatus aus.
    - Wählen Sie Aktiviert aus und klicken Sie auf OK.
  - b. Inaktivieren Sie die Benutzerkontensteuerung für alle Windows-Administratoren:
    - Wählen Sie Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen aus.
    - Wählen Sie Deaktivieren aus und klicken Sie auf OK.
  - c. Inaktivieren Sie die Benutzerkontensteuerung für das integrierte Administratorkonto:
    - Wählen Sie Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto aus.
    - Wählen Sie Deaktivieren aus und klicken Sie auf OK.
- Starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.
2. Starten Sie die lokale Version des Assistenten:
    -  Windows-Betriebssysteme Klicken Sie auf Start > Alle Programme > IBM Spectrum Protect > Konfigurationsassistent. Sie können auch doppelt auf das Programm `dsmicfgx.exe` in *Installationsverzeichnis*\server klicken. Das Standardverzeichnis ist `C:\Programme\Tivoli\TSM`.


Befolgen Sie die Anweisungen zur Ausführung der Konfiguration. Der Assistent kann gestoppt und erneut gestartet werden. Der Server ist jedoch erst betriebsbereit, wenn der gesamte Konfigurationsprozess abgeschlossen ist.

-  Windows-Betriebssysteme Windows: Remote Execution Protocol unter Windows konfigurieren Fernzugriffseinstellungen mit diesen Prozeduren konfigurieren.

## Windows: Serverinstanz manuell konfigurieren

---

Nach der Installation von IBM Spectrum Protect Version 8.1.3 können Sie IBM Spectrum Protect auch manuell und nicht mit dem Konfigurationsassistenten konfigurieren.

- Windows: Serverinstanz erstellen  
Erstellen Sie eine IBM Spectrum Protect-Instanz mit dem Befehl `db2icrt`.
-  Windows-Betriebssysteme Windows: Server- und Clientübertragung konfigurieren  
Nach der Installation des Servers können Sie die Client- und Serverübertragung definieren, indem Sie Optionen in den Server- und Clientoptionsdateien angeben.
- Windows: Datenbank und Protokoll formatieren  
Mit dem Dienstprogramm `DSMSERV FORMAT` können Sie eine Serverinstanz initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls ist keine andere Serveraktivität zulässig.
- Windows: Datenbankmanager für die Datenbanksicherung vorbereiten  
Um die Daten in der Datenbank in IBM Spectrum Protect zu sichern, müssen Sie den Datenbankmanager aktivieren und die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) konfigurieren.

## Windows: Serverinstanz erstellen


---

Erstellen Sie eine IBM Spectrum Protect-Instanz mit dem Befehl `db2icrt`.

## Informationen zu diesem Vorgang


---

Auf einer Workstation kann mindestens eine Serverinstanz vorhanden sein.

 **Windows-Betriebssysteme** Wichtig: Stellen Sie sicher, dass der Benutzer und das Instanzverzeichnis des Benutzers vorhanden sind, bevor der Befehl `db2icrt` ausgeführt wird. Ist kein Instanzverzeichnis vorhanden, müssen Sie es erstellen.

Im Instanzverzeichnis sind folgende Dateien für die Serverinstanz gespeichert:

- Serveroptionsdatei `dmserv.opt`
- Die Serverschlüsseldatenbankdatei `cert.kdb` und die `.arm`-Dateien (werden von Clients und anderen Servern zum Importieren der Secure Sockets Layer-Zertifikate des Servers verwendet)
- Einheitenkonfigurationsdatei, wenn die Serveroption `DEVCONFIG` keinen vollständig qualifizierten Namen angibt
- Protokolldatei für Datenträger, wenn die Serveroption `VOLUMEHISTORY` keinen vollständig qualifizierten Namen angibt
- Datenträger für Speicherpools mit dem Typ `DEVTYPE=FILE`, wenn das Verzeichnis für die Einheitenklasse nicht vollständig angegeben oder nicht vollständig qualifiziert ist
- Benutzerexits
- Traceausgabe (wenn nicht vollständig qualifiziert)

 **Windows-Betriebssysteme**

1. Melden Sie sich als Administrator an und erstellen Sie mithilfe des Befehls `db2icrt` eine IBM Spectrum Protect-Instanz. Geben Sie den folgenden Befehl in eine Zeile ein. Das von Ihnen angegebene Benutzerkonto wird zu der Benutzer-ID, die Eigner des Servers der Version 8.1.3 ist (die Instanzbenutzer-ID).

```
db2icrt -u Benutzerkonto Instanzname
```

Lautet das Benutzerkonto beispielsweise `tminst1` und die Serverinstanz `Server1`, geben Sie folgenden Befehl ein:

```
db2icrt -u tminst1 server1
```

Sie müssen das Kennwort für die Benutzer-ID `tminst1` eingeben. Wenn Sie später die Datenbank erstellen und formatieren, verwenden Sie den in diesem Befehl angegebenen Instanznamen mit der Option `-k`.

2. Geben Sie als Standardpfad für die Datenbank das Laufwerk an, in dem sich das Instanzverzeichnis für den Server befindet. Führen Sie die folgenden Schritte aus:

- a. Klicken Sie auf `Start > Programme > IBM DB2 > DB2TSM1 > Befehlszeilentools > Befehlszeilenprozessor`.
- b. Geben Sie `quit` ein, um den Befehlszeilenprozessor zu beenden.

Jetzt sollte ein Fenster mit einer Eingabeaufforderung geöffnet werden, in dem die Umgebung für eine erfolgreiche Eingabe der Befehle in den nächsten Schritten ordnungsgemäß eingerichtet ist.

- c. Geben Sie in die Eingabeaufforderung dieses Fensters den folgenden Befehl ein, um die Umgebungsvariable für die Serverinstanz zu definieren, mit der Sie arbeiten:

```
set db2instance=Instanzname
```

Der *Instanzname* ist mit dem Instanznamen identisch, den Sie bei Ausgabe des Befehls `db2icrt` angegeben haben. Geben Sie beispielsweise folgenden Befehl aus, um die Umgebungsvariable für die Serverinstanz `Server1` zu definieren:

```
set db2instance=server1
```

- d. Geben Sie den Befehl zur Definition des Standardlaufwerks aus:

```
db2 update dbm cfg using dftdbpath Instanzposition
```

Das Instanzverzeichnis ist beispielsweise `d:\tsm\server1` und die Instanzposition ist Laufwerk `d:`. Geben Sie folgenden Befehl ein:

```
db2 update dbm cfg using dftdbpath d:
```

3. Erstellen Sie eine neue Serveroptionsdatei. Siehe [Windows: Server- und Clientübertragung konfigurieren](#).

 **Windows-Betriebssysteme**

## Windows: Server- und Clientübertragung konfigurieren

---

Nach der Installation des Servers können Sie die Client- und Serverübertragung definieren, indem Sie Optionen in den Server- und Clientoptionsdateien angeben.

### Informationen zu diesem Vorgang

---

Definieren Sie diese Serveroptionen vor dem Start des Servers. Wenn Sie den Server starten, werden die neuen Optionen wirksam. Wenn Sie Serveroptionen nach dem Serverstart ändern, müssen Sie den Server stoppen und erneut starten, um die aktualisierten Optionen zu




aktivieren.

Sie können Serverübertragungsoptionen in der Serveroptionsdatei (`dsmserver.opt.smp`), die sich im Serverinstanzverzeichnis befindet, anzeigen und angeben. Der Server verwendet standardmäßig die Übertragungsmethoden TCP/IP und Named Pipes (Benannte Pipes).

Tipp: Wenn Sie die Serverkonsole starten und in Warnungen angezeigt wird, dass der Server ein Protokoll nicht verwenden konnte, ist entweder das Protokoll nicht installiert oder die Einstellungen entsprechen nicht den Windows-Protokolleinstellungen.

Damit ein Client ein Protokoll verwenden kann, das auf dem Server aktiviert ist, muss die Clientoptionsdatei entsprechende Werte für Übertragungsoptionen enthalten. In der Serveroptionsdatei können Sie die Werte für jedes Protokoll anzeigen.

Sie können mindestens eine der folgenden Übertragungsmethoden angeben:

- TCP/IP Version 4 oder Version 6
- Benannte Pipes
- Shared Memory
- Secure Sockets Layer (SSL)  
Tipp: Sie können Kennwörter im LDAP-Verzeichnisserver oder im Server authentifizieren. Im LDAP-Verzeichnisserver authentifizierte Kennwörter können erweiterte Systemsicherheit zur Verfügung stellen.
-  Windows-Betriebssysteme: TCP/IP-Optionen definieren  
Wählen Sie aus dem Bereich von TCP/IP-Optionen eine Option für den IBM Spectrum Protect-Server aus oder verwenden Sie den Standardwert.
-  Windows-Betriebssysteme: Optionen für benannte Pipes definieren  
Die Übertragungsmethode benannte Pipes (Named Pipes) ist ideal, wenn der Server und der Client auf derselben Windows-Maschine ausgeführt werden. Für benannte Pipes ist keine besondere Konfiguration erforderlich.
-  Windows-Betriebssysteme: Secure Sockets Layer-Optionen definieren  
Mithilfe von Secure Sockets Layer (SSL) können Sie Ihre Daten und Kennwörter besser schützen.

## Windows: TCP/IP-Optionen definieren

---

Wählen Sie aus dem Bereich von TCP/IP-Optionen eine Option für den IBM Spectrum Protect-Server aus oder verwenden Sie den Standardwert.

### Informationen zu diesem Vorgang

---

Das folgende Beispiel zeigt eine Liste der TCP/IP-Optionen, mit denen Sie Ihr System definieren können.


```
commmethod      tcpip
tcpport         1500
tcpwindowsize   0
tcpnodelay      yes
```

Tipp: Sie können TCP/IP Version 4 und/oder Version 6 verwenden.

#### TCPPORT

Die Adresse des Server-Ports für TCP/IP- und SSL-Kommunikation. Der Standardwert ist 1500.

#### Windows-Betriebssysteme: TCPWINDOWSIZE

 Windows-Betriebssysteme: Gibt die Größe des TCP/IP-Puffers an, der beim Senden oder Empfangen von Daten verwendet wird. Die in einer Sitzung verwendete Fenstergröße ist der kleinere Wert der Server- und Clientfenstergröße. Größere Fenstergrößen benötigen zusätzlichen Speicher, können jedoch die Leistung verbessern.

Soll die Standardfenstergröße für das Betriebssystem verwendet werden, geben Sie 0 an.

#### TCPNODELAY

Gibt an, ob der Server kleine Nachrichten sendet oder ob TCP/IP die Nachrichten puffern soll. Das Senden kleiner Nachrichten kann den Durchsatz verbessern, erhöht jedoch die Anzahl der im Netz gesendeten Pakete. Geben Sie YES an, wenn kleine Nachrichten gesendet werden sollen, oder NO, wenn sie TCP/IP puffern soll. Der Standardwert ist YES.

#### TCPADMINPORT

Gibt die Anschlussnummer an, an der der TCP/IP-DFV-Treiber des Servers auf TCP/IP- oder SSL-fähige Kommunikationsanforderungen warten soll, die keine Clientsitzungen sind. Der Standardwert ist der Wert von TCPPORT.

#### SSLTCPPOINT

(Nur SSL) Gibt die SSL-Anschlussnummer (SSL = Secure Sockets Layer) an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen für SSL-fähige Sitzungen des Befehlszeilenclients für Sichern/Archivieren und des Verwaltungsbefehlszeilenclients wartet.

#### SSLTCPADMINPORT



(Nur SSL) Gibt die Anschlussadresse an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen für SSL-fähige Sitzungen für den Verwaltungsbefehlszeilenclient wartet.

## Windows: Optionen für benannte Pipes definieren

---

Die Übertragungsmethode benannte Pipes (Named Pipes) ist ideal, wenn der Server und der Client auf derselben Windows-Maschine ausgeführt werden. Für benannte Pipes ist keine besondere Konfiguration erforderlich.

### Informationen zu diesem Vorgang

---

Eine Beispieleinstellung für benannte Pipes:

```
commethod          namedpipe
namedpipename     \\.\pipe\adsmpipe
```

COMMETHOD kann in der IBM Spectrum Protect-Serveroptionsdatei mehrfach mit einem jeweils anderen Wert verwendet werden. Die folgende Angabe ist beispielsweise möglich:

```
commethod tcpip
commethod namedpipe
```

## Windows: Secure Sockets Layer-Optionen definieren

---

Mithilfe von Secure Sockets Layer (SSL) können Sie Ihre Daten und Kennwörter besser schützen.

### Vorbereitende Schritte

---

SSL ist die Standardtechnologie für die Erstellung verschlüsselter Sitzungen zwischen Servern und Clients. SSL stellt einen sicheren Kanal für die Server- und Clientkommunikation über offene Kommunikationspfade zur Verfügung. Bei SSL wird die Identität des Servers durch Verwendung digitaler Zertifikate überprüft.

Verwenden Sie SSL für Sitzungen nur im Bedarfsfall, um eine bessere Systemleistung sicherzustellen. Sie könnten die Prozessorressourcen auf dem IBM Spectrum Protect-Server erweitern, um den erhöhten Anforderungen gerecht zu werden.


## Windows: Datenbank und Protokoll formatieren

---

Mit dem Dienstprogramm DSMSERV FORMAT können Sie eine Serverinstanz initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls ist keine andere Serveraktivität zulässig.

Nach der Konfiguration der Serverübertragung können Sie die Datenbank initialisieren. Sie müssen sich mit der Instanzbenutzer-ID anmelden. Fügen Sie die Verzeichnisse nicht in Dateisysteme ein, deren Speicherplatz nicht ausreichen könnte. Wenn bestimmte Verzeichnisse (z. B. das Archivprotokoll) nicht verfügbar oder voll werden, stoppt der Server.

Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN.


 **Wichtig:** Das Installationsprogramm erstellt eine Gruppe von Registrierungsschlüsseln. Einer dieser Schlüssel verweist auf das Verzeichnis, in dem ein Standardserver mit dem Namen SERVER1 erstellt wird. Soll ein zusätzlicher Server installiert werden, erstellen Sie ein Verzeichnis und verwenden Sie das Dienstprogramm DSMSERV FORMAT mit dem Parameter -k in diesem Verzeichnis. Dieses Verzeichnis wird die Position des Servers. In der Registrierung werden die installierten Server aufgezeichnet.

### Exitlistenhandler definieren

---

Geben Sie für jede Serverinstanz ON für die Registry-Variable DB2NOEXITLIST an. Melden Sie sich als Serverinstanzeigner beim System an und geben Sie den folgenden Befehl aus:


```
db2set -i Name_der_Serverinstanz DB2NOEXITLIST=ON
```

Beispiel:  Windows-Betriebssysteme

```
db2set -i server1 DB2NOEXITLIST=ON
```

### Serverinstanz initialisieren


---

Mit dem Dienstprogramm DSMSERV FORMAT können Sie eine Serverinstanz initialisieren. Wenn das Verzeichnis der Serverinstanz z. B. `/tsminst1` lautet, geben Sie die folgenden Befehle aus: 

```
cd \tsminst1
dsmserve -k server2 format dbdir=d:\tsm\db001 activelogsiz=32768
activelogdirectory=e:\tsm\activelog archlogdirectory=f:\tsm\archlog
archfailoverlogdirectory=g:\tsm\archfaillog mirrorlogdirectory=h:\tsm\mirrorlog
```

Tipp: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zu Grunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorabesezugriff und zur Verteilung der Datenbank verringert.

#### Zugehörige Informationen:

 DSMSERV FORMAT (Datenbank und Protokoll formatieren)


## Windows: Datenbankmanager für die Datenbanksicherung vorbereiten


Um die Daten in der Datenbank in IBM Spectrum Protect zu sichern, müssen Sie den Datenbankmanager aktivieren und die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) konfigurieren.

### Informationen zu diesem Vorgang

Wenn Sie den Konfigurationsassistenten verwenden, um eine IBM Spectrum Protect-Serverinstanz zu erstellen, müssen Sie diese Schritte nicht ausführen. Wenn Sie eine Instanz manuell konfigurieren, führen Sie die folgenden Schritte aus, bevor Sie den Befehl BACKUP DB oder RESTORE DB ausgeben.

Achtung: Wenn die Datenbank nicht verwendet werden kann, ist der gesamte IBM Spectrum Protect-Server nicht verfügbar. Wenn eine Datenbank verloren geht und nicht wiederhergestellt werden kann, kann die Wiederherstellung der von diesem Server verwalteten Daten schwierig oder unmöglich sein. Daher ist es unbedingt erforderlich, die Datenbank zu sichern.

 Einschränkung: Auf Windows-Systemen ist die Datenbanksicherung und -zurückschreibung für gemeinsam genutzten Speicher nicht verfügbar.

 In den folgenden Befehlen werden `server1` für die Datenbankinstanz und `d:\tmsmserver1` für das IBM Spectrum Protect-Serververzeichnis als Beispiele verwendet. Ersetzen Sie diese Werte durch tatsächliche Werte in den Befehlen.

1. Erstellen Sie eine Datei mit dem Namen `tsmdbmgr.env` im Verzeichnis `d:\tmsmserver1` mit folgendem Inhalt:

```
DSMI_CONFIG=Serverinstanzverzeichnis\tsmdbmgr.opt
DSMI_LOG=Serverinstanzverzeichnis
```

2. Definieren Sie die Konfiguration der API-Umgebungsvariablen `DSMI_` für die Datenbankinstanz:

- a. Öffnen Sie ein DB2-Befehlsfenster. Sie können hierfür in das Verzeichnis `C:\Programme\Tivoli\TSM\db2\bin` wechseln oder, wenn Sie IBM Spectrum Protect an einer anderen Position installiert haben, in das Unterverzeichnis `db2\bin` in Ihrem Hauptinstallationsverzeichnis. Geben Sie dann den folgenden Befehl aus:

```
db2cmd
```

- b. Geben Sie den folgenden Befehl aus:

```
db2set -i server1 DB2_VENDOR_INI=d:\tmsmserver1\tsmdbmgr.env
```

3. Erstellen Sie eine Datei mit dem Namen `tsmdbmgr.opt` im Verzeichnis `d:\tmsmserver1` mit folgendem Inhalt:

```
*****
nodename $$_TSMDBMGR_$$
commethod tcpip
tcpserveraddr localhost
tcpport 1500
passwordaccess generate
errorlogname d:\tmsmserver1\tsmdbmgr.log
```

#### Erläuterungen:

- o *Nodename* gibt den Knotennamen an, mit dem die Client-API während einer Datenbanksicherung eine Verbindung zum Server herstellt. Dieser Wert muss `$$_TSMDBMGR_$$` lauten, damit die Datenbanksicherung funktioniert.
- o *Commethode* gibt die Client-API an, mit der Kontakt zum Server wegen der Datenbanksicherung hergestellt wird.
- o *Tcpserveraddr* gibt die Serveradresse an, mit der die Client-API Kontakt zum Server wegen der Datenbanksicherung herstellt. Um sicherzustellen, dass die Datenbank gesichert werden kann, muss dieser Wert `localhost` lauten.
- o *Tcpport* gibt die Anschlussnummer an, mit der die Client-API Kontakt zum Server wegen der Datenbanksicherung herstellt. Sie müssen denselben `tcpport`-Wert wie in der Serveroptionsdatei `dsmserve.opt` angeben.
- o *Passwordaccess* ist für die Verbindung des Sicherungsknotens zum Server auf Windows-Systemen erforderlich.

- *Errorlogname* gibt das Fehlerprotokoll an, in dem die Client-API Fehler protokolliert, die während einer Datenbanksicherung auftreten. Dieses Protokoll befindet sich normalerweise im Serverinstanzverzeichnis. Dieses Protokoll kann sich jedoch an jeder beliebigen Position befinden, für die die Instanzbenutzer-ID Schreibberechtigung hat.

## Windows: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren


---

Um Probleme bezüglich des Datenbankwachstums und der Serverleistung zu vermeiden, überwacht der Server automatisch seine Datenbanktabellen und reorganisiert diese Tabellen, wenn dies erforderlich ist. Bevor der Server für den Produktionseinsatz gestartet wird, definieren Sie Serveroptionen, mit denen gesteuert wird, wann die Reorganisation ausgeführt wird. Ist die Verwendung der Datendeduplizierung geplant, stellen Sie sicher, dass die Option für die Ausführung der Indexreorganisation aktiviert ist.

### Informationen zu diesem Vorgang

---

Die Tabellen- und Indexreorganisation erfordert in hohem Umfang Prozessorressourcen, Speicherbereich für die aktive Protokolldatei und Speicherbereich für das Archivprotokoll. Da die Datenbanksicherung Vorrang vor der Reorganisation hat, wählen Sie den Zeitpunkt und die Dauer für die Reorganisation aus, um sicherzustellen, dass sich die Prozesse nicht überlappen und die Reorganisation ausgeführt werden kann.


 Windows-Betriebssysteme Sie können die Index- und Tabellenreorganisation für die Serverdatenbank optimieren. Auf diese Weise können Sie die Vermeidung von unerwartetem Datenbankwachstum und Leistungsproblemen verbessern. Anweisungen finden Sie in Technote 1683633.

Wenn Sie diese Serveroptionen aktualisieren, während der Server aktiv ist, müssen Sie den Server stoppen und erneut starten, damit die aktualisierten Werte wirksam werden.

### Vorgehensweise

---

1. Ändern Sie die Serveroptionen.

 Windows-Betriebssysteme Bearbeiten Sie die Serveroptionsdatei `dsmserv.opt` im Serverinstanzverzeichnis mithilfe eines Texteditors. Beachten Sie bei der Bearbeitung der Serveroptionsdatei die folgenden Richtlinien:

- Entfernen Sie den Stern am Zeilenanfang, um eine Option zu aktivieren.
- Geben Sie eine Option in einer beliebigen Zeile ein.
- Geben Sie nur eine Option pro Zeile ein. Die vollständige Option mit ihrem Wert muss sich in einer Zeile befinden.
- Haben Sie mehrere Einträge für eine Option in der Datei, verwendet der Server den letzten Eintrag.

Die verfügbaren Serveroptionen können Sie mit der Musterdatei `dsmserv.opt.smp` im Verzeichnis `c:\Programme\Tivoli\TSM` anzeigen.

2. Ist die Verwendung der Datendeduplizierung geplant, aktivieren Sie die Serveroption `ALLOWREORGINDEX`. Fügen Sie der Serveroptionsdatei die folgende Option und den folgenden Wert hinzu:

```
allowreorgindex yes
```

3. Definieren Sie die Serveroptionen `REORGBEGINTIME` und `REORGDURATION`, mit denen gesteuert wird, wann die Reorganisation gestartet und wie lange sie ausgeführt wird. Wählen Sie den Zeitpunkt und die Dauer so aus, dass die Reorganisation ausgeführt wird, wenn der Server voraussichtlich am wenigsten ausgelastet ist. Diese Serveroptionen steuern sowohl die Tabellen- als auch die Indexreorganisationsprozesse.

- a. Definieren Sie die Startzeit der Reorganisation mit der Serveroption `REORGBEGINTIME`. Geben Sie die Zeit im 24-Stunden-Format an. Um beispielsweise als Startzeit der Reorganisation 20:30 Uhr festzulegen, geben Sie die folgende Option und den folgenden Wert in der Serveroptionsdatei an:





```
reorgbegintime 20:30
```

- b. Definieren Sie das Intervall, in dem der Server die Reorganisation starten kann. Um beispielsweise anzugeben, dass der Server die Reorganisation innerhalb von 4 Stunden nach dem mit der Serveroption `REORGBEGINTIME` definierten Zeitpunkt starten kann, geben Sie die folgende Option und den folgenden Wert in der Serveroptionsdatei an:

```
reorgduration 4
```

4. War der Server aktiv, während Sie die Serveroptionsdatei aktualisiert haben, stoppen Sie den Server und starten Sie ihn erneut.

#### Zugehörige Informationen:

-  [ALLOWREORGINDEX](#)
-  [ALLOWREORGTABLE](#)
-  [REORGBEGINTIME](#)
-  [REORGDURATION](#)

## Windows: Serverinstanz auf Windows-Systemen starten

In einer Produktionsumgebung ist die bevorzugte Methode zum Starten des Servers der Start als Windows-Dienst. In einer Umgebung, in der Sie rekonfigurieren, testen oder Verwaltungstasks ausführen, starten Sie den Server im Vordergrund oder verwenden Sie den Verwaltungsmodus.

### Vorbereitende Schritte

Wählen Sie eine der folgenden Methoden zum Starten des Servers aus:

#### Als Windows-Dienst

Diese Methode ist in einer Produktionsumgebung nützlich. Wenn Sie die Ausführung des Servers als Dienst konfigurieren, können Sie angeben, dass der Server bei jedem Systemstart automatisch startet.

#### Im Vordergrund

Diese Methode ist für die Konfiguration oder den Test des Servers nützlich. Wenn Sie den Server im Vordergrund starten, stellt IBM Spectrum Protect eine spezielle Administrator-ID mit dem Namen SERVER\_CONSOLE bereit. Alle Servernachrichten werden im Vordergrund angezeigt. Die Nachrichten können hilfreich sein, wenn Sie Startprobleme beheben müssen.

#### Im Verwaltungsmodus

Diese Methode ist bei der Ausführung von Verwaltungs- oder Rekonfigurationstasks nützlich. Wenn Sie den Server im Verwaltungsmodus starten, inaktivieren Sie damit Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten.

### Vorgehensweise

Befolgen Sie die Anweisungen für Ihr ausgewählte Option:

| Option                                    | Bezeichnung  |
|---|--|
| <b>Server als Windows-Dienst starten</b>  | <p>Führen Sie einen der folgenden Schritte aus, um den Server als Windows-Dienst zu starten:</p> <ul style="list-style-type: none"> <li>• Wenn Sie den Server mithilfe des Konfigurationsassistenten konfiguriert haben, führen Sie die folgenden Schritte aus:               <ol style="list-style-type: none"> <li>a. Befolgen Sie die Anweisungen in Windows: Server für den Start als Windows-Dienst konfigurieren, um den Server für den Start als Windows-Dienst zu konfigurieren.</li> <li>b. Befolgen Sie die Anweisungen in Windows: Server als Windows-Dienst starten, um den Server zu starten.</li> </ol> </li> <li>• Wenn Sie den Konfigurationsassistenten nicht verwendet haben, befolgen Sie die Anweisungen in Windows: Windows-Dienst manuell erstellen und konfigurieren, um den Windows-Dienst zu erstellen und zu konfigurieren.</li> </ul> |
| <b>Server im Vordergrund starten</b>      | Server im Hintergrund starten: Befolgen Sie die Anweisungen in Windows: Server im Vordergrund starten.   |
| <b>Server im Verwaltungsmodus starten</b> | Server im Verwaltungsmodus starten: Befolgen Sie die Anweisungen in Windows: Server im Verwaltungsmodus starten.   |

## Windows: Server für den Start als Windows-Dienst konfigurieren

Bevor Sie den Server als Windows-Dienst starten können, müssen Sie sicherstellen, dass Optionen und Zugriffsberechtigungen ordnungsgemäß definiert sind.

### Vorbereitende Schritte

Ein Windows-Dienst muss erstellt werden. Wenn Sie den Server mithilfe des Konfigurationsassistenten konfiguriert haben, wurde automatisch ein Windows-Dienst erstellt. In diesem Fall führen Sie diese Prozedur aus, um den Server für den Start als Windows-Dienst zu konfigurieren.

Wenn Sie keinen Assistenten verwendet haben, müssen Sie den Windows-Dienst manuell erstellen und konfigurieren. Führen Sie hierfür die Schritte in Windows: Windows-Dienst manuell erstellen und konfigurieren aus.

## Vorgehensweise

---

1. Klicken Sie im Windows-Menü Start auf Ausführen, geben Sie `services.msc` ein und klicken Sie auf OK.
2. Wählen Sie im Fenster Dienste die Serverinstanz aus, die als Dienst gestartet werden soll, und klicken Sie auf Eigenschaften. Wählen Sie beispielsweise TSM INST1 aus und klicken Sie auf Eigenschaften.
3. Um sicherzustellen, dass der Serverdienst automatisch gestartet wird, klicken Sie auf die Registerkarte Allgemein. Wählen Sie in der Liste bei Starttyp Automatisch aus.
4. Um den Benutzer zum Starten des Serverdienstes zu definieren, klicken Sie auf die Registerkarte Anmelden und führen Sie eine der folgenden Aktionen aus:
  - Wenn Sie den Serverdienst unter dem lokalen Systemkonto ausführen wollen, wählen Sie Lokales Systemkonto aus und klicken Sie auf OK.
  - Wenn der Serverdienst unter der Instanzbenutzer-ID ausgeführt werden soll, führen Sie folgende Aktionen aus:
    - a. Wählen Sie Dieses Konto aus und suchen Sie nach der Benutzer-ID, die Eigner der DB2-Serverinstanz ist und über Berechtigungen zum Starten des Servers verfügt.
    - b. Geben Sie im Fenster Benutzer auswählen im Feld Namen des auszuwählenden Objekts eingeben die Benutzer-ID ein.
    - c. Klicken Sie auf Namen überprüfen.
    - d. Klicken Sie zweimal auf OK.
5. Wenn der Serverdienst für die Ausführung unter dem lokalen Systemkonto konfiguriert wurde, müssen Sie dem lokalen Systemkonto Datenbankzugriffsberechtigung erteilen:
  - a. Melden Sie sich mit der Benutzer-ID an, die zum Erstellen der Serverdatenbank verwendet wurde. Dabei handelt es sich um die Benutzer-ID, die zur Ausführung des Dienstprogramms DSMSEV FORMAT zum Initialisieren der Serverdatenbank verwendet wurde. Wenn der Server mithilfe des Konfigurationsassistenten dsmicfgx konfiguriert wurde, handelt es sich um die Benutzer-ID, mit der die Instanz erstellt wurde.
  - b. Öffnen Sie ein DB2-Befehlsfenster. Wenn der Server unter Windows Server 2012 installiert ist, öffnen Sie das Fenster Start und klicken Sie auf DB2-Befehlsfenster - Administrator.
  - c. Geben Sie im DB2-Befehlsfenster die folgenden Befehle ein:


```
set DB2INSTANCE=server1
db2 connect to TSMDB1
db2 grant dbadm with dataaccess with accessctrl on database to user system
db2 grant secadm on database to user system
```

Tipp: Wenn der Serverdienst für die Ausführung unter dem lokalen Systemkonto konfiguriert ist, kann jeder Administrator im System auf die Datenbank zugreifen. Darüber hinaus kann jeder Administrator, der sich am System anmelden kann, den Server ausführen.

## Nächste Schritte

---

Befolgen Sie die Anweisungen in Windows: Server als Windows-Dienst starten, um den Dienst zu starten.

 Windows-Betriebssysteme

## Windows: Server als Windows-Dienst starten

---

Wenn Sie IBM Spectrum Protect unter einem Windows-Betriebssystem ausführen, können Sie den Server als Dienst starten.

## Vorbereitende Schritte

---

Ein Windows-Dienst muss erstellt werden. Der Dienst wurde automatisch erstellt, wenn Sie den Server mithilfe des Konfigurationsassistenten konfiguriert haben. Wenn der Dienst automatisch erstellt wurde, müssen Sie den Start des Servers als Dienst konfigurieren. Führen Sie hierfür die Schritte in Windows: Server für den Start als Windows-Dienst konfigurieren aus. Führen Sie anschließend die Schritte dieser Prozedur aus, um den Server als Dienst zu starten.

Wenn Sie den Dienst nicht mithilfe des Konfigurationsassistenten erstellt haben, müssen Sie den Dienst manuell erstellen und konfigurieren. Führen Sie die Schritte in Windows: Windows-Dienst manuell erstellen und konfigurieren aus.

## Vorgehensweise

---

Gehen Sie wie folgt vor, um den Server als Windows-Dienst zu starten:

1. Melden Sie sich beim Server mit einer Benutzer-ID an, die zur Gruppe 'Administratoren' gehört.
2. Klicken Sie im Windows-Menü Start auf Ausführen, geben Sie `services.msc` ein und klicken Sie auf OK.
3. Wählen Sie im Fenster Dienste die Serverinstanz aus, die Sie starten wollen, und klicken Sie auf Starten.

## Nächste Schritte

---

Da der Serverdienst Anforderungen ausgeben kann, die eine Aktion erfordern, muss die Serveraktivität mit dem Operations Center oder dem Verwaltungsclient überwacht werden.

Um Abschlussnachrichten für das Starten und Stoppen anzuzeigen, die im Anwendungsprotokoll von Windows protokolliert sind, verwenden Sie das Tool Ereignisanzeige im Ordner Verwaltung.

 Windows-Betriebssysteme

## Windows: Windows-Dienst manuell erstellen und konfigurieren

---

Wenn Sie den Server mithilfe des Konfigurationsassistenten konfiguriert hatten, wurde automatisch ein Windows-Dienst erstellt. Wenn kein Dienst automatisch erstellt wurde, müssen Sie ihn erstellen.

### Vorbereitende Schritte

---

Für diese Prozedur müssen Sie sich mit einer Benutzer-ID anmelden, die zur Gruppe 'Administratoren' gehört.

### Vorgehensweise

---

Gehen Sie wie folgt vor, um einen Windows-Dienst zu erstellen und die Startoptionen für den Dienst zu konfigurieren:

Öffnen Sie ein Befehlsfenster und geben Sie den Befehl `sc.exe create` ein:

```
sc.exe create Servername binPath= "Serverpfad -k Instanzname"  
start= Starttyp obj= Kontoname password= Kennwort
```

Hierbei gilt Folgendes:

***Servername***

Gibt den Namen des Serverdienstes an.

***Serverpfad***

Gibt den Pfad zur ausführbaren Datei `dsmsvc.exe` und den Dateinamen an. Der Standardpfad lautet:

`C:\Programme\Tivoli\TSM\server`

***Instanzname***

Gibt den Namen der DB2-Instanz an, der mit dem Namen der Serverinstanz identisch ist, z. B. `Server1`.

***Starttyp***

Gibt die Startmethode für den Dienst an. Soll der Dienst automatisch gestartet werden, geben Sie `auto` ein. Wenn Sie die Option `auto` angeben, wird der Dienst automatisch beim Systemstart gestartet und bei jedem Neustart des Systems automatisch erneut gestartet. Soll der Dienst manuell gestartet werden, geben Sie `demand` ein.

***Kontoname***

Gibt die Benutzer-ID für das Konto an, unter dem der Dienst ausgeführt wird. Der Kontoname könnten z. B. 'Administrator' lauten. Dieser Parameter ist optional. Wird er nicht angegeben, wird das Konto 'Lokales System' verwendet.

***Kennwort***


Gibt das Kennwort für das Benutzerkonto *Kontoname* an.

Tipp: Achten Sie bei der Befehlseingabe darauf, dass hinter jedem Gleichheitszeichen (=) ein Leerzeichen eingegeben wird.

### Ergebnisse

---

Der Server wird als Windows-Dienst gestartet.

 Windows-Betriebssysteme

## Windows: Server im Vordergrund starten

---

Um direkt mit dem IBM Spectrum Protect-Server interagieren zu können, starten Sie den Server im Vordergrund. Wenn Sie beispielsweise Befehle eingeben möchten, starten Sie den Server im Vordergrund.

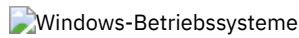
### Vorgehensweise

---

1. Wechseln Sie in das Verzeichnis, in dem der Server installiert ist. Wechseln Sie beispielsweise in das Verzeichnis `c:\Programme\tivoli\tsm\server`.
2. Geben Sie den folgenden Befehl ein:

```
dsmserv -k Instanzname
```

Dabei gibt *Instanzname* die Serverinstanz an.

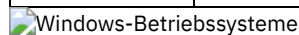


## Windows: Dem Server zugeordnete Services auf Windows-Systemen

Wenn Sie den IBM Spectrum Protect-Server als Dienst starten, starten andere Services automatisch. Diese Services sind dem Datenbankmanager, DB2, zugeordnet.

Die folgenden Services sind dem Server zugeordnet.

| ServiceName                                  | Zweck  | Kommentare  |
|--|--|---|
| TSM<br><i>Serverinstanz</i><br>Z             | Der Service für die Serverinstanz mit dem Namen <i>Serverinstanz</i> .<br><br>Zum Beispiel: TSM <i>Server1</i>             | Definieren Sie die Start- und Stoppoptionen für diesen Service, um die Serverinstanz automatisch zu starten und zu stoppen.<br><br>Jede Serverinstanz wird als separater Service ausgeführt.  |
| DB2 - DB2TSM1<br>-<br>SERVERINSTANZ<br>Z     | Der DB2-Service für die Serverinstanz mit dem Namen <i>Serverinstanz</i> .<br><br>Zum Beispiel: DB2 - DB2TSM1 -<br>SERVER1 | Dieser Service wird automatisch gestartet, wenn der Service für die Serverinstanz gestartet wird. Der DB2-Service wird nicht automatisch gestoppt, wenn Sie den Service für den Server stoppen.<br><br>Das System verfügt über einen dieser Services für jeden Serverinstanzservice, der auf dem System gestartet wird. |
| DB2 Governor<br>(DB2TSM1)                    | Ein DB2-Service, der während der Installation erstellt wird und für alle Serverinstanzen benötigt wird.                    | Ändern Sie nicht die Optionen für diesen Service.   |
| DB2 License<br>Server<br>(DB2TSM1)           | Ein DB2-Service, der während der Installation erstellt wird und für alle Serverinstanzen benötigt wird.                    | Ändern Sie nicht die Optionen für diesen Service.   |
| DB2<br>Management<br>Server<br>(DB2TSM1)     | Ein DB2-Service, der während der Installation erstellt wird und für alle Serverinstanzen benötigt wird.                    | Ändern Sie nicht die Optionen für diesen Service.   |
| DB2 Remote<br>Command<br>Server<br>(DB2TSM1) | Ein DB2-Service, der während der Installation erstellt wird und für alle Serverinstanzen benötigt wird.                    | Ändern Sie nicht die Optionen für diesen Service.   |



## Windows: Server im Verwaltungsmodus starten

Sie können den Server im Verwaltungsmodus starten, um Unterbrechungen während Verwaltungs- oder Rekonfigurationstasks zu vermeiden.

### Informationen zu diesem Vorgang

Führen Sie das Dienstprogramm DSMSEV mit dem Parameter MAINTENANCE aus, um den Server im Verwaltungsmodus zu starten.

Die folgenden Operationen sind im Verwaltungsmodus inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Wiederherstellung von Speicherbereich auf dem Server
- Bestandsverfall
- Umlagerung von Speicherpools

Außerdem wird verhindert, dass Clients Sitzungen mit dem Server starten.

Tipps:

- Sie müssen die Serveroptionsdatei dmserv.opt nicht bearbeiten, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Prozesse für die Speicherbereichswiederherstellung, den Bestandsverfall und die Speicherpoolumlagerung manuell starten.

### Vorgehensweise

Geben Sie den folgenden Befehl aus, um den Server im Verwaltungsmodus zu starten:

```
dsmserve maintenance
```

Tipp: Ein Video zum Starten des Servers im Verwaltungsmodus kann unter [Server im Verwaltungsmodus starten](#) angezeigt werden.

## Nächste Schritte

---

Gehen Sie wie folgt vor, um den Serverbetrieb im Produktionsmodus fortzusetzen:

1. Geben Sie den Befehl HALT aus, um den Server herunterzufahren:

```
halt
```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden.

Die während des Verwaltungsmodus inaktivierten Operationen werden wieder aktiviert.

## Windows: Server stoppen

---

Sie können den Server bei Bedarf stoppen, um die Steuerung an das Betriebssystem zurückzugeben. Um den Verlust von Verwaltungs- und Clientknotenverbindungen zu vermeiden, stoppen Sie den Server erst nach Beendigung oder Abbruch laufender Sitzungen.

### Informationen zu diesem Vorgang

---

Geben Sie den folgenden Befehl in die IBM Spectrum Protect-Befehlszeile ein, um den Server zu stoppen:

```
halt
```

## Windows: Lizenzregistrierung

---

Registrieren Sie alle lizenzierten IBM Spectrum Protect-Funktionen, die Sie beziehen, sofort, damit Sie nach dem Starten der Serveroperationen (z. B. Datensicherung) keine Daten verlieren.

### Informationen zu diesem Vorgang

---

Verwenden Sie hierfür den Befehl REGISTER LICENSE. Weitere Informationen siehe REGISTER LICENSE.

### Beispiel: Lizenz registrieren

---

Die IBM Spectrum Protect-Basislizenz registrieren.

```
register license file=tsmbasic.lic
```

## Windows: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben

---

Sie müssen die zu verwendende Einheitenklasse angeben, um das System für automatische oder manuelle Datenbanksicherungen vorzubereiten.

### Vorbereitende Schritte

---

Stellen Sie sicher, dass eine Bandeinheitenklasse oder eine Einheitenklasse FILE definiert wurde. Ausführliche Informationen finden Sie in DEFINE DEVCLASS oder suchen Sie nach 'Einheitenklasse definieren'.

### Informationen zu diesem Vorgang

---

Gehen Sie wie folgt vor, um Ihr System für Datenbanksicherungen zu konfigurieren.

### Vorgehensweise

---

1. Wenn Sie den Server nicht mit dem Konfigurationsassistenten (dsmicfgx) konfiguriert haben, müssen Sie sicherstellen, dass die Schritte zur manuellen Konfiguration des Systems für Datenbanksicherungen ausgeführt werden.



- Wählen Sie die für Datenbanksicherungen zu verwendende Einheitenklasse aus. Geben Sie den folgenden Befehl über eine IBM Spectrum Protect-Verwaltungsbefehlszeile aus.

```
set dbrecovery Einheitenklassenname
```

Die angegebene Einheitenklasse wird vom Datenbankmanager für Datenbanksicherungen verwendet. Wenn Sie keine Einheitenklasse mit dem Befehl SET DBRECOVERY angeben, schlägt die Sicherung fehl.

## Beispiel

---

Geben Sie beispielsweise den folgenden Befehl aus, um anzugeben, dass die Einheitenklasse DBBACK verwendet werden soll:


```
set dbrecovery dbback
```

## Windows: Mehrere Serverinstanzen auf einem System ausführen

---

Sie können mehrere Serverinstanzen auf Ihrem System erstellen. Jede Serverinstanz verfügt über ein eigenes Instanzverzeichnis sowie über Datenbank- und Protokollverzeichnisse.


Multiplizieren Sie den Speicherbedarf und andere Systemvoraussetzungen für einen Server mit der geplanten Instanzzahl für das System.


 Die Gruppe der Dateien für eine Instanz des Servers wird getrennt von den Dateien gespeichert, die von einer anderen Serverinstanz auf demselben System verwendet werden. Gehen Sie wie in Windows: Serverinstanz erstellen beschrieben für jede neue Instanz vor, mit wahlweiser Erstellung des neuen Instanzbenutzers.

Zur Verwaltung des von jedem Server verwendeten Systemspeichers begrenzen Sie mit der Serveroption DBMEMPERCENT den Prozentsatz des Systemspeichers. Haben alle Server denselben Stellenwert, verwenden Sie für jeden Server denselben Wert. Ist ein Server ein Produktionsserver und andere Server sind Testserver, geben Sie für den Produktionsserver einen höheren Wert an als für die Testserver.


Von Version 7.1 auf Version 8.1 ist ein direktes Upgrade möglich. Weitere Informationen finden Sie im Abschnitt über das Upgrade (Upgrade auf Version 8.1 durchführen). Wenn Sie ein Upgrade durchführen und mehrere Server auf dem System haben, müssen Sie den Installationsassistenten nur einmal ausführen. Der Installationsassistent erfasst die Datenbank- und Variablendaten für alle ursprünglichen Serverinstanzen.

Wenn Sie ein Upgrade von IBM Spectrum Protect Version 6.3 auf Version 8.1.3 durchführen und sich mehrere Server auf Ihrem System befinden, werden alle in DB2 Version 9.7 vorhandenen Instanzen gelöscht und in DB2 Version 11.1 erneut erstellt. Der Assistent gibt den Befehl `db2 upgrade DB DB-Name` für jede Datenbank aus. Die Datenbankumgebungsvariablen für jede Instanz auf Ihrem System werden ebenfalls während des Upgradeprozesses neu konfiguriert.

 Zu einer IBM Spectrum Protect-Standardinstallation gehört eine Serverinstanz auf dem IBM Spectrum Protect-Server-Computer. Sie können eine zweite Instanz installieren, wenn Sie eine Clusterumgebung konfigurieren. Sie können auch mehrere Server auf einem großen Computer ausführen, wenn Sie über mehrere Bandarchive oder über eine Konfiguration verfügen, die nur aus Plattenspeicher besteht. Nach der Installation und Konfiguration des ersten IBM Spectrum Protect-Servers erstellen Sie mithilfe des Assistenten für Serverinitialisierung weitere IBM Spectrum Protect-Serverinstanzen auf demselben Computer.

 Mithilfe des Assistenten für Serverinitialisierung können Sie bis zu vier IBM Spectrum Protect-Serverinstanzen in einem einzelnen System oder Cluster installieren.

### Zugehörige Tasks:

-  Mehrere Serverinstanzen auf einem einzigen System ausführen (Version 7.1.1)

## Windows: Server überwachen

---

Wenn Sie den Server im Produktionsbetrieb einsetzen, überwachen Sie den von ihm verwendeten Speicherbereich, um sicherzustellen, dass die Größe des Speicherbereichs angemessen ist. Ändern Sie den Speicherbereich, falls erforderlich.

### Vorgehensweise

---

- Überwachen Sie die aktive Protokolldatei, um sicherzustellen, dass die Größe für die Auslastung der Serverinstanz korrekt ist.

Wenn die Serverauslastung ihren normalen erwarteten Stand erreicht hat, belegt der von der aktiven Protokolldatei verwendete Speicherbereich 80 bis 90 Prozent des Speicherbereichs, der für das Verzeichnis für aktive Protokolldateien zur Verfügung steht. An diesem Punkt müssen Sie den Speicherbereich möglicherweise vergrößern. Die Vergrößerung des Speicherbereichs ist von der

Art der Transaktionen in der Serververarbeitung abhängig. Transaktionsmerkmale wirken sich auf die Belegung des Speicherbereichs der aktiven Protokolldateien aus.

Die folgenden Transaktionsmerkmale können sich auf die Speicherbereichsbelegung in der aktiven Protokolldatei auswirken:

- Die Anzahl und Größe der Dateien in Sicherungsoperationen
  - Clients, wie z. B. Dateiserver, die zahlreiche kleine Dateien sichern, können zahlreiche Transaktionen verursachen, die in kurzer Zeit ausgeführt werden. Die Transaktionen können sehr viel Speicherbereich in der aktiven Protokolldatei belegen, jedoch nur für kurze Zeit.
  - Clients, wie z. B. E-Mail-Server oder ein Datenbankserver, die große Datenvolumen in wenigen Transaktionen sichern, können wenige Transaktionen verursachen, deren Ausführung viel Zeit in Anspruch nimmt. Die Transaktionen können wenig Speicherbereich in der aktiven Protokolldatei belegen, jedoch für lange Zeit.
- Netzwerktypen
  - Mit schnellen Netzwerkverbindungen ausgeführte Sicherungsoperationen verursachen Transaktionen, die schneller ausgeführt werden. Die Transaktionen belegen Speicherbereich in der aktiven Protokolldatei über einen kürzeren Zeitraum.
  - Mit langsameren Verbindungen ausgeführte Sicherungsoperationen verursachen Transaktionen, deren Ausführung länger dauert. Die Transaktionen belegen Speicherbereich in der aktiven Protokolldatei über einen längeren Zeitraum.

Wenn der Server Transaktionen mit sehr unterschiedlichen Merkmalen verarbeitet, kann der für die aktive Protokolldatei verwendete Speicherbereich im Lauf der Zeit sehr stark schwanken. Für einen solchen Server müssen Sie unter Umständen dafür sorgen, dass ein niedrigerer Prozentsatz des Speicherbereichs der aktiven Protokolldatei verwendet wird. Der zusätzliche Speicherbereich gestattet eine Vergrößerung der aktiven Protokolldatei für Transaktionen, die viel Zeit in Anspruch nehmen.

## 2. Überwachen Sie das Archivprotokoll, um sicherzustellen, dass immer Speicherbereich verfügbar ist.

Hinweis: Wenn das Archivprotokoll und das Übernahmearchivprotokoll voll werden, kann die aktive Protokolldatei voll werden, so dass der Server stoppt. Für das Archivprotokoll muss so viel Speicherbereich zur Verfügung stehen, dass dieser niemals vollständig belegt wird.

Sie werden wahrscheinlich Folgendes feststellen:

- a. Am Anfang wird das Archivprotokoll schnell größer, wenn normale Clientsicherungsoperationen ausgeführt werden.
- b. Datenbanksicherungen werden regelmäßig ausgeführt, entweder mit einem Zeitplan oder manuell.
- c. Nach mindestens zwei Datenbankgesamticherungen wird das Abschneiden des Protokolls automatisch ausgeführt. Der vom Archivprotokoll belegte Speicherbereich verringert sich durch das Abschneiden.
- d. Normale Clientoperationen werden fortgesetzt und das Archivprotokoll wird wieder größer.
- e. Datenbanksicherungen finden regelmäßig statt und die Häufigkeit der Protokollbereinigung ist von der Häufigkeit der Datenbankgesamticherungen abhängig.

Nach diesem Muster nimmt die Größe des Archivprotokolls zunächst zu, verringert sich und nimmt dann eventuell wieder zu. Im Laufe der Zeit sollte der vom Archivprotokoll belegte Speicherbereich während der normalen Verarbeitung einen relativ konstanten Stand erreichen.

Wenn die Größe des Archivprotokolls weiter zunimmt, sollten Sie eine oder beide der folgenden Maßnahmen in Betracht ziehen:

- Ordnen Sie dem Archivprotokoll weiteren Speicherbereich zu. Sie müssen unter Umständen das Archivprotokoll in ein anderes Dateisystem versetzen.
  - Erhöhen Sie die Häufigkeit der Datenbankgesamticherungen, so dass die Protokollbereinigung häufiger stattfindet.
3. Wenn Sie ein Verzeichnis für das Übernahmearchivprotokoll definiert haben, überprüfen Sie, ob darin Protokolle während der normalen Verarbeitung gespeichert werden. Wenn der Speicherbereich des Übernahmeprotokolls verwendet wird, sollten Sie das Archivprotokoll vergrößern. Das Übernahmearchivprotokoll sollte nur unter außergewöhnlichen Bedingungen verwendet werden, nicht während der normalen Verarbeitung.

## Windows: IBM Spectrum Protect-Server-Fixpack installieren

---

IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe.

### Vorbereitende Schritte

---

Damit ein Fixpack oder ein vorläufiger Fix auf dem Server installiert werden kann, müssen Sie den Server mit der Stufe installieren, auf der er ausgeführt werden soll. Sie müssen die Serverinstallation nicht mit dem Basisrelease beginnen. Wenn momentan beispielsweise Version 8.1.1 installiert ist, können Sie das aktuelle Fixpack für Version 8.1 direkt verwenden. Sie müssen nicht mit der Installation von Version 8.1.0 beginnen, wenn eine Wartungsaktualisierung verfügbar ist.

Das IBM Spectrum Protect-Lizenzpaket muss installiert sein. Das Lizenzpaket wird beim Kauf eines Basisreleases bereitgestellt. Wenn Sie ein Fixpack oder einen vorläufigen Fix von Fix Central herunterladen, installieren Sie die Serverlizenz, die auf der Website von

Passport Advantage zur Verfügung steht. Sollen Nachrichten und Hilfetext nicht in Englisch angezeigt werden, installieren Sie das gewünschte Sprachenpaket.

Wenn Sie ein Upgrade des Servers auf Version 8.1.3 oder höher durchführen und den Server dann auf einen Stand vor Version 8.1.3 zurücksetzen, müssen Sie die Datenbank auf einen Zeitpunkt vor dem Upgrade zurückschreiben. Führen Sie während des Upgrades die erforderlichen Schritte aus, mit denen sichergestellt wird, dass die Datenbank zurückschrieben werden kann: Sichern Sie die Datenbank, die Protokolldatei für Datenträger, die Einheitenkonfigurationsdatei und die Serveroptionsdatei. Weitere Informationen finden Sie in Windows: Von Version 8.1.3 auf eine vorherige Serverversion zurücksetzen.

Wenn Sie den Clientverwaltungsservice verwenden, müssen Sie ein Upgrade dieses Service auf dieselbe Version wie beim IBM Spectrum Protect-Server durchführen.

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease des installierten Servers aufbewahrt werden. Wenn Sie IBM Spectrum Protect über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, sind die Installationsmedien für das Basisrelease des Servers für die Neuinstallation der Lizenz erforderlich.

Rufen Sie das IBM® Support Portal auf. Hier finden Sie folgende Informationen:

- Eine Liste der neuesten Wartungs- und Download-Fixes. Klicken Sie auf **Download** und legen Sie alle gültigen Fixes an.
- Informationen zum Erwerb eines Basislizenzpakets. Suchen Sie nach **Downloads > Passport Advantage**.
- Unterstützte Plattformen und Systemvoraussetzungen. Suchen Sie nach **IBM Spectrum Protect supported operating systems**.

Sie müssen ein Upgrade des Servers durchführen, bevor Sie ein Upgrade der Clients für Sichern/Archivieren durchführen. Wenn Sie das Upgrade des Servers nicht zuerst durchführen, könnte die Kommunikation zwischen dem Server und den Clients unterbrochen werden.

Achtung: Sie dürfen die DB2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der DB2-Software und führen Sie kein Upgrade durch, da dies die Datenbank beschädigen kann.

## Vorgehensweise

---

Führen Sie die folgenden Schritte aus, um ein Fixpack oder einen vorläufigen Fix zu installieren:

1. Sichern Sie die Datenbank. Die bevorzugte Methode ist eine Momentaufnahmesicherung. Bei einer Momentaufnahmesicherung handelt es sich um eine Datenbankgesamtsicherung, bei der geplante Datenbanksicherungen nicht unterbrochen werden. Geben Sie beispielsweise den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Sichern Sie die Einheitenkonfigurationsdaten. Geben Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:


```
backup devconfig filenames=Dateiname
```

*Dateiname* gibt den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.

3. Speichern Sie die Protokolldatei für Datenträger in einem anderen Verzeichnis oder benennen Sie die Datei um. Geben Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

```
backup volhistory filenames=Dateiname
```

*Dateiname* gibt den Namen der Datei an, in der Datenträgerhistory-Informationen (Datenträgerprotokolldaten) gespeichert werden sollen.

4. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dsmserv.opt heißt. Die Datei befindet sich im Serverinstanzverzeichnis.
5. Halten Sie den Server vor der Installation eines Fixpacks oder eines vorläufigen Fixes an. Verwenden Sie den Befehl HALT.
6. Stellen Sie sicher, dass im Installationsverzeichnis zusätzlicher Speicherplatz zur Verfügung steht. Für die Installation dieses Fixpacks kann zusätzlicher temporärer Plattenspeicherplatz im Installationsverzeichnis des Servers erforderlich sein. Die Größe des zusätzlichen Plattenspeicherplatzes kann der Größe entsprechen, die für die Installation einer neuen Datenbank während einer IBM Spectrum Protect-Installation benötigt wird. Der IBM Spectrum Protect-Installationsassistent zeigt an, wie viel Speicherplatz für die Installation des Fixpacks benötigt wird und wie viel Platz zur Verfügung steht. Wenn der erforderliche Speicherplatz größer ist als der verfügbare Speicherplatz, stoppt die Installation. Wenn die Installation stoppt, fügen Sie dem Dateisystem den erforderlichen Plattenspeicherplatz hinzu und starten Sie die Installation erneut.
7. Laden Sie die Paketdatei für das Fixpack bzw. den vorläufigen Fix, das bzw. der installiert werden soll, über IBM Support Portal, Passport Advantage oder Fix Central herunter.
8.  Windows-Betriebssysteme Wechseln Sie in das Verzeichnis, in dem sich die ausführbare Datei befindet. Klicken Sie dann entweder doppelt auf die folgende ausführbare Datei oder geben Sie den folgenden Befehl in die Befehlszeile ein, um die Installationsdateien zu extrahieren.

Tipp: Die Dateien werden in das aktuelle Verzeichnis extrahiert. Stellen Sie sicher, dass sich die ausführbare Datei in dem Verzeichnis befindet, in dem sich die extrahierten Dateien befinden sollen.

Hierbei steht *Plattform* für das Betriebssystem, in dem IBM Spectrum Protect installiert werden soll.

9. Wählen Sie eine der folgenden Möglichkeiten für die Installation von IBM Spectrum Protect aus.

Wichtig: Nach der Installation eines Fixpacks muss die Konfiguration nicht wiederholt werden. Sie können nach Beendigung der Installation stoppen, alle Fehler beheben und dann Ihre Server erneut starten.

Installieren Sie die IBM Spectrum Protect-Software mit einer der folgenden Methoden:

#### Installationsassistent

Befolgen Sie die Anweisungen für Ihr Betriebssystem:

Windows: IBM Spectrum Protect mit dem Installationsassistenten installieren

Tipp: Klicken Sie nach dem Start des Assistenten im Fenster von IBM Installation Manager auf das Symbol Aktualisieren. Klicken Sie nicht auf das Symbol Installieren oder Ändern.

#### Befehlszeile im Konsolenmodus

Befolgen Sie die Anweisungen für Ihr Betriebssystem:

Windows: IBM Spectrum Protect im Konsolenmodus installieren

#### Unbeaufsichtigter Modus

Befolgen Sie die Anweisungen für Ihr Betriebssystem:

Windows: IBM Spectrum Protect im unbeaufsichtigten Modus installieren

Tipp: Befinden sich mehrere Serverinstanzen auf Ihrem System, führen Sie den Installationsassistenten nur einmal aus. Der Installationsassistent führt ein Upgrade aller Serverinstanzen durch.



## Ergebnisse

---

Beheben Sie alle Fehler, die während des Installationsprozesses festgestellt werden.

Wenn Sie den Server mithilfe des Installationsassistenten installiert haben, können Sie Installationsprotokolle mithilfe des Tools IBM Installation Manager anzeigen. Klicken Sie auf Datei > Protokoll anzeigen. Um Protokolldateien zu erfassen, klicken Sie in IBM Installation Manager auf Hilfe > Daten zur Fehleranalyse exportieren.

Wenn Sie den Server im Konsolenmodus oder im unbeaufsichtigten Modus installiert haben, können Sie Fehlerprotokolle im IBM Installation Manager-Protokollverzeichnis anzeigen. Zum Beispiel:

-  Windows-BetriebssystemeC:\Programme\IBM\Installation Manager\logs
-  Windows-BetriebssystemeWindows: Fixpack auf IBM Spectrum Protect 8.1.3 in einer Clusterumgebung unter Windows anwenden  
Damit neue Produktfunktionen genutzt werden können, können Sie ein Upgrade eines Servers, der unter einem Windows-Betriebssystem in einer Clusterumgebung installiert ist, von Version 6.3 oder Version 7.1 auf IBM Spectrum Protect Version 8.1.3 durchführen.

## Windows: Von Version 8.1.3 auf eine vorherige Serverversion zurücksetzen

---

Wenn Sie nach einem Upgrade auf die vorherige Version des Servers zurücksetzen müssen, benötigen Sie eine Datenbankgesamtsicherung der ursprünglichen Version. Außerdem benötigen Sie die Serverinstallationsmedien für Ihre ursprüngliche Version und Schlüsselkonfigurationsdateien. Führen Sie die Schritte zur Vorbereitung sorgfältig aus, bevor Sie das Upgrade des Servers durchführen. Dadurch könnte das Zurücksetzen auf die vorherige Version des IBM Spectrum Protect-Servers mit minimalem Datenverlust möglich sein.

### Vorbereitende Schritte

---

Sie benötigen die folgenden Elemente aus der früheren Version des Servers:


- Serverdatenbanksicherung
- Protokolldatei für Datenträger
- Einheitenkonfigurationsdatei
- Serveroptionsdatei

### Informationen zu diesem Vorgang

---

Die Anweisungen sind für das Zurücksetzen innerhalb eines Releases oder von einem Release auf ein vorheriges Release identisch, z. B. von 8.1.3 auf 8.1.2 oder von 8.1.3 auf 7.1.2. Die ältere Version muss mit der Version übereinstimmen, die Sie vor dem Upgrade auf Version 8.1 verwendet haben.

Achtung: Geben Sie den Parameter REUSEDELAY an, um den Verlust von Daten des Clients für Sichern/Archivieren verhindern zu helfen, wenn Sie den Server auf eine vorherige Version zurücksetzen.

-  Windows-Betriebssysteme: Zurücksetzen auf vorherige Serverversion in einer Clusterkonfiguration  
Wenn Sie nach einem Upgrade auf die vorherige Version des Servers zurücksetzen müssen, benötigen Sie eine Datenbankgesamtsicherung der ursprünglichen Version. Außerdem benötigen Sie die Serverinstallationsmedien für Ihre ursprüngliche Version und Schlüsselkonfigurationsdateien. Führen Sie die Schritte zur Vorbereitung sorgfältig aus, bevor Sie das Upgrade des Servers durchführen. Dadurch könnte das Zurücksetzen auf die vorherige Version des IBM Spectrum Protect-Servers mit minimalem Datenverlust möglich sein.


## Vorgehensweise beim Zurücksetzen auf vorherige Serverversion


---

### Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte auf dem System aus, auf dem sich der Server der Version 8.1 befindet.

### Vorgehensweise

1. Stoppen Sie den Server, um alle Serveroperationen zu beenden. Verwenden Sie hierfür den Befehl HALT.
2. Entfernen Sie die Datenbank aus dem Datenbankmanager und löschen Sie anschließend die Datenbank- und Wiederherstellungsprotokollverzeichnisse.
  - a. Entfernen Sie die Datenbank manuell. Eine Möglichkeit zum Entfernen ist der folgende Befehl:  
  

```
dsmserv -k Instanzname removedb tsmdbl
```
  - b. Wenn Sie den von den Datenbank- und Wiederherstellungsprotokollverzeichnissen belegten Speicherplatz wiederverwenden müssen, können Sie diese Verzeichnisse jetzt löschen.
3. Deinstallieren Sie den Server der Version 8.1 mit dem Deinstallationsprogramm. Bei der Deinstallation werden der Server und der Datenbankmanager mit den jeweiligen Verzeichnissen entfernt. Ausführliche Informationen siehe Windows: IBM Spectrum Protect deinstallieren.
4. Stoppen Sie den Clusterdienst. Installieren Sie die Version des Serverprogramms, die Sie vor dem Upgrade auf Version 8.1.3 verwendet haben, erneut. Diese Version muss mit der Version übereinstimmen, die auf Ihrem Server verwendet wurde, als Sie die Datenbanksicherung erstellt haben, die Sie zu einem späteren Zeitpunkt wiederherstellen wollen. Wenn der Server vor dem Upgrade z. B. die Version 7.1.7 hatte und wenn Sie die Datenbanksicherung verwenden wollen, die auf diesem Server verwendet wurde, müssen Sie das Fixpack V7.1.7 installieren, damit Sie die Datenbanksicherung zurückschreiben können.
5. Konfigurieren Sie die neue Serverdatenbank mithilfe des Konfigurationsassistenten. Geben Sie den folgenden Befehl aus, um den Assistenten zu starten:   

```
/dsmicfgx
```
6. Stellen Sie sicher, dass keine Server im Hintergrund ausgeführt werden.
7. Schreiben Sie die Datenbank zu einem Zeitpunkt vor dem Upgrade zurück.
8. Kopieren Sie die folgenden Dateien in das Instanzverzeichnis.
  - Einheitenkonfigurationsdatei
  - Protokolldatei für Datenträger
  - Serveroptionsdatei (normalerweise dsmserv.opt)
9. Wenn Sie die Datendeduplizierung für Speicherpools des Typs FILE, die vor dem Upgrade vorhanden waren, aktiviert haben oder wenn Sie während der Verwendung des Servers der Version 8.1.3 Daten, die vor dem Upgrade vorhanden waren, in neue Speicherpools verschoben haben, müssen Sie zusätzliche Schritte ausführen. Weitere Informationen finden Sie in Zusätzliche Wiederherstellungsschritte wegen der Erstellung neuer Speicherpools oder der Aktivierung der Datendeduplizierung.
10. Wenn die Einstellung des Parameters REUSEDELAY für Speicherpools das Alter der zurückgeschriebenen Datenbank unterschreitet, schreiben Sie Datenträger auf allen Speicherpools mit sequenziellem Zugriff, die nach dieser Datenbanksicherung wiederhergestellt wurden, zurück. Verwenden Sie den Befehl RESTORE VOLUME.  
Wenn keine Sicherung eines Speicherpools vorliegt, prüfen Sie die wiederhergestellten Datenträger mit dem Befehl AUDIT VOLUME und dem Parameter FIX=YES, um Inkonsistenzen zu beheben. Beispiel:  

```
audit volume Datenträgername fix=yes
```
11. Wurden mit dem Server der Version 8.1 Clientsicherungs- oder -archivierungsoperationen ausgeführt, prüfen Sie die Speicherpooldatenträger, auf denen die Daten gespeichert wurden.

## Zusätzliche Wiederherstellungsschritte wegen der Erstellung neuer Speicherpools oder der Aktivierung der Datendeduplizierung

---

Wenn Sie während der Ausführung des Servers mit Version 8.1.3 neue Speicherpools erstellt und/oder die Datendeduplizierung für Speicherpools des Typs FILE aktiviert haben, müssen Sie zusätzliche Schritte ausführen, um die vorherige Serverversion

wiederherzustellen.

## Vorbereitende Schritte

Für diese Task benötigen Sie eine Gesamtsicherung des Speicherpools, die vor dem Upgrade auf Version 8.1.3 erstellt wurde.

## Informationen zu diesem Vorgang

Verwenden Sie diese Informationen, wenn Sie einen oder beide der folgenden Schritte ausgeführt haben, während Ihr Server mit Version 8.1.3 ausgeführt wurde:

- Sie haben die Datendeduplizierungsfunktion für beliebige Speicherpools aktiviert, die vor dem Upgrade auf Version 8.1.3 bereits vorhanden waren. Die Datendeduplizierung ist nur für Speicherpools gültig, die den Einheitentyp FILE verwenden.
- Sie haben neue primäre Speicherpools nach dem Upgrade erstellt *und* Daten, die in anderen Speicherpools gespeichert waren, in die neuen Speicherpools versetzt.

Führen Sie diese Schritte aus, nachdem der Server wieder auf Version 7 zurückgesetzt wurde.

## Vorgehensweise

- Schreiben Sie für jeden Speicherpool, für den Sie die Datendeduplizierungsfunktion aktiviert haben, den gesamten Speicherpool mit dem Befehl RESTORE STGPOOL zurück.
- Bestimmen Sie für Speicherpools, die Sie nach dem Upgrade erstellt haben, welche Maßnahme durchzuführen ist. Daten, die aus vorhandenen Speicherpools der Version 8 in die neuen Speicherpools versetzt wurden, gehen möglicherweise verloren, weil die neuen Speicherpools auf Ihrem auf Version 8 zurückgesetzten Server nicht mehr vorhanden sind. Die Wiederherstellungsmaßnahmen sind vom Typ des Speicherpools abhängig:
  - Wurden Daten aus Speicherpools des Typs DISK der Version 8 in einen neuen Speicherpool versetzt, wurde der von den versetzten Daten belegte Speicherplatz wahrscheinlich wiederverwendet. Daher müssen Sie die ursprünglichen Speicherpools der Version 8 mithilfe der Speicherpoolsicherungen zurückschreiben, die vor dem Upgrade auf Version 8.1.3 erstellt wurden.

Wurden *keine* Daten aus Speicherpools des Typs DISK der Version 8 in einen neuen Speicherpool versetzt, müssen Sie die Speicherpooldatenträger in diesen Speicherpools des Typs DISK prüfen.
  - Wurden Daten aus Speicherpools mit sequenziellem Zugriff der Version 8 in einen neuen Speicherpool versetzt, sind diese Daten möglicherweise noch vorhanden und sie können eventuell auf Speicherpooldatenträgern auf dem wiederhergestellten Server der Version 8 verwendet werden. Die Daten können verwendbar sein, wenn für den Parameter REUSEDELAY des Speicherpools ein Wert definiert wurde, der die Wiederherstellung verhindert hat, während der Server mit der Version 8.1.3 ausgeführt wurde. Wurden Datenträger wiederhergestellt, während der Server mit der Version 8.1.3 ausgeführt wurde, müssen Sie diese Datenträger aus Speicherpoolsicherungen zurückschreiben, die vor dem Upgrade auf Version 8.1.3 erstellt wurden.

## Windows: Referenz: DB2-Befehle für IBM Spectrum Protect-Serverdatenbanken

Verwenden Sie diese Liste als Referenz, wenn der IBM® Support Sie anweist, DB2-Befehle auszugeben.





### Zweck

Nach der Installation und Konfiguration von IBM Spectrum Protect mithilfe der Assistenten müssen Sie DB2-Befehle nur selten verwenden. Eine begrenzte Gruppe von DB2-Befehlen, die Sie verwenden bzw. zu deren Verwendung Sie aufgefordert werden könnten, ist in Tabelle 1 aufgelistet. Diese Liste ist nicht umfassend, es handelt sich lediglich um ergänzende Informationen. Es besteht keine Implikation, dass ein IBM Spectrum Protect-Administrator sie täglich oder regelmäßig verwendet. Beispiele einiger Befehle sind angegeben. Ausgabedaten sind nicht enthalten.

Vollständige Erläuterungen zu den hier beschriebenen Befehlen und zu deren Syntax finden Sie in der Produktinformation zu DB2.

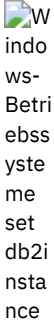

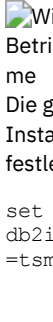
Tabelle 1. DB2-Befehle

| Befehl | Beschreibung | Beispiel |
|--------|--------------|----------|
|--------|--------------|----------|

| Befehl  | Beschreibung   | Beispiel  |
|---|--|---|
|  Windows-Betriebssysteme<br>db2cmd |  Windows-Betriebssysteme<br>Öffnet das DB2-Fenster mit dem Befehlszeilenprozessor und initialisiert die DB2-Befehlszeilenumgebung.  |  Windows-Betriebssysteme<br>DB2-Befehlsfenster öffnen:<br><br>db2cmd   |
| db2icrt   | <p>Erstellt DB2-Instanzen im Ausgangsverzeichnis des Instanzeigners.<br/>Tipp: Der IBM Spectrum Protect-Konfigurationsassistent erstellt die vom Server und von der Datenbank verwendete Instanz. Nach der Installation und Konfiguration eines Servers mithilfe des Konfigurationsassistenten wird der Befehl db2icrt in der Regel nicht verwendet.</p>  Windows-Betriebssysteme<br>Dieses Dienstprogramm befindet sich im Verzeichnis DB2PATH\bin. Hierbei steht DB2PATH für das Verzeichnis, in dem die DB2-Kopie installiert ist. | IBM Spectrum Protect-Instanz manuell erstellen (geben Sie den Befehl in einer einzigen Zeile ein):<br><br><pre> /opt/tivoli /tsm/db2/in stance/ db2icrt -a server -u Instanznam e Instanznam e           </pre> |
| db2set  | Zeigt DB2-Variablen an.  | DB2-Variablen auflisten:<br><br>db2set  |
| CATALOG DATABASE  | Speichert Informationen zur Speicherposition der Datenbank im Systemdatenbankverzeichnis. Die Datenbank kann sich auf der lokalen Workstation oder auf einem fernen Datenbankpartitionsserver befinden. Der Serverkonfigurationsassistent kümmert sich um jeden Katalog, der zur Verwendung der Serverdatenbank benötigt wird. Führen Sie diesen Befehl nach der Konfiguration und Aktivierung eines Servers nur dann manuell aus, wenn es eine Änderung oder Beschädigung in der Umgebung gibt.   | Datenbank katalogisieren:<br><br><pre> db2 catalog database tsmdb1           </pre>   |
| CONNECT TO DATABASE   | Stellt eine Verbindung zu einer angegebenen Datenbank für Befehlszeilenschnittstellenzwecke her.   | Eine Verbindung zur IBM Spectrum Protect-Datenbank über eine DB2-Befehlszeilenschnittstelle herstellen:<br><br><pre> db2 connect to tsmdb1           </pre>   |

| Befehl  | Beschreibung   | Beispiel  |
|---|--|---|
| GET<br>DAT<br>ABA<br>SE<br>CON<br>FIG<br>URA<br>TION                    | Gibt die Werte einzelner Einträge in einer bestimmten Datenbankkonfigurationsdatei zurück.<br>Wichtig: Dieser Befehl und seine Parameter werden direkt von DB2 definiert und verwaltet. Sie sind an dieser Stelle für Informationszwecke aufgelistet, um zu zeigen, wie die vorhandenen Einstellungen abgerufen werden können. Eine Änderung dieser Einstellungen könnte durch IBM Support oder Service-Bulletins wie z. B. APARs oder "Technical Guidance"-Dokumente (Technotes) empfohlen werden. Ändern Sie diese Einstellungen nicht manuell. Nehmen Sie eine Änderung nur nach einer entsprechenden Anweisung von IBM und nur mithilfe von IBM Spectrum Protect-Serverbefehlen oder -Prozeduren vor.  | Die Konfigurationsdaten für einen Datenbankaliasnamen anzeigen:<br><br>db2 get db<br>cfg for<br>tsmdb1<br><br>Informationen abrufen, um Einstellungen zu überprüfen (z. B. Datenbankkonfiguration, Protokollmodus und Pflege).<br><br>db2 get db<br>config for<br>tsmdb1<br>show detail |
| GET<br>DAT<br>ABA<br>SE<br>MAN<br>AGE<br>R<br>CON<br>FIG<br>URA<br>TION | Gibt die Werte einzelner Einträge in einer bestimmten Datenbankkonfigurationsdatei zurück.<br>Wichtig: Dieser Befehl und seine Parameter werden direkt von DB2 definiert und verwaltet. Sie sind an dieser Stelle für Informationszwecke aufgelistet, um zu zeigen, wie die vorhandenen Einstellungen abgerufen werden können. Eine Änderung dieser Einstellungen könnte durch IBM Support oder Service-Bulletins wie z. B. APARs oder "Technical Guidance"-Dokumente (Technotes) empfohlen werden. Ändern Sie diese Einstellungen nicht manuell. Nehmen Sie eine Änderung nur nach einer entsprechenden Anweisung von IBM und nur mithilfe von IBM Spectrum Protect-Serverbefehlen oder -Prozeduren vor.  | Konfigurationsdaten für den Datenbankmanager abrufen:<br><br>db2 get dbm<br>cfg   |
| GET<br>HEA<br>LTH<br>SNA<br>PSH<br>OT                                   | Ruft die Informationen zum Allgemeinzustand für den Datenbankmanager und seine Datenbanken ab. Die zurückgegebenen Informationen stellen eine Momentaufnahme des Status zum Zeitpunkt der Befehlsausgabe dar. IBM Spectrum Protect überwacht den Status der Datenbank mithilfe der Diagnosemomentaufnahme und anderer Mechanismen, die von DB2 bereitgestellt werden. Es kann vorkommen, dass die Diagnosemomentaufnahme oder andere DB2-Dokumentation anzeigt, dass sich ein Element bzw. eine Datenbankressource im Alertstatus befindet. In einem solchen Fall müssen entsprechende Schritte zur Behebung der Situation in Betracht gezogen werden. IBM Spectrum Protect überwacht die Bedingung und reagiert entsprechend. Nicht alle deklarierten Alerts der DB2-Datenbank haben Maßnahmen zur Folge. | Einen Bericht über Anzeiger des DB2-Diagnosemonitors abrufen:<br><br>db2 get<br>health<br>snapshot<br>for<br>database on<br>tsmdb1  |



| Befehl  | Beschreibung  | Beispiel  |
|---|---|---|
| GRANT<br>(Datenbankberechtigungen)  | Erteilt Berechtigungen, die sich auf die gesamte Datenbank beziehen, und keine Zugriffsrechte, die sich auf bestimmte Objekte in der Datenbank beziehen.  | Der Benutzer-ID itmuser Zugriffsberechtigung erteilen:<br><br>db2 GRANT<br>CONNECT ON<br>DATABASE<br>TO USER<br>itmuser<br>db2 GRANT<br>CREATETAB<br>ON DATABASE<br>TO USER<br>itmuser            |
| RUNSTATS  | Aktualisiert statistische Daten zu den Merkmalen einer Tabelle und der zugeordneten Indizes oder Statistiksichten. Zu diesen Merkmalen gehören die Anzahl der Datensätze, die Anzahl der Seiten und die durchschnittliche Datensatzlänge.<br><br>Soll eine Tabelle angezeigt werden, verwenden Sie dieses Dienstprogramm nach dem Aktualisieren oder Reorganisieren der Tabelle.<br><br>Eine Sicht muss für die Optimierung aktiviert sein, damit ihre statistischen Daten für die Optimierung einer Abfrage verwendet werden können. Eine für die Optimierung aktivierte Sicht wird als Statistiksicht bezeichnet. Sie können eine Sicht mit der DB2-Anweisung ALTER VIEW für die Optimierung aktivieren. Verwenden Sie das Dienstprogramm RUNSTATS, wenn sich Änderungen zugrunde liegender Tabellen auf die von der Sicht zurückgegebenen Zeilen auswirken.<br><br>Tipp: Der Server konfiguriert DB2 so, dass der Befehl RUNSTATS nach Bedarf ausgeführt wird. | Statistische Daten für eine einzelne Tabelle aktualisieren.<br><br>db2<br>runstats on<br>table<br>SCHEMA_NAME<br>.TABLE_NAME<br>with<br>distribution<br>and<br>sampled<br>detailed<br>indexes all |
|  Windows-Betriebssysteme set db2instance |  Windows-Betriebssysteme Legt fest, welche Instanz für die aktuelle Sitzung gültig ist.  |  Windows-Betriebssysteme Die gültige Instanz festlegen:<br><br>set<br>db2instance<br>=tsminst1               |
| SETSCHEMA   | Ändert den Wert des Sonderregisters CURRENT SCHEMA als Vorbereitung für die direkte Ausgabe von SQL-Befehlen über die DB2-Befehlszeilenschnittstelle.<br><br>Tipp: Ein Sonderregister ist ein Speicherbereich, den der Datenbankmanager für einen Anwendungsprozess definiert. In diesem Bereich werden Informationen gespeichert, auf die in SQL-Anweisungen verwiesen werden kann.  | Das Schema für IBM Spectrum Protect festlegen:<br><br>db2 set<br>schema<br>tsmdb1   |
| START DATABASE MANAGER  | Startet die Hintergrundprozesse der aktuellen Datenbankmanagerinstanz. Der Server startet und stoppt die Instanz und die Datenbank bei jedem Start und Stopp des Servers.<br><br>Wichtig: Lassen Sie den Server das Starten und Stoppen der Instanz und der Datenbank steuern, sofern keine anderweitige Anweisung durch IBM Support vorliegt.  | Den Datenbankmanager starten:<br><br>db2start   |

| Befehl        | Beschreibung   | Beispiel   |
|---------------|--|--|
| STOP          | Stoppt die aktuelle Datenbankmanagerinstanz. Der Datenbankmanager bleibt so lange aktiv, bis er explizit gestoppt wird. Dieser Befehl stoppt die Datenbankmanagerinstanz nicht, wenn Anwendungen mit Datenbanken verbunden sind. Liegen keine Datenbankverbindungen, aber Instanzverbindungen vor, erzwingt der Befehl zunächst das Stoppen der Instanzverbindungen. Dann wird der Datenbankmanager gestoppt. Dieser Befehl inaktiviert außerdem alle ausstehenden Datenbankaktivierungen, bevor der Datenbankmanager gestoppt wird. | Den Datenbankmanager stoppen:<br><br>db2 stop<br>dbm |
| DATASEMANAGER | Dieser Befehl ist auf einem Client nicht gültig.   |  |
|               | Der Server startet und stoppt die Instanz und die Datenbank bei jedem Start und Stopp des Servers.<br><br>Wichtig: Lassen Sie den Server das Starten und Stoppen der Instanz und der Datenbank steuern, sofern keine anderweitige Anweisung durch IBM Support vorliegt.  |  |


## Windows: IBM Spectrum Protect deinstallieren

Sie können IBM Spectrum Protect mit den folgenden Methoden deinstallieren. Vor dem Entfernen von IBM Spectrum Protect müssen Sie sicherstellen, dass Ihre Sicherungs- und Archivierungsdaten nicht verloren gehen.

### Vorbereitende Schritte

Führen Sie folgende Schritte aus, bevor Sie IBM Spectrum Protect deinstallieren:

- Führen Sie eine Gesamtsicherung der Datenbank aus.
- Speichern Sie eine Kopie der Datenträgerhistory- und Einheitenkonfigurationsdateien.
- Bewahren Sie die Ausgabedatenträger an einem sicheren Ort auf.

 **Windows-Betriebssysteme**Achtung: Verwenden Sie nicht das Tool zum Hinzufügen/Entfernen von Programmen in der Windows-Systemsteuerung, um IBM Spectrum Protect zu deinstallieren. Verwenden Sie nur die in diesem Abschnitt beschriebene Deinstallationsprozedur.

### Informationen zu diesem Vorgang

Sie können IBM Spectrum Protect mit jeder der folgenden Methoden deinstallieren: grafisch orientierter Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

- **Windows: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren**  
Sie können IBM Spectrum Protect mit dem Installationsassistenten von IBM® Installation Manager deinstallieren.
- **Windows: IBM Spectrum Protect im Konsolenmodus deinstallieren**  
Zum Deinstallieren von IBM Spectrum Protect mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.
- **Windows: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren**  
Zum Deinstallieren von IBM Spectrum Protect im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.
- **Windows: IBM Spectrum Protect deinstallieren und erneut installieren**  
Wenn Sie IBM Spectrum Protect nicht mit dem Assistenten, sondern manuell erneut installieren wollen, müssen Sie einige Maßnahmen ergreifen, um Ihre Serverinstanznamen und Datenbankverzeichnisse zu bewahren. Während einer Deinstallation werden alle bereits definierten Serverinstanzen entfernt, die Datenbankkataloge für diese Instanzen sind jedoch noch vorhanden.
- **Windows: IBM Installation Manager deinstallieren**  
Sie können IBM Installation Manager deinstallieren, wenn keine Produkte mehr vorhanden sind, die mit IBM Installation Manager installiert wurden.

### Nächste Schritte

Die Vorgehensweise für die Reinstallation der IBM Spectrum Protect-Komponenten finden Sie in Windows: Serverkomponenten installieren.


## Windows: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren

Sie können IBM Spectrum Protect mit dem Installationsassistenten von IBM® Installation Manager deinstallieren.

## Vorgehensweise

---

1. Starten Sie Installation Manager.

 Windows-Betriebssysteme Öffnen Sie Installation Manager über das Menü Start.

2. Klicken Sie auf Deinstallieren.
3. Wählen Sie IBM Spectrum Protect-Server aus und klicken Sie auf Weiter.
4. Klicken Sie auf Deinstallieren.
5. Klicken Sie auf Fertigstellen.


## Windows: IBM Spectrum Protect im Konsolenmodus deinstallieren

---



Zum Deinstallieren von IBM Spectrum Protect mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.

### Vorgehensweise

---

1. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das folgende Unterverzeichnis:
  -  Windows-Betriebssysteme\ eclipse\ tools

Beispiel:

-  Windows-Betriebssysteme\ C:\Programme\IBM\Installation Manager\ eclipse\ tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus:
    -  Windows-Betriebssysteme\ imcl.exe -c
  3. Für die Deinstallation geben Sie 5 ein.
  4. Wählen Sie die Deinstallation aus der IBM Spectrum Protect-Paketgruppe aus.
  5. Geben Sie N für 'Next' (Weiter) ein.
  6. Wählen Sie die Deinstallation des IBM Spectrum Protect-Serverpakets aus.
  7. Geben Sie N für 'Next' (Weiter) ein.
  8. Geben Sie U für 'Uninstall' (Deinstallieren) ein.
  9. Geben Sie F für 'Finish' (Fertigstellen) ein.

## Windows: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren

---

Zum Deinstallieren von IBM Spectrum Protect im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.

### Vorbereitende Schritte

---


Sie können die Dateneingabe für eine unbeaufsichtigte Deinstallation der IBM Spectrum Protect-Serverkomponenten mithilfe einer Antwortdatei bereitstellen. IBM Spectrum Protect enthält eine Musterantwortdatei, uninstall\_response\_sample.xml, im Verzeichnis input, in dem das Installationspaket extrahiert wird. Diese Datei enthält Standardwerte, durch die Sie unnötige Warnungen vermeiden können.

Wenn Sie alle IBM Spectrum Protect-Komponenten deinstallieren wollen, lassen Sie die Einstellung `modify="false"` für jede Komponente in der Antwortdatei unverändert. Wenn Sie eine Komponente nicht deinstallieren wollen, geben Sie den Wert `modify="true"` an.



Wenn Sie die Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

### Vorgehensweise

---

1. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das folgende Unterverzeichnis:
  -  Windows-Betriebssysteme\ eclipse\ tools

Beispiel:

-  Windows-Betriebssysteme\ C:\Programme\IBM\Installation Manager\ eclipse\ tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus, wobei *Antwortdatei* den Pfad der Antwortdatei einschließlich des Dateinamens angibt:  
 Windows-Betriebssysteme

```
imcl.exe -input Antwortdatei -silent
```

Der folgende Befehl ist ein Beispiel:

 Windows-Betriebssysteme


```
imcl.exe -input C:\tmp\input\uninstall_response.xml -silent
```

## Windows: IBM Spectrum Protect deinstallieren und erneut installieren

Wenn Sie IBM Spectrum Protect nicht mit dem Assistenten, sondern manuell erneut installieren wollen, müssen Sie einige Maßnahmen ergreifen, um Ihre Serverinstanznamen und Datenbankverzeichnisse zu bewahren. Während einer Deinstallation werden alle bereits definierten Serverinstanzen entfernt, die Datenbankkataloge für diese Instanzen sind jedoch noch vorhanden.

### Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um IBM Spectrum Protect manuell zu deinstallieren und erneut zu installieren:

1.  Windows-Betriebssysteme Erstellen Sie eine Liste Ihrer aktuellen Serverinstanzen, bevor Sie mit der Deinstallation beginnen. Führen Sie den folgenden Befehl aus:

```
db2ilist
```


2. Führen Sie die folgenden Befehle für jede Serverinstanz aus:

 Windows-Betriebssysteme

```
db2 attach to server1
db2 get dbm cfg show detail
db2 detach
```


Notieren Sie den Datenbankpfad für jede Instanz.

3. Deinstallieren Sie IBM Spectrum Protect. Siehe [Windows: IBM Spectrum Protect deinstallieren](#).

 Windows-Betriebssysteme Überprüfen Sie nach der Deinstallation von IBM Spectrum Protect über Systemsteuerung > Software, ob IBM Spectrum Protect DB2 deinstalliert ist.

4. Wenn Sie eine beliebige unterstützte Version von IBM Spectrum Protect deinstallieren (einschließlich Fixpack), wird eine Instanzdatei erstellt. Die Instanzdatei wird erstellt, um die Reinstallation von IBM Spectrum Protect zu erleichtern. Überprüfen Sie diese Datei und verwenden Sie die Informationen, wenn Sie bei der Reinstallation zur Eingabe der Berechtigungsnachweise der Instanz aufgefordert werden. Bei der unbeaufsichtigten Installation geben Sie diese Berechtigungsnachweise mit der Variablen `INSTANCE_CRED` an.


Sie finden die Instanzdatei an der folgenden Position:

- o  Windows-Betriebssysteme `C:\ProgramData\IBM\Tivoli\TSM\instanceList.obj` im Installationsverzeichnis des IBM Spectrum Protect-Servers

5. Installieren Sie IBM Spectrum Protect erneut. Siehe [Windows: Serverkomponenten installieren](#).

Ist die Datei `instanceList.obj` nicht vorhanden, müssen Sie Ihre Serverinstanzen wie folgt erneut erstellen:

- a. Erstellen Sie Ihre Serverinstanzen erneut. Siehe [Windows: Serverinstanz erstellen](#).  
Tipp: Der Installationsassistent konfiguriert die Serverinstanzen, Sie müssen jedoch überprüfen, ob sie vorhanden sind. Wenn sie nicht vorhanden sind, müssen Sie sie manuell konfigurieren.
- b. Katalogisieren Sie die Datenbank. Melden Sie sich bei jeder Serverinstanz nacheinander als Instanzbenutzer an und geben Sie folgende Befehle aus:

 Windows-Betriebssysteme

```
set db2instance=server1
db2 catalog database tsmdb1
db2 attach to server1
db2 update dbm cfg using dftdbpath Instanzlaufwerk
db2 detach
```

- c. Überprüfen Sie, ob IBM Spectrum Protect die Serverinstanz erkennt, indem Sie Ihre Verzeichnisse auflisten. Ihr Ausgangsverzeichnis wird angezeigt, wenn Sie es nicht geändert haben. Ihr Instanzverzeichnis wird angezeigt, wenn Sie den Konfigurationsassistenten verwendet haben. Geben Sie den folgenden Befehl aus:

```
db2 list database directory
```


Wenn Sie TSMDB1 in der Liste finden, können Sie den Server starten.

# Windows: IBM Installation Manager deinstallieren

Sie können IBM® Installation Manager deinstallieren, wenn keine Produkte mehr vorhanden sind, die mit IBM Installation Manager installiert wurden.

## Vorbereitende Schritte

Bevor Sie IBM Installation Manager deinstallieren, müssen Sie sicherstellen, dass alle mit IBM Installation Manager installierten Pakete deinstalliert sind. Schließen Sie IBM Installation Manager, bevor Sie den Deinstallationsprozess starten.

 Windows-Betriebssysteme Klicken Sie auf Start > Alle Programme > IBM Installation Manager > Installierte Pakete anzeigen.

## Vorgehensweise

Gehen Sie wie folgt vor, um IBM Installation Manager zu deinstallieren:

 Windows-Betriebssysteme

1. Klicken Sie im Menü Start auf Systemsteuerung > Programme und Funktionen.
2. Wählen Sie IBM Installation Manager aus und klicken Sie auf Deinstallieren.







## Upgrade auf Version 8.1 durchführen

Führen Sie ein Upgrade des IBM Spectrum Protect-Servers auf Version 8.1.3 durch, damit neue Produktfunktionen und Aktualisierungen genutzt werden können.

## Informationen zu diesem Vorgang

Informationen zum Upgrade des Servers auf demselben Betriebssystem finden Sie in den Upgradeanweisungen. Anweisungen zur Migration des Servers in ein anderes Betriebssystem finden Sie in IBM Spectrum Protect Upgrade and Migration Process - Frequently Asked Questions.

Tabelle 1. Upgradeanweisungen

| Upgrade von Version       | Auf Version                               | Siehe  |
|---------------------------|---|--|
| Version 8.1               | Version 8.1, Fixpack oder vorläufiger Fix |  AIX-Betriebssysteme IBM Spectrum Protect-Server-Fixpack installieren<br> Linux-Betriebssysteme IBM Spectrum Protect-Server-Fixpack installieren<br> Windows-Betriebssysteme IBM Spectrum Protect-Server-Fixpack installieren |
| Version 7.1               | Version 8.1                               | Server installieren und Upgrade prüfen   |
| Version 7.1               | Version 8.1, Fixpack oder vorläufiger Fix |  AIX-Betriebssysteme IBM Spectrum Protect-Server-Fixpack installieren<br> Linux-Betriebssysteme IBM Spectrum Protect-Server-Fixpack installieren<br> Windows-Betriebssysteme IBM Spectrum Protect-Server-Fixpack installieren |
| Version 5.5, 6.2 oder 6.3 | Version 8.1                               | IBM Spectrum Protect Upgrade and Migration Process - Frequently Asked Questions  |

Ein Upgrade von Version 7 auf Version 8.1 dauert ca. 20 - 50 Minuten. Die Ergebnisse in Ihrer Umgebung können von den im Labor erzielten Ergebnissen abweichen.

Informationen zu Upgrades in einer Clusterumgebung finden Sie in Server-Upgrade in einer Clusterumgebung durchführen.

Soll nach einem Upgrade oder einer Migration auf eine frühere Version des Servers zurückgesetzt werden, benötigen Sie eine Datenbankgesamtsicherung und die Installationssoftware für den ursprünglichen Server. Sie benötigen außerdem die folgenden Schlüsselkonfigurationsdateien:

- Protokolldatei für Datenträger
- Einheitenkonfigurationsdatei
- Serveroptionsdatei

- Upgrade auf Version 8.1 durchführen  
Von Version 7.1 auf Version 8.1 ist ein direktes Upgrade des Servers möglich. Sie müssen Version 7.1 nicht deinstallieren.
- Server-Upgrade in einer Clusterumgebung durchführen  
Sie müssen Vorbereitungs- und Installationstasks ausführen, um ein Upgrade eines Servers auf Version 8.1.3 in einer Clusterumgebung durchzuführen. Die Vorgehensweise ist vom Betriebssystem und vom Release abhängig.

**Zugehörige Informationen:**

 [IBM Spectrum Protect-Upgrade- und -Migrationsprozess - Häufig gestellte Fragen](#)

## Upgrade auf Version 8.1 durchführen

---

Von Version 7.1 auf Version 8.1 ist ein direktes Upgrade des Servers möglich. Sie müssen Version 7.1 nicht deinstallieren.

### Vorbereitende Schritte

---

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease der Server, für das Sie ein Upgrade durchführen wollen, vorhanden sind. Wenn Sie die Serverkomponenten von DVD installiert haben, stellen Sie sicher, dass die DVD verfügbar ist. Wenn Sie die Serverkomponenten über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, sind die Installationsmedien für das Basisrelease des Servers für die Neuinstallation der Lizenz erforderlich.

Tipp: Bei Version 8.1 und höher sind DVDs nicht mehr verfügbar.

### Vorgehensweise

---

Führen Sie folgende Tasks aus, um ein Upgrade des Servers auf Version 8.1 durchzuführen:

- **Planung des Upgrades**  
Bevor Sie ein Upgrade des Servers von Version 7.1 auf Version 8.1 durchführen, müssen Sie die relevanten Planungsinformationen lesen, z. B. die Systemvoraussetzungen und die Releaseinformationen. Dann wählen Sie einen geeigneten Zeitpunkt für das Systemupgrade aus, um die Auswirkung auf den Produktionsbetrieb so gering wie möglich zu halten.
- **Vorbereitung des Systems**  
Um das System für das Upgrade von Version 7.1 auf Version 8.1 vorzubereiten, müssen Sie Informationen zu jeder DB2-Instanz zusammenstellen. Dann sichern Sie die Serverdatenbank, speichern Sie Schlüsselkonfigurationsdateien, brechen Sie Sitzungen ab und stoppen Sie den Server.
- **Server installieren und Upgrade prüfen**  
Sie müssen den Server der Version 8.1 installieren, um den Upgradeprozess des Servers auf Version 8.1 abzuschließen. Dann überprüfen Sie, ob das Upgrade erfolgreich war, indem Sie die Serverinstanz starten.

## Planung des Upgrades

---

Bevor Sie ein Upgrade des Servers von Version 7.1 auf Version 8.1 durchführen, müssen Sie die relevanten Planungsinformationen lesen, z. B. die Systemvoraussetzungen und die Releaseinformationen. Dann wählen Sie einen geeigneten Zeitpunkt für das Systemupgrade aus, um die Auswirkung auf den Produktionsbetrieb so gering wie möglich zu halten.

### Informationen zu diesem Vorgang

---

In Labortests dauerte der Upgradeprozess für den Server von Version 7.1 auf Version 8.1 14 bis 45 Minuten. Die Dauer in Ihrer Umgebung kann abweichen und ist von Ihrer Hardware und Software sowie der Größe der Serverdatenbank abhängig.

### Vorgehensweise

---

1. Überprüfen Sie die Hardware- und Softwarevoraussetzungen:

 [AIX-BetriebssystemeSystemvoraussetzungen für AIX-Systeme](#)

 [Linux-BetriebssystemeSystemvoraussetzungen für Linux-Systeme](#)

 [Windows-BetriebssystemeSystemvoraussetzungen für Windows-Systeme](#)

Aktuelle Informationen zu den Systemvoraussetzungen finden Sie auf der IBM Spectrum Protect-Unterstützungswebsite unter Technote 1243309.

2. Lesen Sie die Releaseinformationen für Serverkomponenten der Version 8.1 und die Readme-Dateien für Fixpacks für den IBM Spectrum Protect-Server der Version 8.1, die spezielle Anweisungen und Informationen für Ihr Betriebssystem enthalten.


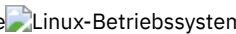
3. Wählen Sie einen geeigneten Zeitpunkt für das Systemupgrade aus, um die Auswirkung auf den Produktionsbetrieb so gering wie möglich zu halten. Die für die Aktualisierung des Systems erforderliche Zeit ist von der Größe der Datenbank und vielen anderen Faktoren abhängig. Wenn Sie den Upgradeprozess starten, können Clients keine Verbindung zum Server herstellen, bis die neue Software installiert ist und alle erforderlichen Lizenzen wieder registriert sind.
4. Wenn Sie ein Upgrade des Servers von Version 6 oder Version 7 auf Version 8.1 durchführen, müssen Sie die System-ID und das Kennwort für die DB2-Instanz des IBM Spectrum Protect-Servers kennen. Diese Berechtigungsnachweise sind für ein Upgrade des Systems erforderlich.

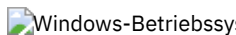
## Vorbereitung des Systems

Um das System für das Upgrade von Version 7.1 auf Version 8.1 vorzubereiten, müssen Sie Informationen zu jeder DB2-Instanz zusammenstellen. Dann sichern Sie die Serverdatenbank, speichern Sie Schlüsselkonfigurationsdateien, brechen Sie Sitzungen ab und stoppen Sie den Server.

## Vorgehensweise

1. Melden Sie sich bei dem Computer an, auf dem der Server installiert ist.


  Stellen Sie sicher, dass Sie mit der Instanzbenutzer-ID angemeldet sind.

 Stellen Sie sicher, dass Sie mit der Benutzer-ID mit Administratorberechtigung angemeldet sind, mit der der Server der Version 7.1 installiert wurde.

2. Rufen Sie eine Liste der DB2-Instanzen ab. Geben Sie den folgenden Systembefehl aus:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```



```
db2ilist
```

Die Ausgabe kann wie in dem folgenden Beispiel aussehen:


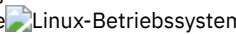
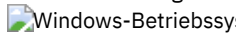
 

```
tsminst1
```



```
SERVER1
```

Stellen Sie sicher, dass jede Instanz einem Server entspricht, der auf dem System aktiv ist.

3.   Notieren Sie für jede DB2-Instanz den Standarddatenbankpfad, den tatsächlichen Datenbankpfad, den Datenbanknamen, den Aliasnamen der Datenbank und alle DB2-Variablen, die für die Instanz konfiguriert wurden. Bewahren Sie die Aufzeichnung für spätere Referenzzwecke auf. Diese Informationen werden für die Zurückschreibung der Datenbank der Version 7.1 benötigt.
4.  Stellen Sie Informationen zu jeder DB2-Instanz zusammen. Notieren Sie den Standarddatenbankpfad, den tatsächlichen Datenbankpfad, den Datenbanknamen, den Aliasnamen der Datenbank und alle DB2-Variablen, die für die Instanz konfiguriert wurden. Bewahren Sie die Aufzeichnung für spätere Referenzzwecke auf. Diese Informationen werden für die Zurückschreibung der Datenbank der Version 7.1 benötigt.
  - a. Geben Sie folgenden Systembefehl aus, um das DB2-Befehlsfenster zu öffnen:

```
db2cmd
```

- b. Geben Sie den folgenden Systembefehl aus, um die Instanz zu ändern:

```
set DB2INSTANCE=Instanz
```

*Instanz* gibt die DB2-Instanz an.

- c. Geben Sie den folgenden Systembefehl aus, um den Standarddatenbankpfad der DB2-Instanz abzurufen:

```
db2 get dbm cfg | findstr DFTDBPATH
```

Die Ausgabe kann wie in dem folgenden Beispiel aussehen:

```
Standarddatenbankpfad
```

```
(DFTDBPATH) = D:
```

- d. Geben Sie den folgenden Systembefehl aus, um Informationen zu den DB2-Instanzdatenbanken abzurufen:

```
db2 list database directory
```

Die Ausgabe kann wie in dem folgenden Beispiel aussehen:

Systemdatenbankverzeichnis

```
Anzahl Einträge im Verzeichnis = 2
```

```
Eintrag für Datenbank 1:
```

```
Aliasname der Datenbank           = TSMAL001
Datenbankname                     = TSMDB1
Knotenname                       = TSMNODE1
Release-Level der Datenbank       = d.00
Kommentar                         = TSM SERVER DATABASE VIA TCPIP
Verzeichniseintragungsart        = Fern
Datenbankpartitionsnummer für Katalog= -1
Hostname des Alternativservers    =
Portnummer des Alternativservers  =
```

```
Eintrag für Datenbank 2:
```

```
Aliasname der Datenbank           = TSMDB1
Datenbankname                     = TSMDB1
                                Lokales Datenbankverzeichnis      = D:
Release-Level der Datenbank       = d.00
Kommentar                         =
Verzeichniseintragungsart        = Indirekt
Datenbankpartitionsnummer für Katalog= 0
Hostname des Alternativservers    =
Portnummer des Alternativservers  =
```

e. Geben Sie den folgenden Systembefehl aus, um die DB2-Instanzvariablen abzurufen:

```
db2set -all
```

Die Ausgabe kann wie in dem folgenden Beispiel aussehen:

```
[e] DB2CODEPAGE=1208
[e] DB2PATH=D:\TSM\db2
[i] DB2_PMODEL_SETTINGS=MAX_BACKGROUND_SYSAPPS:500
[i] DB2_SKIPINSERTED=ON
[i] DB2_KEEPTABLELOCK=OFF
[i] DB2_EVALUNCOMMITTED=ON
[i] DB2_VENDOR_INI=D:\Server1\tsmdbmgr.env
[i] DB2_SKIPDELETED=ON
[i] DB2INSTPROF=C:\ProgramData\IBM\DB2\DB2TSM1
[i] DB2COMM=TCPIP
[i] DB2CODEPAGE=819
[i] DB2_PARALLEL_IO=*
[g] DB2_EXTSECURITY=YES
[g] DB2_COMMON_APP_DATA_PATH=C:\ProgramData

[g] DB2PATH=D:\TSM\db2
[g] DB2INSTDEF=SERVER1
```

5. Stellen Sie mithilfe der Benutzer-ID mit Administratorberechtigung eine Verbindung zum Server her.
6. Sichern Sie die Datenbank mit dem Befehl BACKUP DB. Die bevorzugte Methode ist eine Momentaufnahmesicherung, bei der eine Datenbankgesamticherung erstellt wird, ohne geplante Datenbanksicherungen zu unterbrechen. Sie können eine Momentaufnahmesicherung beispielsweise mit dem folgenden Befehl erstellen:

```
backup db type=dbsnapshot devclass=tapeclass
```

7. Geben Sie den folgenden Verwaltungsbefehl aus, um die Einheitenkonfigurationsdaten in einem anderen Verzeichnis zu sichern:

```
backup devconfig filenames=Dateiname
```

*Dateiname* gibt den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.

Tipp: Diese Datei wird benötigt, wenn die Datenbank der Version 7.1 zurückgeschrieben werden soll.

8. Sichern Sie die Protokolldatei für Datenträger in einem anderen Verzeichnis. Geben Sie den folgenden Verwaltungsbefehl aus:

```
backup volhistory filenames=Dateiname
```

*Dateiname* gibt den Namen der Datei an, in der Datenträgerhistory-Informationen (Datenträgerprotokolldaten) gespeichert werden sollen.

Tipp: Diese Datei wird benötigt, wenn die Datenbank der Version 7.1 zurückgeschrieben werden soll.



- Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dmserv.opt heißt. Die Datei befindet sich im Serverinstanzverzeichnis.
- Verhindern Sie Aktivität auf dem Server durch Inaktivierung neuer Sitzungen. Geben Sie die folgenden Verwaltungsbefehle aus:

```
disable sessions client  
disable sessions server
```

- Überprüfen Sie, ob Sitzungen bestehen, und benachrichtigen Sie die Benutzer, dass der Server gestoppt wird. Geben Sie den folgenden Verwaltungsbefehl aus, um auf bestehende Sitzungen zu überprüfen:

```
query session
```

- Geben Sie den folgenden Verwaltungsbefehl aus, um Sitzungen abubrechen:



```
cancel session all
```

Dieser Befehl bricht alle Sitzungen außer der aktuellen Sitzung ab.


- Geben Sie den folgenden Verwaltungsbefehl aus, um den Server zu stoppen:

```
halt
```

- Stellen Sie sicher, dass der Server heruntergefahren wird und dass keine Prozesse ausgeführt werden.

  Geben Sie den folgenden Befehl aus:

```
ps -ef | grep dmserv
```

 Öffnen Sie die Windows-Anwendung 'Task-Manager' und überprüfen Sie die Liste der aktiven Prozesse.

- Suchen Sie die Datei NODELOCK im Serverinstanzverzeichnis Ihrer Installation und verschieben Sie sie in ein anderes Verzeichnis, in dem Sie Konfigurationsdateien speichern. Die Datei NODELOCK enthält die vorherigen Lizenzinformationen für Ihre Installation. Diese Lizenzinformationen werden bei Beendigung des Upgrades ersetzt.

#### Zugehörige Verweise:

BACKUP DB (Datenbank sichern)  
BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)  
BACKUP VOLHISTORY (History-Daten für sequentielle Datenträger sichern)  
DISABLE SESSIONS (Verhindern, dass neue Sitzungen auf Tivoli Storage Manager zugreifen)  
QUERY SESSION (Clientsitzungen abfragen)  
CANCEL SESSION (Clientsitzungen abbrechen)  
HALT (Server herunterfahren)

## Server installieren und Upgrade prüfen


---

Sie müssen den Server der Version 8.1 installieren, um den Upgradeprozess des Servers auf Version 8.1 abzuschließen. Dann überprüfen Sie, ob das Upgrade erfolgreich war, indem Sie die Serverinstanz starten.



### Vorbereitende Schritte

---

  Sie müssen mit der Rootbenutzer-ID am System angemeldet sein.

 Sie müssen mit der Benutzer-ID mit Administratorberechtigung, die für die Installation des Servers der früheren Version verwendet wurde, am System angemeldet sein.

Das Installationspaket kann von einer IBM® Download-Site heruntergeladen werden.

  Legen Sie als Systembenutzergrenzwert für die maximale Dateigröße 'unlimited' (unbegrenzt) fest, um sicherzustellen, dass die Dateien ordnungsgemäß heruntergeladen werden können.

- Führen Sie den folgenden Befehl aus, um den Wert für die maximale Dateigröße abzufragen:

```
ulimit -Hf
```

- Wenn als Systembenutzergrenzwert für die maximale Dateigröße nicht 'unlimited' (unbegrenzt) angegeben ist, geben Sie 'unlimited' gemäß den Anweisungen in der Dokumentation Ihres Betriebssystems an.

### Informationen zu diesem Vorgang

---

Mithilfe der IBM Spectrum Protect-Installationssoftware können Sie die folgenden Komponenten installieren:

- Server  
Tipp: Die Datenbank (DB2), Global Security Kit (GSKit) und IBM Java™ Runtime Environment (JRE) werden automatisch installiert, wenn Sie die Serverkomponente auswählen.
- Sprachen des Servers
- Lizenzen
- Einheiten
- IBM Spectrum Protect for SAN
- Operations Center

## Vorgehensweise

---

1. Laden Sie die entsprechende Paketdatei von einer der folgenden Websites herunter:
  - Laden Sie das Serverpaket über Passport Advantage oder Fix Central herunter.
  - Die neuesten Informationen, Aktualisierungen und Fixes finden Sie im IBM Support Portal.
2. Führen Sie die folgenden Schritte aus:


- a. Überprüfen Sie, ob genug Speicherbereich zum Speichern der Installationsdateien nach dem Extrahieren aus dem Produktpaket vorhanden ist. Informationen zum Speicherbedarf finden Sie im Downloaddokument für Ihr Produkt.
  - IBM Spectrum Protect Technote 4042944
  - IBM Spectrum Protect Extended Edition Technote 4042945
  - IBM Spectrum Protect for Data Retention Technote 4042946
- b. Laden Sie die Paketdatei in ein beliebiges Verzeichnis herunter. Der Pfad darf maximal 128 Zeichen enthalten. Sie müssen die Installationsdateien in ein leeres Verzeichnis extrahieren. Verwenden Sie kein Verzeichnis, das bereits extrahierte Dateien oder andere Dateien enthält.

Stellen Sie außerdem sicher, dass Sie über die Ausführberechtigung für die Paketdatei verfügen.

- c. Falls erforderlich, führen Sie den folgenden Befehl aus, um die Dateiberechtigungen zu ändern:

```
chmod a+x Paketname.bin
```

*Paketname* sieht wie in dem folgenden Beispiel aus:



```
8.1.x.000-IBM-SPSRV-AIX.bin
```



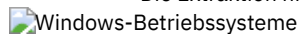
```
8.1.x.000-IBM-SPSRV-Linuxs390x.bin
8.1.x.000-IBM-SPSRV-Linuxx86_64.bin
8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
```


In den Beispielen gibt *8.1.x.000* das Release-Level des Produkts an.

- d. Führen Sie den folgenden Befehl aus, um die Installationsdateien zu extrahieren:

```
./Paketname.bin
```

Die Extraktion nimmt etwas Zeit in Anspruch, weil das Paket groß ist.







- a. Überprüfen Sie, ob genug Speicherbereich zum Speichern der Installationsdateien nach dem Extrahieren aus dem Produktpaket vorhanden ist. Informationen zum Speicherbedarf finden Sie im Downloaddokument für Ihr Produkt.
  - IBM Spectrum Protect Technote 4042944
  - IBM Spectrum Protect Extended Edition Technote 4042945
  - IBM Spectrum Protect for Data Retention Technote 4042946
- b. Wechseln Sie in das Verzeichnis, in dem sich die ausführbare Datei befindet.  
Tipp: Im nächsten Schritt werden die Dateien in das aktuelle Verzeichnis extrahiert. Der Pfad darf maximal 128 Zeichen enthalten. Sie müssen die Installationsdateien in ein leeres Verzeichnis extrahieren. Verwenden Sie kein Verzeichnis, das bereits extrahierte Dateien oder andere Dateien enthält.
- c. Doppelklicken Sie auf der ausführbaren Datei, um die Installationsdateien zu extrahieren:

```
Paketname.exe
```


*Paketname* sieht wie in dem folgenden Beispiel aus:


```
8.1.x.000-SPSRV-WindowsX64.exe
```


Die Extraktion nimmt etwas Zeit in Anspruch, weil das Paket groß ist.

3.  Prüfen Sie, ob der folgende Befehl aktiviert ist, um sicherzustellen, dass die IBM Spectrum Protect-Assistenten ordnungsgemäß funktionieren:
  - o  `lsuser`Der Befehl ist standardmäßig aktiviert.
4. Installieren Sie die IBM Spectrum Protect-Software mit einer der folgenden Methoden. Installieren Sie die IBM Spectrum Protect-Lizenz während des Installationsprozesses.  
Tipp: Befinden sich mehrere Serverinstanzen auf Ihrem System, installieren Sie die IBM Spectrum Protect-Software nur einmal, um alle Serverinstanzen zu aktualisieren.

#### Installationsassistent


 Befolgen Sie die Anweisungen in IBM Spectrum Protect mit dem Installationsassistenten installieren, um den Server mithilfe des grafisch orientierten Assistenten von IBM Installation Manager zu installieren.


 Befolgen Sie die Anweisungen in IBM Spectrum Protect mit dem Installationsassistenten installieren, um den Server mithilfe des grafisch orientierten Assistenten von IBM Installation Manager zu installieren.


 Befolgen Sie die Anweisungen in IBM Spectrum Protect mit dem Installationsassistenten installieren, um den Server mithilfe des grafisch orientierten Assistenten von IBM Installation Manager zu installieren.

Stellen Sie sicher, dass Ihr System die Voraussetzungen für die Verwendung des Installationsassistenten erfüllt. Führen Sie anschließend die Installationsschritte aus. Klicken Sie im Fenster von IBM Installation Manager auf das Symbol Aktualisieren oder Ändern.

#### Server im Konsolenmodus installieren


 Befolgen Sie die Anweisungen in Tivoli Storage Manager im Konsolenmodus installieren, um den Server im Konsolenmodus zu installieren.


 Befolgen Sie die Anweisungen in Tivoli Storage Manager im Konsolenmodus installieren, um den Server im Konsolenmodus zu installieren.


 Befolgen Sie die Anweisungen in Tivoli Storage Manager im Konsolenmodus installieren, um den Server im Konsolenmodus zu installieren.

Lesen Sie die Informationen zur Installation des Servers im Konsolenmodus und führen Sie anschließend die Installationsschritte aus.

#### Unbeaufsichtigter Modus

 Befolgen Sie die Anweisungen in Tivoli Storage Manager im unbeaufsichtigten Modus installieren, um den Server im unbeaufsichtigten Modus zu installieren.

 Befolgen Sie die Anweisungen in Tivoli Storage Manager im unbeaufsichtigten Modus installieren, um den Server im unbeaufsichtigten Modus zu installieren.

 Befolgen Sie die Anweisungen in Tivoli Storage Manager im unbeaufsichtigten Modus installieren, um den Server im unbeaufsichtigten Modus zu installieren.



Lesen Sie die Informationen zur Installation des Servers im unbeaufsichtigten Modus und führen Sie anschließend die Installationsschritte aus.



Nach der Installation der Software müssen Sie das System nicht rekonfigurieren.


5. Beheben Sie alle Fehler, die während des Installationsprozesses festgestellt werden.

Wenn Sie den Server mithilfe des Installationsassistenten installiert haben, können Sie Installationsprotokolle mithilfe des Tools IBM Installation Manager anzeigen. Klicken Sie auf Datei > Protokoll anzeigen. Um Protokolldateien zu erfassen, klicken Sie in IBM Installation Manager auf Hilfe > Daten zur Fehleranalyse exportieren.

Wenn Sie den Server im Konsolenmodus oder im unbeaufsichtigten Modus installiert haben, können Sie Fehlerprotokolle im IBM Installation Manager-Protokollverzeichnis anzeigen. Zum Beispiel:

- o  `/var/ibm/InstallationManager/logs`
- o  `C:\Programme\IBM\Installation Manager\logs`

6. Rufen Sie das IBM Support Portal auf, um Fixes abzurufen. Klicken Sie auf Fixes, updates, and drivers und legen Sie alle gültigen Fixes an.
7.   Überprüfen Sie, ob das Upgrade erfolgreich war:
  - a. Starten Sie die Serverinstanz.

 AIX-Betriebssysteme Anweisungen finden Sie in Serverinstanz starten.

 Linux-Betriebssysteme Anweisungen finden Sie in Serverinstanz starten.

- b. Überwachen Sie die Nachrichten, die der Server bei seinem Start ausgibt. Achten Sie auf Fehlermeldungen und Warnungen und lösen Sie alle Probleme.
- c. Überprüfen Sie, ob Sie mithilfe des Verwaltungsclients eine Verbindung zum Server herstellen können. Führen Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um eine Verwaltungsclientsitzung zu starten:


```
dsmadmc
```

- d. Führen Sie QUERY-Befehle aus, um Informationen zum aktualisierten System abzurufen. Führen Sie beispielsweise den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um konsolidierte Informationen zum System abzurufen:

```
query system
```

Führen Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um Informationen zur Datenbank abzurufen:

```
query db format=detailed
```

8.  Windows-Betriebssysteme Überprüfen Sie, ob das Upgrade erfolgreich war:
  - a. Starten Sie die Serverinstanz. Führen Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um den Server aus dem Standardverzeichnis C:\Programme\Tivoli\TSM zu starten:

```
dsmserve -k Serverinstanz
```

*Serverinstanz* ist der Name Ihrer Serverinstanz. *Server1* ist der Standardname für die erste Instanz des IBM Spectrum Protect-Servers.

Wenn Sie den Server als Dienst im lokalen Systemkonto ausführen wollen, muss dem lokalen Systemkonto die Zugriffsberechtigung für die Serverdatenbank explizit erteilt werden. Anweisungen finden Sie in Server mit Windows-Diensten starten.

- b. Überwachen Sie die Nachrichten, die der Server bei seinem Start ausgibt. Achten Sie auf Fehlermeldungen und Warnungen und lösen Sie alle Probleme.
- c. Überprüfen Sie, ob Sie mithilfe des Verwaltungsclients eine Verbindung zum Server herstellen können. Führen Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um eine Verwaltungsclientsitzung zu starten:



```
dsmadmc
```

- d. Führen Sie QUERY-Befehle aus, um Informationen zum aktualisierten System abzurufen. Führen Sie beispielsweise den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um konsolidierte Informationen zum System abzurufen:

```
query system
```

Führen Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um Informationen zur Datenbank abzurufen:

```
query db format=detailed
```

9.  AIX-Betriebssysteme  Linux-Betriebssysteme Registrieren Sie die Lizenzen für die IBM Spectrum Protect-Serverkomponenten, die auf Ihrem System installiert sind. Führen Sie hierfür den Befehl REGISTER LICENSE aus:

```
register license file=Installationsverzeichnis/server/bin/Komponentenname.lic
```

Hierbei gibt *Installationsverzeichnis* das Verzeichnis an, in dem Sie die Komponente installiert haben, und *Komponentenname* ist die Abkürzung für die Komponente.

Wenn Sie den Server beispielsweise im Standardverzeichnis /opt/tivoli/tsm installiert haben, registrieren Sie die Lizenz mit dem folgenden Befehl:

```
register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
```

Wenn Sie IBM Spectrum Protect Extended Edition beispielsweise im Verzeichnis /opt/tivoli/tsm installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
```

Wenn Sie IBM Spectrum Protect for Data Retention beispielsweise im Verzeichnis /opt/tivoli/tsm installiert haben, führen Sie den folgenden Befehl aus:


```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

Einschränkung:

Sie können den IBM Spectrum Protect-Server nicht zum Registrieren von Lizenzen für die folgenden Produkte verwenden:

- o IBM Spectrum Protect for Mail
- o IBM Spectrum Protect for Databases
- o IBM Spectrum Protect for ERP
- o IBM Spectrum Protect for Space Management

Der Befehl REGISTER LICENSE ist für diese Lizenzen nicht gültig. Die Lizenzierung für diese Produkte wird von IBM Spectrum Protect-Clients ausgeführt.

10.  Windows-Betriebssysteme Registrieren Sie die Lizenzen für die Serverkomponenten, die auf Ihrem System installiert sind. Führen Sie hierfür den Befehl REGISTER LICENSE aus:

```
register license file=Installationsverzeichnis\server\Komponentenname.lic
```

Hierbei gibt *Installationsverzeichnis* das Verzeichnis an, in dem Sie die Komponente installiert haben, und *Komponentenname* ist die Abkürzung für die Komponente.

Wenn Sie den Server beispielsweise im Standardverzeichnis c:\Programme\Tivoli\TSM installiert haben, registrieren Sie die Lizenz mit dem folgenden Befehl:

```
register license file=c:\Programme\Tivoli\TSM\server\tsmbasic.lic
```

Wenn Sie IBM Spectrum Protect Extended Edition beispielsweise im Verzeichnis c:\Programme\Tivoli\TSM installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=c:\Programme\Tivoli\TSM\server\tsmee.lic
```

Wenn Sie IBM Spectrum Protect for Data Retention beispielsweise im Verzeichnis c:\Programme\Tivoli\TSM installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=c:\Programme\Tivoli\TSM\server\dataret.lic
```

Einschränkung:

Sie können den IBM Spectrum Protect-Server nicht zum Registrieren von Lizenzen für die folgenden Produkte verwenden:

- o IBM Spectrum Protect for Mail
- o IBM Spectrum Protect for Databases
- o IBM Spectrum Protect for ERP
- o IBM Spectrum Protect for Space Management


Der Befehl REGISTER LICENSE ist für diese Lizenzen nicht gültig. Die Lizenzierung für diese Produkte wird von IBM Spectrum Protect-Clients ausgeführt.

11. Optional: Für die Installation eines zusätzlichen Sprachenpakets verwenden Sie die Funktion 'Ändern' von IBM Installation Manager.
12. Optional: Für ein Upgrade auf eine neuere Version eines Sprachenpakets verwenden Sie die Funktion 'Aktualisieren' von IBM Installation Manager.

## Nächste Schritte

---

Sie können Kennwörter im LDAP-Verzeichnisserver oder im IBM Spectrum Protect-Server authentifizieren. Im LDAP-Verzeichnisserver authentifizierte Kennwörter können erweiterte Systemsicherheit zur Verfügung stellen.




 Windows-Betriebssysteme Ist unter Windows ein Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, verwenden Sie den Einheitentreiber. Ist unter Windows kein Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, installieren Sie den IBM Spectrum Protect-Einheitentreiber mithilfe des Befehls `dpinst.exe /a`. Die Datei `dpinst.exe` befindet sich im Verzeichnis des Einheitentreibers. Das Standardverzeichnis ist `C:\Programme\Tivoli\TSM\device\drivers`.

### Zugehörige Verweise:

QUERY SYSTEM (Systemkonfiguration und Kapazität abfragen)

QUERY DB (Datenbankinformationen anzeigen)

REGISTER LICENSE (Neue Lizenz registrieren)

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Server-Upgrade in einer Clusterumgebung durchführen

---

Sie müssen Vorbereitungs- und Installationstasks ausführen, um ein Upgrade eines Servers auf Version 8.1.3 in einer Clusterumgebung durchzuführen. Die Vorgehensweise ist vom Betriebssystem und vom Release abhängig.

### Vorgehensweise

---

Führen Sie die Schritte für Ihr Betriebssystem, Quellenrelease und Zielrelease aus:

Tabelle 1. Prozeduren für ein Upgrade des Servers in einer Clusterumgebung in einem AIX-Betriebssystem

| Quellenrelease                        | Zielrelease               | Prozedur   |
|---------------------------------------|---------------------------|--|
| Version 8.1                           | Fixpack für Version 8.1.3 | Fixpack auf Version 8 in einer Clusterumgebung unter AIX anwenden  |
| Version 6.3 oder Version 7.1          | Version 8.1.3             | Upgrade für IBM Spectrum Protect von Version 6.3 oder Version 7.1 auf Version 8.1.3 in einer Clusterumgebung unter AIX mit einer gemeinsam genutzten Datenbankinstanz durchführen<br><br>Upgrade von Version 6.3 auf Version 8.1.3 in einer Clusterumgebung unter AIX mit separaten Datenbankinstanzen durchführen |
| Version 5.5, Version 6.1, Version 6.2 | Version 7.1.1 oder höher  | IBM Spectrum Protect Upgrade and Migration Process - Frequently Asked Questions  |

Tabelle 2. Prozeduren für ein Upgrade des Servers in einer Clusterumgebung in einem Linux-Betriebssystem

| Quellenrelease         | Zielrelease   | Prozedur  |
|------------------------|---------------|---|
| Version 6.3 oder höher | Version 8.1.3 | Upgrade für einen Server durchführen, der mit Tivoli System Automation konfiguriert ist |

Tabelle 3. Prozeduren für ein Upgrade des Servers in einer Clusterumgebung in einem Windows-Betriebssystem

| Quellenrelease                        | Zielrelease               | Prozedur  |
|---------------------------------------|---------------------------|---|
| Version 8.1                           | Fixpack für Version 8.1.3 | Fixpack auf Version 8 in einer Clusterumgebung unter Windows anwenden                                       |
| Version 6.3 oder Version 7.1          | Version 8.1.3             | Upgrade von Version 6.3 oder Version 7.1 auf Version 8.1 in einer Clusterumgebung unter Windows durchführen |
| Version 5.5, Version 6.1, Version 6.2 | Version 7.1 oder höher    | IBM Spectrum Protect Upgrade and Migration Process - Frequently Asked Questions                             |

- Upgrade für IBM Spectrum Protect von Version 6.3 oder Version 7.1 auf Version 8.1.3 in einer Clusterumgebung unter AIX mit einer gemeinsam genutzten Datenbankinstanz durchführen  
Sie können ein Upgrade des IBM Spectrum Protect-Servers von Version 6.3 oder Version 7.1 auf Version 8.1.3 in einer Clusterumgebung unter AIX mit einer gemeinsam genutzten Datenbankinstanz durchführen. Auf diese Weise können Sie die neuen Funktionen in IBM Spectrum Protect Version 8.1.3 nutzen.
- Upgrade von Version 6.3 auf Version 8.1.3 in einer Clusterumgebung unter AIX mit separaten Datenbankinstanzen durchführen  
Sie können ein Upgrade des Servers von Version 6.3 auf Version 8.1.3 in einer Clusterumgebung unter AIX mit separaten Datenbankinstanzen durchführen. Auf diese Weise können Sie die neuen Funktionen in Version 8.1.3 nutzen.
- IBM Spectrum Protect-Upgrade auf Version 8.1.3 in einer Clusterumgebung unter Linux durchführen  
Damit neue Funktionen in IBM Spectrum Protect genutzt werden können, können Sie ein Upgrade des IBM Spectrum Protect-Servers, der unter einem Linux-Betriebssystem in einer Clusterumgebung installiert ist, durchführen.
- Upgrade eines Servers der Version 6.3 oder Version 7.1 auf Version 8.1.3 in einer Clusterumgebung unter Windows durchführen  
Damit neue Produktfunktionen genutzt werden können, können Sie ein Upgrade eines Servers, der unter einem Windows-Betriebssystem in einer Clusterumgebung installiert ist, von Version 6.3 oder Version 7.1 auf IBM Spectrum Protect Version 8.1.3 durchführen.

## Upgrade für IBM Spectrum Protect von Version 6.3 oder Version 7.1 auf Version 8.1.3 in einer Clusterumgebung unter AIX mit einer gemeinsam genutzten Datenbankinstanz durchführen

Sie können ein Upgrade des IBM Spectrum Protect-Servers von Version 6.3 oder Version 7.1 auf Version 8.1.3 in einer Clusterumgebung unter AIX mit einer gemeinsam genutzten Datenbankinstanz durchführen. Auf diese Weise können Sie die neuen Funktionen in IBM Spectrum Protect Version 8.1.3 nutzen.

### Vorbereitende Schritte

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease des Servers der Version 6.3 oder Version 7.1, für das Sie ein Upgrade durchführen wollen, vorhanden sind. Wenn Sie IBM Spectrum Protect von DVD installiert haben, stellen Sie sicher, dass die DVD verfügbar ist. Wenn Sie IBM Spectrum Protect über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, müssen Sie die Lizenz von den Installationsmedien des Serverbasisrelease erneut installieren.

## Informationen zu diesem Vorgang

---

Gehen Sie wie folgt vor, wenn das DB2-Instanzverzeichnis von den Knoten im Cluster gemeinsam genutzt wird. Das DB2-Instanzverzeichnis befindet sich an der folgenden Position:

```
/home/tsminst1/sqlllib
```

Wenn das DB2-Instanzverzeichnis von den Knoten nicht gemeinsam genutzt wird, führen Sie die Anweisungen in Upgrade von Version 6.3 auf Version 8.1.3 in einer Clusterumgebung unter AIX mit separaten Datenbankinstanzen durchführen aus.

## Vorgehensweise

---

1. Sichern Sie die Datenbank mit dem Befehl `BACKUP DB`. Die bevorzugte Methode ist eine Momentaufnahmesicherung, bei der eine Datenbankgesamtsicherung erstellt wird, ohne geplante Sicherungen zu unterbrechen. Sie können eine Momentaufnahmesicherung beispielsweise mit dem folgenden Befehl erstellen:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Führen Sie den folgenden Befehl aus, um die Einheitenkonfigurationsdaten in einem anderen Verzeichnis zu sichern:

```
backup devconfig filenames=Dateiname
```

Hierbei gibt *Dateiname* den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.

3. Führen Sie den folgenden Befehl aus, um die Protokolldatei für Datenträger in einem anderen Verzeichnis zu sichern:

```
backup volhistory filenames=Dateiname
```

Hierbei gibt *Dateiname* den Namen der Datei an, in der Datenträgerprotokolldaten gespeichert werden sollen.

4. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise `dsmserv.opt` heißt und sich im Serverinstanzverzeichnis befindet.
5. Stoppen Sie alle Instanzen des Servers. Stellen Sie sicher, dass keine Serverprozesse ausgeführt werden. Wenn Sie die Überwachung auf Anwendungsebene für den IBM Spectrum Protect-Server verwenden, setzen Sie die Überwachung der `dsmserv`-Anwendungsressource mit Ihrem Cluster-Tool aus.
6. Stellen Sie sicher, dass der Datenbankmanager auf keiner Instanz ausgeführt wird. Stellen Sie fest, ob `db2sysc`-Prozesse ausgeführt werden. Der Eigner aktiver Prozesse zeigt an, welche Instanzen aktiv sind. Führen Sie für jeden Serverinstanzeigner den folgenden Befehl aus, um DB2 zu stoppen:

```
db2stop
```

7. Installieren Sie den IBM Spectrum Protect-Server der Version 8.1.3 auf dem primären Knoten. Führen Sie hierfür den Befehl `./install.sh` aus. Anweisungen finden Sie in Serverkomponenten installieren. Klicken Sie nach dem Start des Assistenten im Fenster von IBM Installation Manager auf das Symbol Aktualisieren oder Ändern.
8. Starten Sie jeden Server der Version 8.1.3 im Vordergrund:
  - a. Stellen Sie sicher, dass Sie mit der Instanzeigner-ID angemeldet sind.
  - b. Navigieren Sie zum Instanzverzeichnis und führen Sie den folgenden Befehl aus:

```
/opt/tivoli/tsm/server/bin/dsmserv
```

Warten Sie, bis die Eingabeaufforderung des Servers angezeigt wird, was bedeutet, dass der Server gestartet wurde.

9. Stoppen Sie den Server für jede IBM Spectrum Protect-Instanz, die aktualisiert wird. Geben Sie den folgenden Befehl aus:

```
halt
```

Tipp: Weil das DB2-Instanzverzeichnis von den Knoten im Cluster gemeinsam genutzt wird, müssen Sie die gemeinsam genutzten Ressourcen nicht auf den sekundären Knoten im Cluster verschieben.

10. Führen Sie auf jedem sekundären Knoten im Cluster die folgenden Schritte aus:
  - a. Installieren Sie den IBM Spectrum Protect-Server der Version 8.1.3 mit dem Befehl `./install.sh`. Anweisungen finden Sie in Serverkomponenten installieren. 8.1.
    - i. Wenn Sie den Installationsassistenten ausführen, klicken Sie im Fenster von IBM Installation Manager auf das Symbol Aktualisieren oder Ändern.
    - ii. Wenn Sie den Installationsassistenten ausführen, wählen Sie im Fenster Instanzberechtigungsanzeige das Kontrollkästchen Diese Instanz aktualisieren für jede Instanz ab.

- iii. Wenn Sie den Server im Konsolenmodus installieren, geben Sie an der Eingabeaufforderung Soll diese Instanz aktualisiert werden? für jede Instanz Nein ein.
  - iv. Wenn Sie den Server im unbeaufsichtigten Modus installieren, geben Sie FALSE als Wert der Variablen `user.Instanzname_update` für jede Instanz an.
- b. Stellen Sie sicher, dass jeder IBM Spectrum Protect-Server der Version 8.1.3 startet. Wenn Sie die Überwachung auf Anwendungsebene verwenden, starten Sie den Server mithilfe des Cluster-Tools.

Anweisungen zum Starten des Servers finden Sie in Serverinstanz starten.

11. Registrieren Sie die Lizenzen für die Serverkomponenten, die auf Ihrem System installiert sind. Führen Sie hierfür den Befehl REGISTER LICENSE aus:

```
register license file=Installationsverzeichnis/server/bin/Komponentenname.lic
```

Hierbei gibt *Installationsverzeichnis* das Verzeichnis an, in dem Sie die Komponente installiert haben, und *Komponentenname* ist die Abkürzung für die Komponente.

Wenn Sie den Server beispielsweise im Standardverzeichnis `/opt/tivoli/tsm` installiert haben, registrieren Sie die Lizenz mit dem folgenden Befehl:

```
register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
```

Wenn Sie IBM Spectrum Protect Extended Edition beispielsweise im Verzeichnis `/opt/tivoli/tsm` installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
```

Wenn Sie IBM Spectrum Protect for Data Retention beispielsweise im Verzeichnis `/opt/tivoli/tsm` installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

Einschränkung:

Sie können den IBM Spectrum Protect-Server nicht zum Registrieren von Lizenzen für die folgenden Produkte verwenden:

- o IBM Spectrum Protect for Mail
- o IBM Spectrum Protect for Databases
- o IBM Spectrum Protect for ERP
- o IBM Spectrum Protect for Space Management

Der Befehl REGISTER LICENSE ist für diese Lizenzen nicht gültig. Die Lizenzierung für diese Produkte wird von IBM Spectrum Protect-Clients ausgeführt.

#### Zugehörige Verweise:


BACKUP DB (Datenbank sichern)

BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)

BACKUP VOLHISTORY (History-Daten für sequentielle Datenträger sichern)

HALT (Server herunterfahren)

REGISTER LICENSE (Neue Lizenz registrieren)

 AIX-Betriebssysteme

## Upgrade von Version 6.3 auf Version 8.1.3 in einer Clusterumgebung unter AIX mit separaten Datenbankinstanzen durchführen

---

Sie können ein Upgrade des Servers von Version 6.3 auf Version 8.1.3 in einer Clusterumgebung unter AIX mit separaten Datenbankinstanzen durchführen. Auf diese Weise können Sie die neuen Funktionen in Version 8.1.3 nutzen.

### Vorbereitende Schritte

---

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease des Servers der Version 6.3 oder Version 7.1, für das Sie ein Upgrade durchführen wollen, vorhanden sind. Wenn Sie IBM Spectrum Protect von DVD installiert haben, stellen Sie sicher, dass die DVD verfügbar ist. Wenn Sie IBM Spectrum Protect über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, müssen Sie die Lizenz von den Installationsmedien des Serverbasisrelease erneut installieren.

### Informationen zu diesem Vorgang

---

Gehen Sie wie folgt vor, wenn das DB2-Instanzverzeichnis von den Knoten im Cluster nicht gemeinsam genutzt wird. Das DB2-Instanzverzeichnis befindet sich an der folgenden Position:



Wenn das DB2-Instanzverzeichnis von den Knoten im Cluster gemeinsam genutzt wird, führen Sie die Anweisungen in Upgrade für IBM Spectrum Protect von Version 6.3 oder Version 7.1 auf Version 8.1.3 in einer Clusterumgebung unter AIX mit einer gemeinsam genutzten Datenbankinstanz durchführen aus.

## Vorgehensweise

---

1. Sichern Sie die Datenbank mit dem Befehl BACKUP DB. Die bevorzugte Methode ist eine Momentaufnahmesicherung, bei der eine Datenbankgesamtsicherung erstellt wird, ohne geplante Sicherungen zu unterbrechen. Sie können eine Momentaufnahmesicherung beispielsweise mit dem folgenden Befehl erstellen:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Führen Sie den folgenden Befehl aus, um die Einheitenkonfigurationsdaten in einem anderen Verzeichnis zu sichern:

```
backup devconfig filenames=Dateiname
```

Hierbei gibt *Dateiname* den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.

3. Führen Sie den folgenden Befehl aus, um die Protokolldatei für Datenträger in einem anderen Verzeichnis zu sichern:

```
backup volhistory filenames=Dateiname
```

Hierbei gibt *Dateiname* den Namen der Datei an, in der Datenträgerprotokolldaten gespeichert werden sollen.

4. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dsmserv.opt heißt und sich im Serverinstanzverzeichnis befindet.
5. Stoppen Sie alle Instanzen des Servers. Stellen Sie sicher, dass keine Serverprozesse ausgeführt werden. Wenn Sie die Überwachung auf Anwendungsebene für den IBM Spectrum Protect-Server verwenden, setzen Sie die Überwachung der dsmserv-Anwendungsressource mit Ihrem Cluster-Tool aus.
6. Stellen Sie sicher, dass der Datenbankmanager auf keiner Instanz ausgeführt wird. Stellen Sie fest, ob db2sysc-Prozesse ausgeführt werden. Der Eigner aktiver Prozesse zeigt an, welche Instanzen aktiv sind. Führen Sie für jeden Serverinstanzeigner den folgenden Befehl aus, um DB2 zu stoppen:

```
db2stop
```

7. Stellen Sie sicher, dass sich die gemeinsam genutzten Ressourcen für alle IBM Spectrum Protect-Instanzen auf dem primären Knoten befinden. Stellen Sie sicher, dass keine anderen Knoten Schreibzugriff auf diese Ressourcen während des Upgrades haben. Wenn in der Umgebung mehrere Instanzen des Servers vorhanden sind, muss der primäre Knoten auf gemeinsam genutzte Ressourcen für alle Instanzen zugreifen können.
8. Installieren Sie den Server der Version 8.1.3 auf dem primären Knoten. Führen Sie hierfür den Befehl ./install.sh aus. Anweisungen finden Sie in Serverkomponenten installieren. Klicken Sie nach dem Start des Assistenten im Fenster von IBM Installation Manager auf das Symbol Installieren. Klicken Sie nicht auf das Symbol Aktualisieren oder Ändern. Sie müssen den Server der Version 8.1.3 installieren, um das Upgrade von Version 6.3 auf Version 8.1.3 abzuschließen.
9. Starten Sie jeden Server der Version 8.1.3 im Vordergrund:
  - a. Stellen Sie sicher, dass Sie mit der Instanzeigner-ID angemeldet sind.
  - b. Navigieren Sie zum Instanzverzeichnis und führen Sie den folgenden Befehl aus:

```
/opt/tivoli/tsm/server/bin/dsmserv
```

Warten Sie, bis die Eingabeaufforderung des Servers angezeigt wird, was bedeutet, dass der Server gestartet wurde.

10. Stoppen Sie den Server für jede IBM Spectrum Protect-Instanz, die aktualisiert wird. Führen Sie den folgenden Befehl aus:

```
halt
```

11. Führen Sie auf jedem sekundären Knoten im Cluster die folgenden Schritte aus:
  - a. Verschieben Sie alle gemeinsam genutzten Ressource auf den sekundären Knoten. Wenn in der Umgebung mehrere Instanzen des Servers vorhanden sind, müssen die sekundären Knoten während des Upgrades auf gemeinsam genutzte Ressourcen für alle Instanzen zugreifen können.
  - b. Stoppen Sie alle Instanzen des Servers. Stellen Sie sicher, dass keine Serverprozesse ausgeführt werden.
  - c. Stellen Sie sicher, dass der Datenbankmanager auf keiner Instanz ausgeführt wird. Stellen Sie fest, ob db2sysc-Prozesse ausgeführt werden. Der Eigner aktiver Prozesse zeigt an, welche Instanzen aktiv sind. Führen Sie für jeden Serverinstanzeigner den folgenden Befehl aus, um DB2 zu stoppen:

```
db2stop
```

- d. Installieren Sie den Server der Version 8.1.3 mit dem Befehl ./install.sh. Anweisungen finden Sie in Serverkomponenten installieren.
  - i. Wenn Sie den Installationsassistenten verwenden, klicken Sie im Fenster von IBM Installation Manager auf das Symbol Installieren. Klicken Sie nicht auf das Symbol Aktualisieren oder Ändern.

- ii. Wenn Sie den Installationsassistenten verwenden, wählen Sie auf der Seite Instanzberechtigungsanzeige das Kontrollkästchen Diese Instanz auf einem sekundären Knoten des Clusters konfigurieren für jede Instanz aus, die Sie konfigurieren wollen.
  - iii. Wenn Sie den Server im Konsolenmodus installieren, geben Sie an der Eingabeaufforderung Diese Instanz auf einem sekundären Knoten des Clusters konfigurieren? für jede Instanz Ja ein.
  - iv. Wenn Sie den Server im unbeaufsichtigten Modus installieren, geben Sie TRUE als Wert der Variablen `user.Instanzname_secondaryNode` für jede Instanz an.
- e. Stellen Sie sicher, dass jeder Server der Version 8.1.3 startet. Wenn Sie die Überwachung auf Anwendungsebene verwenden, starten Sie den Server mithilfe des Cluster-Tools.

Anweisungen zum Starten des Servers finden Sie in Serverinstanz starten.

12. Registrieren Sie die Lizenzen für die Serverkomponenten, die auf Ihrem System installiert sind. Führen Sie hierfür den Befehl REGISTER LICENSE aus:

```
register license file=Installationsverzeichnis/server/bin/Komponentenname.lic
```

Hierbei gibt *Installationsverzeichnis* das Verzeichnis an, in dem Sie die Komponente installiert haben, und *Komponentenname* ist die Abkürzung für die Komponente.

Wenn Sie den Server beispielsweise im Standardverzeichnis `/opt/tivoli/tsm` installiert haben, registrieren Sie die Lizenz mit dem folgenden Befehl:

```
register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
```

Wenn Sie IBM Spectrum Protect Extended Edition beispielsweise im Verzeichnis `/opt/tivoli/tsm` installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
```

Wenn Sie IBM Spectrum Protect for Data Retention beispielsweise im Verzeichnis `/opt/tivoli/tsm` installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

Einschränkung:

Sie können den IBM Spectrum Protect-Server nicht zum Registrieren von Lizenzen für die folgenden Produkte verwenden:

- o IBM Spectrum Protect for Mail
- o IBM Spectrum Protect for Databases
- o IBM Spectrum Protect for ERP
- o IBM Spectrum Protect for Space Management

Der Befehl REGISTER LICENSE ist für diese Lizenzen nicht gültig. Die Lizenzierung für diese Produkte wird von IBM Spectrum Protect-Clients ausgeführt.

#### Zugehörige Verweise:


BACKUP DB (Datenbank sichern)

BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)

BACKUP VOLHISTORY (History-Daten für sequentielle Datenträger sichern)

HALT (Server herunterfahren)

REGISTER LICENSE (Neue Lizenz registrieren)

 Linux-Betriebssysteme

## IBM Spectrum Protect-Upgrade auf Version 8.1.3 in einer Clusterumgebung unter Linux durchführen


---

Damit neue Funktionen in IBM Spectrum Protect genutzt werden können, können Sie ein Upgrade des IBM Spectrum Protect-Servers, der unter einem Linux-Betriebssystem in einer Clusterumgebung installiert ist, durchführen.

### Vorgehensweise

---

Befolgen Sie die Anweisungen in Linux-Umgebung für Clustering konfigurieren.

 Windows-Betriebssysteme

## Upgrade eines Servers der Version 6.3 oder Version 7.1 auf Version 8.1.3 in einer Clusterumgebung unter Windows durchführen

---

Damit neue Produktfunktionen genutzt werden können, können Sie ein Upgrade eines Servers, der unter einem Windows-Betriebssystem in einer Clusterumgebung installiert ist, von Version 6.3 oder Version 7.1 auf IBM Spectrum Protect Version 8.1.3 durchführen.

## Vorbereitende Schritte

---

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease des Servers der Version 6.3 oder Version 7.1, für das Sie ein Upgrade durchführen wollen, vorhanden sind. Wenn Sie den Server über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, müssen Sie die Lizenz von den Installationsmedien des Serverbasisrelease erneut installieren.

## Vorgehensweise

---

1. Sichern Sie die Datenbank mit dem Befehl BACKUP DB. Die bevorzugte Methode ist eine Momentaufnahmesicherung, bei der eine Datenbankgesamticherung erstellt wird, ohne geplante Sicherungen zu unterbrechen. Sie können beispielsweise den folgenden Befehl ausführen, um eine Momentaufnahmesicherung zu erstellen:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Sichern Sie die Einheitenkonfigurationsdaten in einem anderen Verzeichnis. Führen Sie den folgenden Befehl aus:

```
backup devconfig filenames=Dateiname
```

Hierbei gibt *Dateiname* den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.

3. Sichern Sie die Protokolldatei für Datenträger in einem anderen Verzeichnis. Führen Sie den folgenden Befehl aus:

```
backup volhistory filenames=Dateiname
```

Hierbei gibt *Dateiname* den Namen der Datei an, in der Datenträgerprotokolldaten gespeichert werden sollen.


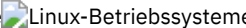

4. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dsmserv.opt heißt und sich im Serverinstanzverzeichnis befindet.
5. Stellen Sie sicher, dass sich die Ressourcengruppe im primären Knoten befindet und dass alle Knoten im Cluster aktiv sind. Führen Sie auf dem primären Knoten die folgenden Schritte aus:
  - a. Schalten Sie im Fenster Failovercluster-Manager die Serverressource offline und löschen Sie sie:
    - i. Wählen Sie Dienste und Anwendungen und dann die Clustergruppe aus. Die Serverressource wird im Abschnitt Andere Ressourcen angezeigt.
    - ii. Wählen Sie die Serverressource aus und klicken Sie auf Diese Ressource offline schalten.
    - iii. Um die Serverressource zu löschen, wählen Sie sie aus und klicken Sie auf Löschen.
  - b. Löschen Sie den Netznamen und die IP-Adresse im Fenster Failovercluster-Manager:
    - i. Blenden Sie im Abschnitt Servername den Netznamen ein, um die IP-Adresse anzuzeigen. Notieren Sie den Netznamen und die IP-Adresse.
    - ii. Wählen Sie den Netznamen und die IP-Adresse aus und klicken Sie auf Entfernen.
  - c. Schalten Sie im Fenster Failovercluster-Manager die DB2-Serverressource offline:
    - i. Wählen Sie Dienste und Anwendungen und dann die Clustergruppe aus. Die IBM Spectrum Protect-Serverressource wird im Abschnitt Andere Ressourcen angezeigt.
    - ii. Wählen Sie eine DB2-Serverressource aus (z. B. SERVER1) und klicken Sie auf Diese Ressource offline schalten.
6. Stellen Sie sicher, dass der Server auf dem Primärknoten ausgeführt wird. Führen Sie folgende Schritte auf allen anderen Clusterknoten aus:
  - a. Installieren Sie den IBM Spectrum Protect-Server der Version 8.1.3.
  - b. Stoppen Sie den Clusterdienst. Eine Möglichkeit ist die Verwendung der Anwendung 'Dienste'. Klicken Sie mit der rechten Maustaste auf Clusterdienst und wählen Sie Beenden aus.
  - c. Löschen Sie die Dateien tsmsvrscexX64.dll und tsmsvrscx64.dll aus dem Verzeichnis C:\Windows\Cluster.
  - d. Kopieren Sie die folgenden DLL-Dateien aus dem Installationsverzeichnis in das Verzeichnis C:\Windows\Cluster:
    - tsmsvrscexX64.dll
    - tsmsvrscx64.dll
  - e. Kopieren Sie die folgende DLL-Datei aus dem Installationsverzeichnis in das Verzeichnis C:\TSM\db2\security\plugin\IBM\server: dsmdb2pw64.dll
  - f. Starten Sie den Clusterdienst. Eine Möglichkeit ist die Verwendung der Anwendung 'Dienste'. Klicken Sie mit der rechten Maustaste auf Clusterdienst und wählen Sie Starten aus.
7. Versetzen Sie in Failovercluster-Manager die IBM Spectrum Protect-Serverinstanz vom Primärknoten auf einen anderen Knoten im Cluster.
8. Führen Sie auf dem Primärknoten die folgenden Schritte aus:
  - a. Installieren Sie den IBM Spectrum Protect-Server der Version 8.1.3.
  - b. Stoppen Sie den Clusterdienst.
  - c. Löschen Sie die Dateien tsmsvrscexX64.dll und tsmsvrscx64.dll aus dem Verzeichnis C:\Windows\Cluster.
  - d. Kopieren Sie die folgenden DLL-Dateien aus dem Installationsverzeichnis in das Verzeichnis C:\Windows\Cluster:
    - tsmsvrscexX64.dll

- tsmvrrscx64.dll
  - e. Kopieren Sie die folgende DLL-Datei aus dem Installationsverzeichnis in das Verzeichnis C:\TSM\db2\security\plugin\IBM\server: dsmdb2pw64.dll
  - f. Starten Sie den Clusterdienst.
9. Optional: Versetzen Sie die IBM Spectrum Protect-Serverinstanz zurück auf den Primärknoten.

## Nächste Schritte

Ist unter Windows ein Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, verwenden Sie den Einheitentreiber. Ist kein Einheitentreiber vorhanden, installieren Sie den IBM Spectrum Protect-Einheitentreiber mithilfe des Befehls dpinst.exe /a. Die Datei dpinst.exe befindet sich im Verzeichnis des Einheitentreibers und die Standardposition ist C:\Programme\Tivoli\TSM\device\drivers.

### Zugehörige Verweise:

- BACKUP DB (Datenbank sichern)
- BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)
- BACKUP VOLHISTORY (History-Daten für sequentielle Datenträger sichern)
- REGISTER LICENSE (Neue Lizenz registrieren)
-   

## Operations Center installieren und Operations Center-Upgrade durchführen

Das IBM Spectrum Protect Operations Center ist die webbasierte Schnittstelle für die Verwaltung Ihrer Speicherumgebung.

### Vorbereitende Schritte

Lesen Sie die folgenden Informationen, bevor Sie das Operations Center installieren und konfigurieren:

- Systemvoraussetzungen für das Operations Center
  - Voraussetzungen für den Computer des Operations Center
  - Voraussetzungen für Hub- und Peripherieserver
  - Betriebssystemvoraussetzungen
  - Voraussetzungen für den Web-Browser
  - Voraussetzungen für die Sprache
  - Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices
- Administrator-IDs, die für das Operations Center erforderlich sind
- IBM Installation Manager
- Prüfliste für die Installation
- Operations Center-Installationspaket abrufen

### Informationen zu diesem Vorgang



In Tabelle 1 sind die Methoden für die Installation oder Deinstallation des Operations Center aufgelistet. Außerdem ist angegeben, wo Sie die zugehörigen Anweisungen finden.


Informationen zum Upgrade des Operations Center finden Sie in Upgrade des Operations Center.

Tabelle 1. Methoden für die Installation oder Deinstallation des Operations Center

| Methode                         | Anweisungen  |
|---------------------------------|--|
| Grafisch orientierter Assistent | <ul style="list-style-type: none"> <li>• Operations Center mit einem grafisch orientierten Assistenten installieren</li> <li>• Operations Center mit einem grafisch orientierten Assistenten deinstallieren</li> </ul> |
| Konsolenmodus                   | <ul style="list-style-type: none"> <li>• Operations Center im Konsolenmodus installieren</li> <li>• Operations Center im Konsolenmodus deinstallieren</li> </ul>   |
| Unbeaufsichtigter Modus         | <ul style="list-style-type: none"> <li>• Operations Center im unbeaufsichtigten Modus installieren</li> <li>• Operations Center im unbeaufsichtigten Modus deinstallieren</li> </ul>                                   |

- Installation des Operations Center planen  
Vor der Installation des Operations Center müssen Sie die Systemvoraussetzungen, die Administrator-IDs, die das Operations Center benötigt, und die im Installationsprogramm anzugebenden Informationen kennen.

- Operations Center installieren  
Sie können das Operations Center mit jeder der folgenden Methoden installieren: grafischer Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.
- Upgrade des Operations Center  
Sie können ein Upgrade des Operations Center mit jeder der folgenden Methoden durchführen: grafisch orientierter Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.
- Erste Schritte mit dem Operations Center  
Bevor Sie das Operations Center für die Verwaltung Ihrer Speicherumgebung verwenden können, müssen Sie es konfigurieren.
-  AIX-Betriebssysteme  Linux-Betriebssysteme Fehlerbehebung für die Operations Center-Installation  
Wenn bei der Installation des Operations Center ein Problem auftritt, das Sie nicht lösen können, können Sie in den Beschreibungen der bekannten Probleme nach einer Lösungsmöglichkeit suchen.
- Operations Center deinstallieren  
Sie können das Operations Center mit jeder der folgenden Methoden deinstallieren: grafischer Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.
- Rollback zu einer vorherigen Version des Operations Center durchführen  
Standardmäßig speichert IBM Installation Manager ältere Versionen eines Pakets, damit ein Rollback ausgeführt werden kann, falls Probleme mit neueren Versionen von Updates, Fixes oder Paketen auftreten.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Installation des Operations Center planen

---

Vor der Installation des Operations Center müssen Sie die Systemvoraussetzungen, die Administrator-IDs, die das Operations Center benötigt, und die im Installationsprogramm anzugebenden Informationen kennen.

### Informationen zu diesem Vorgang

---

Mithilfe des Operations Center können Sie die folgenden Hauptaspekte der Speicherumgebung verwalten:

- IBM Spectrum Protect-Server und -Clients
- Services wie Sichern und Zurückschreiben, Archivieren und Abrufen sowie Umlagern und Zurückrufen
- Speicherpool und Speichereinheiten

Das Operations Center verfügt über folgende Funktionen:

Benutzerschnittstelle für mehrere Server

Sie können mit dem Operations Center mindestens einen IBM Spectrum Protect-Server verwalten.

In einer Umgebung mit mehreren Servern können Sie einen Server als *Hub-Server* und die übrigen Server als *Peripherieserver* festlegen. Der Hub-Server kann Alerts und Statusinformationen von den Peripherieservern empfangen und in einer konsolidierten Sicht im Operations Center anzeigen.

Alertüberwachung

Ein *Alert* ist eine Benachrichtigung über ein relevantes Problem auf dem Server und wird durch eine Servernachricht ausgelöst. Sie können definieren, welche Nachrichten Alerts auslösen, und nur diese Nachrichten werden als Alerts in der Operations Center oder in einer E-Mail aufgelistet.

Diese Alertüberwachung kann Ihnen beim Erkennen und Verfolgen relevanter Probleme auf dem Server helfen.

Komfortable Befehlszeilenschnittstelle

Das Operations Center verfügt über eine Befehlszeilenschnittstelle für erweiterte Funktionen und Konfiguration.

- Systemvoraussetzungen für das Operations Center  
Stellen Sie vor der Installation des Operations Center sicher, dass Ihr System die Mindestvoraussetzungen erfüllt.
- Administrator-IDs, die für das Operations Center erforderlich sind  
Ein Administrator muss für die Anmeldung beim Operations Center eine gültige ID und ein gültiges Kennwort auf dem Hub-Server haben. Eine Administrator-ID wird auch dem Operations Center zugeordnet, damit das Operations Center Server überwachen kann.
- IBM Installation Manager  
Das Operations Center verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositorys installiert oder aktualisiert werden können.
- Prüfliste für die Installation  
Bevor Sie das Operations Center installieren, müssen Sie bestimmte Informationen überprüfen, z. B. die Berechtigungsnachweise für die Installation, und Sie müssen die Eingabedaten festlegen, die in IBM Installation Manager für die Installation angegeben werden sollen.

## Systemvoraussetzungen für das Operations Center

Stellen Sie vor der Installation des Operations Center sicher, dass Ihr System die Mindestvoraussetzungen erfüllt.

Mithilfe des Operations Center System Requirements Calculator können Sie die Systemvoraussetzungen für die Ausführung des Operations Center sowie der vom Operations Center überwachten Hub- und Peripherieserver schätzen.

### Während der Installation überprüfte Voraussetzungen

Tabelle 1 enthält eine Auflistung der Voraussetzungen, die während der Installation überprüft werden, und Verweise auf weitere Informationen zu diesen Voraussetzungen.

Tabelle 1. Während der Installation überprüfte Voraussetzungen

| Voraussetzungen  | Details  |
|--|--|
| Mindestspeicherbedarf  | Voraussetzungen für den Computer des Operations Center |
| Betriebssystemvoraussetzungen  | Betriebssystemvoraussetzungen                          |
| Hostnamen des Computers, auf dem das Operations Center installiert werden soll | Prüfliste für die Installation                         |
| Voraussetzungen für das Operations Center-Installationsverzeichnis             | Prüfliste für die Installation                         |

- **Voraussetzungen für den Computer des Operations Center**  
Sie können das Operations Center auf einem Computer installieren, auf dem auch der IBM Spectrum Protect-Server ausgeführt wird, oder auf einem andere Computer. Wenn Sie das Operations Center zusammen mit einem Server auf demselben Computer installieren, muss dieser Computer die Systemvoraussetzungen für das Operations Center und für den Server erfüllen.
- **Voraussetzungen für Hub- und Peripherieserver**  
Wenn Sie das Operations Center zum ersten Mal öffnen, müssen Sie das Operations Center einem einzelnen IBM Spectrum Protect-Server zuordnen, der als *Hub-Server* festgelegt ist. In einer Umgebung mit mehreren Servern können Sie die anderen Server, die als *Peripherieserver* bezeichnet werden, mit dem Hub-Server verbinden.
- **Betriebssystemvoraussetzungen**  
Das Operations Center ist für AIX-, Linux- und Windows-Systeme verfügbar.
- **Voraussetzungen für den Web-Browser**  
Das Operations Center kann in Apple-, Google-, Microsoft- und Mozilla-Web-Browsern ausgeführt werden.
- **Voraussetzungen für die Sprache**  
Standardmäßig verwendet das Operations Center dieselbe Sprache wie der Web-Browser. Beim Installationsprozess wird jedoch die Sprache des Betriebssystems verwendet. Überprüfen Sie, ob für den Web-Browser und das Betriebssystem die erforderliche Sprache definiert ist.
- **Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices**  
IBM Spectrum Protect-Clientverwaltungsservices ist eine Komponente, die Sie auf Clients für Sichern/Archivieren installieren, um Diagnoseinformationen (z. B. Clientprotokolldateien) zu erfassen. Bevor Sie den Clientverwaltungsservice auf Ihrem System installieren, müssen Sie die Voraussetzungen und Einschränkungen kennen.

## Voraussetzungen für den Computer des Operations Center

Sie können das Operations Center auf einem Computer installieren, auf dem auch der IBM Spectrum Protect-Server ausgeführt wird, oder auf einem andere Computer. Wenn Sie das Operations Center zusammen mit einem Server auf demselben Computer installieren, muss dieser Computer die Systemvoraussetzungen für das Operations Center und für den Server erfüllen.

### Ressourcenanforderungen

Die folgenden Ressourcen sind für die Ausführung des Operations Center erforderlich:

- Ein Prozessorkern
- 4 GB Speicher
- 1 GB Plattenspeicherplatz

Für den Hub-Server und die Peripherieserver, die vom Operations Center überwacht werden, sind zusätzliche Ressourcen erforderlich (siehe Voraussetzungen für Hub- und Peripherieserver).

## Voraussetzungen für Hub- und Peripherieserver

Wenn Sie das Operations Center zum ersten Mal öffnen, müssen Sie das Operations Center einem einzelnen IBM Spectrum Protect-Server zuordnen, der als *Hub-Server* festgelegt ist. In einer Umgebung mit mehreren Servern können Sie die anderen Server, die als *Peripherieserver* bezeichnet werden, mit dem Hub-Server verbinden.

Die Peripherieserver senden Alerts und Statusinformationen an den Hub-Server. Das Operations Center zeigt eine konsolidierte Sicht der Alerts und Statusinformationen für den Hub-Server und alle Peripherieserver an.

Wird nur ein einziger Server vom Operations Center überwacht, wird dieser Server als Hub-Server bezeichnet, obwohl keine Peripherieserver mit ihm verbunden sind.

In Tabelle 1 ist die Version des IBM Spectrum Protect-Servers aufgeführt, die auf dem Hub-Server und auf jedem vom Operations Center verwalteten Peripherieserver installiert sein muss.

Tabelle 1. Voraussetzungen bezüglich der IBM Spectrum Protect-Serverversion für Hub- und Peripherieserver

| Operations Center | Version auf dem Hub-Server | Version auf jedem Peripherieserver  |
|-------------------|----------------------------|---|
| Version 8.1.3     | Version 8.1.3              | Version 6.3.4 oder höher<br>Einschränkung: Für Server mit einer Version vor Version 8.1.3 sind einige Operations Center-Funktionen nicht verfügbar. |

## Anzahl Peripherieserver, die ein Hub-Server unterstützen kann

Die Anzahl der Peripherieserver, die ein Hub-Server unterstützen kann, ist von der Konfiguration und von der Version von IBM Spectrum Protect auf jedem Peripherieserver abhängig. Eine allgemeine Richtlinie ist jedoch, dass ein Hub-Server 10 - 20 Peripherieserver der Version 6.3.4, aber mehr Peripherieserver der Version 7.1 oder höher unterstützen kann.

- Tipps für das Entwerfen der Hub- und Peripherieserverkonfiguration  
Berücksichtigen Sie beim Entwurf der Hub- und Peripherieserverkonfiguration insbesondere die Ressourcenanforderungen für die Statusüberwachung. Überlegen Sie außerdem, wie Sie Hub- und Peripherieserver gruppieren und ob Sie mehrere Hub-Server verwenden wollen.
- Tipps für die Auswahl eines Hub-Servers  
Als Hub-Server müssen Sie einen Server auswählen, der über angemessene Ressourcen verfügt und sich an einem Standort befindet, der minimale Umlaufzeit im Netz gewährleistet.

## Tipps für das Entwerfen der Hub- und Peripherieserverkonfiguration

Berücksichtigen Sie beim Entwurf der Hub- und Peripherieserverkonfiguration insbesondere die Ressourcenanforderungen für die Statusüberwachung. Überlegen Sie außerdem, wie Sie Hub- und Peripherieserver gruppieren und ob Sie mehrere Hub-Server verwenden wollen.

Mithilfe des Operations Center System Requirements Calculator können Sie die Systemvoraussetzungen für die Ausführung des Operations Center sowie der vom Operations Center überwachten Hub- und Peripherieserver schätzen.

## Primäre leistungsrelevante Faktoren

Die folgenden Faktoren haben den größten Einfluss auf die Leistung des Operations Center:

- Der Prozessor und Speicher auf dem Computer, auf dem das Operations Center installiert ist.
- Die Systemressourcen der Hub- und Peripherieserver, einschließlich des für die Hub-Serverdatenbank verwendeten Plattensystems.
- Die Anzahl der Clientknoten und Dateibereiche für virtuelle Maschinen, die von den Hub- und Peripherieservern verwaltet werden.
- Die Aktualisierungshäufigkeit der Daten im Operations Center.

## Hub- und Peripherieserver gruppieren

Erwägen Sie die Gruppierung von Hub- und Peripherieservern nach Standort. Durch die Verwaltung der Server in demselben Rechenzentrum können beispielsweise Probleme vermieden werden, die durch Firewalls oder unzulängliche Netzbandbreite zwischen verschiedenen Standorten verursacht werden. Bei Bedarf können Sie die Server anhand der folgenden Merkmale weiter unterteilen:

- Administrator, der die Server verwaltet
- Organisationsentität, die die Server finanziert
- Serverbetriebssystem
- Sprache, mit der die Server ausgeführt werden.

Tipp: Werden Hub- und Peripherieserver nicht mit derselben Sprache ausgeführt, könnte fehlerhafter Text im Operations Center angezeigt werden.

## Hub- und Peripherieserver in einer unternehmensweiten Konfiguration gruppieren

---

In einer unternehmensweiten Konfiguration wird ein IBM Spectrum Protect-Servernetz als Gruppe verwaltet. Im *Konfigurationsmanager* vorgenommene Änderungen können automatisch an mindestens einen *verwalteten Server* im Netz verteilt werden.

Normalerweise registriert und verwaltet das Operations Center eine dedizierte Administrator-ID auf den Hub- und Peripherieservern. Dieser *Überwachungsadministrator* muss auf allen Servern immer dasselbe Kennwort haben.

Wenn Sie eine unternehmensweite Konfiguration verwenden, können Sie den Prozess, durch den die Administratorberechtigungsanzeige auf Peripherieservern synchronisiert werden, verbessern. Gehen Sie wie folgt vor, um die Leistung und Effizienz bei der Verwaltung der Überwachungsadministrator-ID zu verbessern:

1. Legen Sie den Konfigurationsmanagerserver als Hub-Server des Operations Center fest. Während der Hub-Server-Konfiguration wird die Überwachungsadministrator-ID 'IBM-OC-Hub-Server-Name' registriert.
2. Auf dem Hub-Server fügen Sie die Überwachungsadministrator-ID einem neuen oder vorhandenen Profil für die unternehmensweite Konfiguration hinzu. Geben Sie den Befehl NOTIFY SUBSCRIBERS aus, um das Profil an die verwalteten Server zu verteilen.
3. Fügen Sie mindestens einen der verwalteten Server als Peripherieserver des Operations Center hinzu.

Das Operations Center erkennt diese Konfiguration und gestattet dem Konfigurationsmanager, die Überwachungsadministrator-ID auf den Peripherieservern zu verteilen und zu aktualisieren.

## Verwendung mehrerer Hub-Server

---

Sind mehr als 10 bis 20 Peripherieserver der Version 6.3.4 vorhanden oder muss die Umgebung aufgrund von Ressourceneinschränkungen partitioniert werden, können Sie mehrere Hub-Server konfigurieren und jeden Hub-Server mit einer Untergruppe der Peripherieserver verbinden.

Einschränkungen:

- Derselbe Server kann nicht gleichzeitig Hub-Server und Peripherieserver sein.
- Jeder Peripherieserver kann nur einem einzigen Hub-Server zugeordnet sein.
- Für jeden Hub-Server ist eine separate Operations Center-Instanz mit einer separaten Webadresse erforderlich.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Tipps für die Auswahl eines Hub-Servers

---

Als Hub-Server müssen Sie einen Server auswählen, der über angemessene Ressourcen verfügt und sich an einem Standort befindet, der minimale Umlaufzeit im Netz gewährleistet.

Achtung: Verwenden Sie nicht einen einzigen Server als Hub-Server für mehrere Operations Center.

Treffen Sie Ihre Entscheidung darüber, welcher Server als Hub-Server festgelegt werden soll, anhand der folgenden Richtlinien:

Wählen Sie einen Server mit **geringer Auslastung**

Sie sollten einen Server mit einer geringen Auslastung für Operationen wie z. B. Clientsicherung und -archivierung auswählen. Ein Server mit geringer Auslastung ist auch eine gute Wahl als Hostsystem für das Operations Center.

Stellen Sie sicher, dass der Server über die Ressourcen zur Bearbeitung sowohl seiner normalen Serverauslastung als auch der geschätzten Auslastung für seine Rolle als Hub-Server verfügt.

Positionieren Sie den Server so, dass minimale Umlaufzeit im Netz entsteht

Positionieren Sie den Hub-Server so, dass die Netzverbindung zwischen dem Hub-Server und den Peripherieservern eine Umlaufzeit von maximal 5 ms aufweist. Diese Latenzzeit kann normalerweise erreicht werden, wenn sich die Server in demselben lokalen Netz (LAN) befinden.

Netze, die schlecht eingestellt sind, von anderen Anwendungen stark genutzt werden oder eine Umlaufzeit von sehr viel mehr als 5 ms haben, können die Kommunikation zwischen dem Hub-Server und den Peripherieservern verschlechtern. Umlaufzeiten von 50 ms oder mehr können z. B. Überschreitungen des Kommunikationszeitlimits bewirken, die eine Trennung oder Wiederherstellung der Peripherieserververbindung zum Operations Center verursachen. Derartig lange Latenzzeiten können bei der Kommunikation im Weitverkehrsnetz (WAN) auftreten.



Wenn der Abstand zwischen den Peripherieservern und dem Hub-Server sehr groß ist und häufige Trennungen der Peripherieserververbindung im Operations Center auftreten, können Sie den Wert der Option ADMINCOMMTIMEOUT auf jedem Server erhöhen, um das Problem zu verkleinern.

Stellen Sie sicher, dass der Hub-Server die Ressourcenanforderungen für die Statusüberwachung erfüllt

Für die Statusüberwachung werden zusätzliche Ressourcen auf jedem Server benötigt, auf dem sie aktiviert ist. Der Ressourcenbedarf ist hauptsächlich von der Anzahl Clients abhängig, die von den Hub- und Peripherieservern verwaltet werden. Auf einem Hub-Server mit einem Peripherieserver der Version 7.1 oder höher werden weniger Ressourcen verwendet als auf einem Hub-Server mit einem Peripherieserver der Version 6.3.4.

Stellen Sie sicher, dass der Hub-Server die Ressourcenanforderungen bezüglich der Prozessorauslastung, des Datenbankbereichs, des Speicherbereichs für das Archivprotokoll und der IOPS-Kapazität erfüllt (IOPS = E/A-Operationen pro Sekunde).

Ein Hub-Server mit hoher IOPS-Kapazität kann ein hohes Volumen eingehender Statusdaten von Peripherieservern bearbeiten. Die Erfüllung dieser Kapazitätsanforderung kann durch die Verwendung der folgenden Speichereinheiten für die Hub-Server-Datenbank erleichtert werden:

- Ein Solid-State-Laufwerk (SSD) auf Unternehmensebene
- Eine externe SAN-Plattenspeichereinheit mit mehreren Datenträgern oder mehreren Spindeln unter jedem Datenträger

In einer Umgebung mit weniger als 1000 Clients sollten Sie das Einrichten einer Basiskapazität von 1000 E/A-Operationen pro Sekunde für die Hub-Serverdatenbank in Betracht ziehen, wenn der Hub-Server Peripherieserver verwaltet.

Stellen Sie fest, ob in Ihrer Umgebung mehrere Hub-Server erforderlich sind

Wenn eine aus einem Hub-Server und Peripherieservern bestehende Gruppe mehr als 10.000 bis 20.000 Clientknoten und Dateibereiche für virtuelle Maschinen verwaltet, könnte der Ressourcenbedarf die verfügbaren Ressourcen des Hub-Servers übersteigen, insbesondere, wenn es sich bei den Peripherieservern um Server der Version 6.3.4 handelt. In diesem Fall sollten Sie einen zweiten Server als Hub-Server angeben und zum Lastausgleich Peripherieserver zum neuen Hub-Server versetzen.

## Betriebssystemvoraussetzungen

---

Das Operations Center ist für AIX-, Linux- und Windows-Systeme verfügbar.

Sie können das Operations Center auf den folgenden Systemen ausführen:

-  AIX-Betriebssysteme AIX-Systeme:
  - IBM® AIX V7.1 (64 Bit) TL 4 und SP 2
  - IBM AIX V7.2 (64 Bit) TL 0 und SP 2
-  Linux-Betriebssysteme Linux on x86\_64-Systeme:
  - Red Hat Enterprise Linux 6.7
  - Red Hat Enterprise Linux 7.1
  - SUSE Linux Enterprise Server 11, Service-Pack 4 oder höher
  - SUSE Linux Enterprise Server 12
-  Linux-Betriebssysteme Linux on System z-Systeme (s390x 64-Bit-Architektur):
  - Red Hat Enterprise Linux 7.1
  - SUSE Linux Enterprise Server 12
-  Linux-Betriebssysteme Linux on Power Systems-Systeme (Little Endian):
  - Red Hat Enterprise Linux 7 mit PPC64LE-Architektur
-  Windows-Betriebssysteme Windows-Systeme:
  - Microsoft Windows Server 2012: Standard, Enterprise oder Datacenter Edition (64-Bit)
  - Microsoft Windows Server 2012 R2 (64-Bit)
  - Microsoft Windows Server 2016

Aktuelle Informationen zu den Anforderungen finden Sie unter Software and Hardware Requirements.

## Voraussetzungen für den Web-Browser

---

Das Operations Center kann in Apple-, Google-, Microsoft- und Mozilla-Web-Browsern ausgeführt werden.

Stellen Sie für eine optimale Anzeige des Operations Center im Web-Browser sicher, dass die Bildschirmauflösung für das System mindestens auf 1024 x 768 Pixel gesetzt ist.

Verwenden Sie einen Web-Browser mit guter JavaScript-Leistung und aktivieren Sie Browser-Caching, um eine optimale Leistung zu erzielen.

Das Operations Center kann in den folgenden Web-Browsern ausgeführt werden:

- Apple Safari auf dem iPad  
Einschränkung: Wird Apple Safari unter iOS 8.x oder iOS 9.x ausgeführt, können Sie ein selbst signiertes Zertifikat für die sichere Kommunikation mit dem Operations Center nur mit zusätzlicher Konfiguration des Zertifikats verwenden. Verwenden Sie ein Zertifikat einer Zertifizierungsstelle (CA-Zertifikat) oder konfigurieren Sie das selbst signierte Zertifikat nach Bedarf. Anweisungen finden Sie im technischen Hinweis (Technote) <http://www.ibm.com/support/docview.wss?uid=swg21963153>.
- Google Chrome 40 oder höher
- Microsoft Internet Explorer 11 oder höher
- Mozilla Firefox ESR 31 oder höher

Damit das Operations Center gemäß der Empfehlung von National Institute of Standards and Technology (NIST) Special Publications (SP) 800-131A ausgeführt werden kann, muss die Kommunikation zwischen dem Operations Center und dem Web-Browser mit dem TLS 1.2-Protokoll (TLS = Transport Layer Security) geschützt werden. Während der Installation geben Sie an, ob die Einhaltung von SP 800-131A erforderlich ist, sowie die Stufe der Einhaltung. Wenn während der Installation die strikte Einhaltung von SP 800-131A angegeben wird, muss der Web-Browser TLS 1.2 unterstützen und TLS 1.2 muss aktiviert sein.

Der Web-Browser zeigt einen SSL-Fehler an, wenn während der Installation die strikte Einhaltung von SP 800-131A angegeben wird, ohne dass der Web-Browser die vorangegangenen Voraussetzungen erfüllt.

## Voraussetzungen für die Sprache

Standardmäßig verwendet das Operations Center dieselbe Sprache wie der Web-Browser. Beim Installationsprozess wird jedoch die Sprache des Betriebssystems verwendet. Überprüfen Sie, ob für den Web-Browser und das Betriebssystem die erforderliche Sprache definiert ist.

 AIX-Betriebssysteme

Tabelle 1. Operations Center-Sprachwerte, die Sie auf AIX-Systemen verwenden können

| <b>Sprache</b>                         | <b>Wert für die Sprachoption</b> |
|--|----------------------------------|
| Chinesisch, vereinfacht                | zh_CN                            |
| Chinesisch, vereinfacht (UTF-8)        | ZH_CN                            |
| Chinesisch, traditionell (Big5)        | Zh_TW                            |
| Chinesisch, traditionell (UTF-8)       | ZH_TW                            |
| Chinesisch, traditionell (euc_tw)      | zh_TW                            |
| Englisch                               | en_US                            |
| Englisch (UTF-8)                       | EN_US                            |
| Französisch                            | fr_FR                            |
| Französisch (UTF-8)                    | FR_FR                            |
| Deutsch                                | de_DE                            |
| Deutsch (UTF-8)                        | DE_DE                            |
| Italienisch                            | it_IT                            |
| Italienisch (UTF-8)                    | IT_IT                            |
| Japanisch (EUC)                        | ja_JP                            |
| Japanisch (PC)                         | Ja_JP                            |
| Japanisch (UTF-8)                      | JA_JP                            |
| Koreanisch                             | ko_KR                            |
| Koreanisch (UTF-8)                     | KO_KR                            |
| Portugiesisch, Brasilianisches         | pt_BR                            |
| Portugiesisch, Brasilianisches (UTF-8) | PT_BR                            |

| <b>Sprache</b>   | <b>Wert für die Sprachoption</b> |
|------------------|----------------------------------|
| Russisch         | ru_RU                            |
| Russisch (UTF-8) | RU_RU                            |
| Spanisch         | es_ES                            |
| Spanisch (UTF-8) | ES_ES                            |


 Linux-Betriebssysteme

Tabelle 2. Operations Center-Sprachwerte, die Sie auf Linux-Systemen verwenden können

| <b>Sprache</b>                         | <b>Wert für die Sprachoption</b> |
|--|----------------------------------|
| Chinesisch, vereinfacht                | zh_CN                            |
| Chinesisch, vereinfacht (GBK)          | zh_CN.gb18030                    |
| Chinesisch, vereinfacht (UTF-8)        | zh_CN.utf8                       |
| Chinesisch, traditionell (Big5)        | Zh_TW                            |
| Chinesisch, traditionell (euc_tw)      | zh_TW                            |
| Chinesisch, traditionell (UTF-8)       | zh_TW.utf8                       |
| Englisch, Vereinigte Staaten           | en_US                            |
| Englisch (UTF-8)                       | en_US.utf8                       |
| Französisch                            | fr_FR                            |
| Französisch (UTF-8)                    | fr_FR.utf8                       |
| Deutsch                                | de_DE                            |
| Deutsch (UTF-8)                        | de_DE.utf8                       |
| Italienisch                            | it_IT                            |
| Italienisch (UTF-8)                    | it_IT.utf8                       |
| Japanisch (EUC)                        | ja_JP                            |
| Japanisch (UTF-8)                      | ja_JP.utf8                       |
| Koreanisch                             | ko_KR                            |
| Koreanisch (UTF-8)                     | ko_KR.utf8                       |
| Portugiesisch, Brasilianisches         | pt_BR                            |
| Portugiesisch, Brasilianisches (UTF-8) | pt_BR.utf8                       |
| Russisch                               | ru_RU                            |
| Russisch (UTF-8)                       | ru_RU.utf8                       |
| Spanisch                               | es_ES                            |
| Spanisch (UTF-8)                       | es_ES.utf8                       |





 Windows-Betriebssysteme

Tabelle 3. Operations Center-Sprachwerte, die Sie auf Windows-Systemen verwenden können

| <b>Sprache</b>           | <b>Wert für die Sprachoption</b> |
|--------------------------|----------------------------------|
| Chinesisch, vereinfacht  | chs                              |
| Chinesisch, traditionell | cht                              |
| Englisch                 | ameng                            |
| Französisch              | fra                              |
| Deutsch                  | deu                              |
| Italienisch              | ita                              |
| Japanisch (Shift-JIS)    | jpn                              |
| Koreanisch               | kor                              |

| Sprache                        | Wert für die Sprachoption |
|--------------------------------|---------------------------|
| Portugiesisch, Brasilianisches | ptb                       |
| Russisch                       | rus                       |
| Spanisch                       | esp                       |

## Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices

IBM Spectrum Protect-Clientverwaltungsservices ist eine Komponente, die Sie auf Clients für Sichern/Archivieren installieren, um Diagnoseinformationen (z. B. Clientprotokolldateien) zu erfassen. Bevor Sie den Clientverwaltungsservice auf Ihrem System installieren, müssen Sie die Voraussetzungen und Einschränkungen kennen.

In der Dokumentation für den Clientverwaltungsservice ist *Clientsystem* das System, in dem der Client für Sichern/Archivieren installiert ist.

Diagnoseinformationen können nur von Linux- und Windows-Clients erfasst werden. Administratoren können jedoch die Diagnoseinformationen unter AIX, Linux oder Windows im Operations Center anzeigen.

### Voraussetzungen für den Clientverwaltungsservice

Lesen Sie die folgenden Informationen zu den Voraussetzungen, bevor Sie den Clientverwaltungsservice installieren:

- Für einen Fernzugriff auf den Client benötigt der Operations Center-Administrator Systemberechtigung oder eine der folgenden Clientberechtigungsstufen:
  - Maßnahmenberechtigung
  - Clienteignerberechtigung
  - Clientknotenzugriffsberechtigung
- Stellen Sie sicher, dass das Clientsystem die folgenden Voraussetzungen erfüllt:
  - Der Clientverwaltungsservice kann nur in Clientsystemen installiert werden, die mit Linux- oder Windows-Betriebssystemen ausgeführt werden:
    - Linux x86-64-Bit-Betriebssysteme, die für den Client für Sichern/Archivieren unterstützt werden.
    - Windows-32-Bit- und -64-Bit-Betriebssysteme, die für den Client für Sichern/Archivieren unterstützt werden.
  - Für die Datenübertragung zwischen dem Clientverwaltungsservice und dem Operations Center muss Transport Layer Security (TLS) 1.2 installiert sein. Es steht Basisauthentifizierung zur Verfügung und Daten sowie Authentifizierungsinformationen werden über den SSL-Kanal verschlüsselt. TLS 1.2 wird bei der Installation des Clientverwaltungsservice automatisch zusammen mit den erforderlichen SSL-Zertifikaten installiert.
- Auf Linux-Clientsystemen benötigen Sie Rootberechtigung für die Installation des Clientverwaltungsservice.
- Bei Clientsystemen, die mehrere Clientknoten haben können, z. B. Linux-Clientsysteme, muss jeder Knotenname im Clientsystem eindeutig sein.  
Tipp: Nach der Installation des Clientverwaltungsservice müssen Sie ihn nicht erneut installieren, weil der Service mehrere Clientoptionsdateien erkennen kann.

### Einschränkungen des Clientverwaltungsservice

Der Clientverwaltungsservice stellt Basisservices für die Erfassung von Diagnoseinformationen aus den Clients für Sichern/Archivieren bereit. Für den Clientverwaltungsservice bestehen die folgenden Einschränkungen:

- Sie können den Clientverwaltungsservice nur auf Systemen mit Clients für Sichern/Archivieren installieren, einschließlich Clients für Sichern/Archivieren, die auf Knoten mit Einheiten zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware installiert sind.
- Sie können den Clientverwaltungsservice nicht auf anderen IBM Spectrum Protect-Clientkomponenten oder -Produkten installieren, die keine Clients für Sichern/Archivieren aufweisen.
- Wenn die Clients für Sichern/Archivieren durch eine Firewall geschützt sind, müssen Sie sicherstellen, dass das Operations Center durch die Firewall mithilfe des konfigurierten Anschlusses für den Clientverwaltungsservice eine Verbindung zu den Clients für Sichern/Archivieren herstellen kann. Der Standardanschluss ist 9028, der jedoch geändert werden kann.
- Der Clientverwaltungsservice überprüft alle Clientprotokolldateien auf Einträge für den vorhergehenden Zeitraum von 72 Stunden.
- Die Diagnosesseite im Operations Center enthält Basisinformationen zur Fehlerbehebung für Clients für Sichern/Archivieren. Bei einigen Sicherungsproblemen müssen Sie jedoch u. U. auf das Clientsystem zugreifen und weitere Diagnoseinformationen abrufen.
- Wenn die Clientfehlerprotokolldateien und die Planungsprotokolldateien in einem Clientsystem zusammen eine Größe von mehr als 500 MB haben, können beim Senden von Protokollsätzen an das Operations Center Verzögerungen auftreten. Sie können die




Größe der Protokolldateien steuern, indem Sie eine Bereinigung oder einen Umlauf von Protokolldateien durch Angabe der Clientoption `errorlogretention` bzw. `errorlogmax` ermöglichen.

- Wenn Sie denselben Clientknotenamen verwenden, um eine Verbindung zu mehreren IBM Spectrum Protect-Servern herzustellen, die auf derselben Server-Hardware installiert sind, können Sie Protokolldateien für nur einen der Clientknoten anzeigen.

Aktualisierungen zum Clientverwaltungsservice, einschließlich Voraussetzungen, Einschränkungen und Dokumentationsaktualisierungen, finden Sie in [Technote 1963610](#).

#### Zugehörige Tasks:

Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen

## Administrator-IDs, die für das Operations Center erforderlich sind

---

Ein Administrator muss für die Anmeldung beim Operations Center eine gültige ID und ein gültiges Kennwort auf dem Hub-Server haben. Eine Administrator-ID wird auch dem Operations Center zugeordnet, damit das Operations Center Server überwachen kann.

Für das Operations Center sind die folgenden IBM Spectrum Protect-Administrator-IDs erforderlich:

Auf dem Hub-Server registrierte Administrator-IDs

Jede Administrator-ID, die auf dem Hub-Server registriert ist, kann für die Anmeldung beim Operations Center verwendet werden. Die Berechtigungsstufe der ID bestimmt die Tasks, die ausgeführt werden können. Sie können neue Administrator-IDs mit dem Befehl `REGISTER ADMIN` erstellen.

Einschränkung: Um eine Administrator-ID in einer serverübergreifenden Konfiguration verwenden zu können, muss die ID mit demselben Kennwort und derselben Berechtigungsstufe auf dem Hub-Server und den Peripherieservern registriert werden. Die Authentifizierung für diese Server können Sie mit einer der folgenden Methoden verwalten:

- Mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol).
- Mit den Funktionen für die unternehmensweite Konfiguration, mit denen Änderungen an den Administratordefinitionen automatisch verteilt werden.

Überwachungsadministrator-ID




Wenn Sie den Hub-Server anfänglich konfigurieren, wird eine Administrator-ID mit dem Namen `IBM-OC-Servername` mit Systemberechtigung auf dem Hub-Server registriert und dem von Ihnen angegebenen Anfangskennwort zugeordnet. Diese ID, die manchmal als *Überwachungsadministrator* bezeichnet wird, ist nur für die Verwendung durch das Operations Center bestimmt.

Sie dürfen diese ID nicht löschen, sperren oder ändern. Dieselbe Administrator-ID mit demselben Kennwort wird auf den Peripherieservern registriert, die Sie hinzufügen. Das Kennwort wird automatisch alle 90 Tage auf dem Hub-Server und den Peripherieservern geändert. Sie müssen dieses Kennwort nicht verwenden oder verwalten.

Einschränkung: Das Operations Center verwaltet die ID und das Kennwort des Überwachungsadministrators auf Peripherieservern, falls Sie diese Berechtigungsnachweise nicht mithilfe einer unternehmensweiten Konfiguration verwalten. Weitere Informationen zur Verwaltung der Berechtigungsnachweise mithilfe einer unternehmensweiten Konfiguration finden Sie in [Tipps für das Entwerfen der Hub- und Peripherieserverkonfiguration](#).

#### Zugehörige Verweise:

`REGISTER ADMIN` (Administrator-ID registrieren)

## IBM Installation Manager

---

Das Operations Center verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositorys installiert oder aktualisiert werden können.

Wenn die erforderliche Version von IBM Installation Manager nicht bereits installiert ist, wird sie automatisch installiert oder aktualisiert, wenn Sie das Operations Center installieren. Die Software muss auf dem System installiert bleiben, damit das Operations Center später nach Bedarf aktualisiert oder deinstalliert werden kann.

Die folgende Liste enthält Erläuterungen einiger Begriffe, die in IBM Installation Manager verwendet werden:

Angebot

Eine installierbare Einheit eines Softwareprodukts.

Das Angebot 'Operations Center' enthält alle Datenträger, die IBM Installation Manager für die Installation des Operations Center benötigt.

## Paket

Die Gruppe der Softwarekomponenten, die für die Installation eines Angebots benötigt werden.  
Das Operations Center-Paket enthält folgende Komponenten:

- Installationsprogramm von IBM Installation Manager
- Das Angebot 'Operations Center'

## Paketgruppe

Eine Gruppe von Paketen mit demselben übergeordneten Verzeichnis.

## Repository

Ein ferner oder lokaler Speicherbereich für Daten und andere Anwendungsressourcen.

Das Operations Center-Paket wird in einem Repository in IBM Fix Central gespeichert.

## Verzeichnis für gemeinsam genutzte Ressourcen

Ein Verzeichnis, das Softwaredateien oder Plug-ins enthält, die von Paketen gemeinsam genutzt werden.

In dem Verzeichnis für gemeinsam genutzte Ressourcen speichert IBM Installation Manager installationsbezogene Dateien, darunter Dateien, die für das Rollback zu einer vorherigen Version des Operations Center verwendet werden.



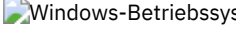
# Prüfliste für die Installation




Bevor Sie das Operations Center installieren, müssen Sie bestimmte Informationen überprüfen, z. B. die Berechtigungsnachweise für die Installation, und Sie müssen die Eingabedaten festlegen, die in IBM® Installation Manager für die Installation angegeben werden sollen.

Die folgende Prüfliste enthält eine Zusammenfassung der Informationen, die Sie überprüfen bzw. festlegen müssen, bevor Sie das Operations Center installieren. In Tabelle 1 werden diese Informationen dann ausführlich beschrieben.

- Den Hostnamen des Computers überprüfen, auf dem das Operations Center installiert werden soll.
- Die Berechtigungsnachweise für die Installation überprüfen.
- Das Installationsverzeichnis für das Operations Center festlegen, wenn der Standardpfad nicht übernommen werden soll.
- Das Installationsverzeichnis für IBM Installation Manager festlegen, wenn der Standardpfad nicht übernommen werden soll.
- Die vom Operations Center zu verwendende Anschlussnummer festlegen, wenn die Standardanschlussnummer nicht übernommen werden soll.
- Das Kennwort für die sichere Kommunikation festlegen.

Tabelle 1. Vor der Installation des Operations Center zu überprüfende bzw. festzulegende Informationen

| Informationen  | Details   |
|--|---|
| Hostname des Computers, auf dem das Operations Center installiert werden soll. | Der Hostname muss die folgenden Kriterien erfüllen: <ul style="list-style-type: none"><li>• Der Name darf keine Zeichen aus Doppelbytezeichensätzen (DBCS) und keine Unterstreichungszeichen ( _ ) enthalten.</li><li>• Der Hostname darf zwar einen Bindestrich ( - ) enthalten, jedoch nicht als letztes Zeichen.</li></ul>   |
| Berechtigungsnachweise für die Installation                                    | Für die Installation des Operations Center müssen Sie das folgende Benutzerkonto verwenden: <ul style="list-style-type: none"><li>•   Rootbenutzer</li><li>•  Administrator</li></ul> |



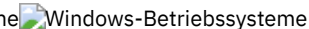
| Informationen   | Details   |
|---|---|
| <p>Operations Center-Installationsverzeichnis</p>                   | <p>Das Operations Center wird im Unterverzeichnis ui des Installationsverzeichnisses installiert.</p> <p>Der folgende Pfad ist der Standardpfad für das Operations Center-Installationsverzeichnis:</p> <ul style="list-style-type: none"> <li>•  Linux-Betriebssysteme/opt/tivoli/tsm<br/>Wenn Sie beispielsweise diesen Standardpfad verwenden, wird das Operations Center in dem folgenden Verzeichnis installiert:<br/><br/><code>/opt/tivoli/tsm/ui</code></li> <li>•  Windows-Betriebssysteme:\Programme\Tivoli\TSM<br/>Wenn Sie beispielsweise diesen Standardpfad verwenden, wird das Operations Center in dem folgenden Verzeichnis installiert:<br/><br/><code>c:\Programme\Tivoli\TSM\ui</code></li> </ul> <p>Der Installationsverzeichnispfad muss die folgenden Kriterien erfüllen:</p> <ul style="list-style-type: none"> <li>• Der Pfad darf maximal 128 Zeichen enthalten.</li> <li>• Der Pfad darf nur ASCII-Zeichen enthalten.</li> <li>• Der Pfad darf keine nicht anzeigbaren Steuerzeichen enthalten.</li> <li>• Der Pfad darf keines der folgenden Zeichen enthalten:<br/><br/><code>%   &lt; &gt; ' " \$ &amp; ; *</code></li> </ul> |
| <p>IBM Installation Manager-Installationsverzeichnis</p>            | <p>Der folgende Pfad ist der Standardpfad für das IBM Installation Manager-Installationsverzeichnis:</p> <ul style="list-style-type: none"> <li>•  Linux-Betriebssysteme/opt/IBM/InstallationManager</li> <li>•  Windows-BetriebssystemeC:\Programme\IBM\Installation Manager</li> </ul>  |
| <p>Vom Operations Center-Web-Server verwendete Anschlussnummer.</p> | <p>Der Wert für die sichere (HTTPS) Anschlussnummer muss die folgenden Kriterien erfüllen:</p> <ul style="list-style-type: none"> <li>• Die Nummer muss eine ganze Zahl im Bereich von 1024 bis 65535 sein.</li> <li>• Die Nummer darf nicht bereits im Gebrauch oder anderen Programmen zugeordnet sein.</li> </ul> <p>Wenn Sie keine Anschlussnummer angeben, lautet der Standardwert 11090.</p> <p>Tipp: Wenn Sie sich später nicht mehr an die angegebene Anschlussnummer erinnern können, schauen Sie in der folgenden Datei nach (<i>Installationsverzeichnis</i> steht für das Verzeichnis, in dem das Operations Center installiert ist):</p> <ul style="list-style-type: none"> <li>•  Linux-Betriebssysteme<br/><code>Installationsverzeichnis/ui/Liberty/usr/servers/guiServer/bootstrap.properties</code></li> <li>•  Windows-Betriebssysteme<br/><code>Installationsverzeichnis\ui\Liberty\usr\servers\guiServer\bootstrap.properties</code></li> </ul> <p>Die Datei bootstrap.properties enthält die Verbindungsdaten des IBM Spectrum Protect-Servers.</p>   |

| Informationen                          | Details  |
|--|--|
| Kennwort für die sichere Kommunikation | <p>Das Operations Center verwendet HTTPS (Hypertext Transfer Protocol Secure) für die Kommunikation mit Web-Browsern.</p> <p>Für das Operations Center ist die sichere Kommunikation zwischen dem Server und dem Operations Center erforderlich. Um die Kommunikation zu schützen, müssen Sie das TLS-Zertifikat des Hub-Servers zur Truststore-Datei des Operations Center hinzufügen (TLS = Transport Layer Security).</p> <p>Die Truststore-Datei des Operations Center enthält das Zertifikat, das das Operations Center für die HTTPS-Kommunikation mit Web-Browsern verwendet. Während der Installation des Operations Center erstellen Sie ein Kennwort für die Truststore-Datei. Wenn Sie die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server einrichten zu können, müssen Sie dasselbe Kennwort verwenden, um das Zertifikat des Hub-Servers der Truststore-Datei hinzuzufügen.</p> <p>Das Kennwort für die Truststore-Datei muss die folgenden Kriterien erfüllen:</p> <ul style="list-style-type: none"> <li>• Das Kennwort darf mindestens 6 Zeichen und maximal 64 Zeichen enthalten.</li> <li>• Das Kennwort muss mindestens die folgenden Zeichen enthalten: <ul style="list-style-type: none"> <li>○ Einen Großbuchstaben (A – Z)</li> <li>○ Einen Kleinbuchstaben (a – z)</li> <li>○ Eine Ziffer (0 – 9)</li> <li>○ Zwei der nachfolgend aufgelisteten nicht alphanumerischen Zeichen:</li> </ul> <pre> ~ ! @ # \$ % ^ &amp; * _ - + = `   ( ) { } [ ] : ; &lt; &gt; , . ? / </pre> </li> </ul> |

#### Zugehörige Tasks:

Sichere Kommunikation konfigurieren

Kennwort für die Truststore-Datei des Operations Center zurücksetzen

## Operations Center installieren

Sie können das Operations Center mit jeder der folgenden Methoden installieren: grafischer Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

### Vorbereitende Schritte

Sie können das Operations Center erst konfigurieren, nachdem Sie den IBM Spectrum Protect-Server installiert, konfiguriert und gestartet haben. Daher installieren Sie vor der Installation des Operations Center das entsprechende Serverpaket gemäß den in den Voraussetzungen für Hub- und Peripherieserver aufgeführten Voraussetzungen bezüglich der Serverversion.

Sie können das Operations Center auf demselben Computer wie den IBM Spectrum Protect-Server oder auf einem separaten Computer installieren.

- Operations Center-Installationspaket abrufen  
Das Installationspaket kann von einer IBM® Download-Site heruntergeladen werden, z. B. IBM Passport Advantage oder IBM Fix Central.
- Operations Center mit einem grafisch orientierten Assistenten installieren  
Sie können das Operations Center mithilfe des grafisch orientierten Assistenten von IBM Installation Manager installieren oder aktualisieren.
- Operations Center im Konsolenmodus installieren  
Sie können das Operations Center mithilfe der Befehlszeile im Konsolenmodus installieren oder aktualisieren.
- Operations Center im unbeaufsichtigten Modus installieren  
Sie können das Operations Center im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlermeldungen in Protokolldateien gespeichert.

## Operations Center-Installationspaket abrufen

Das Installationspaket kann von einer IBM® Download-Site heruntergeladen werden, z. B. IBM Passport Advantage oder IBM Fix Central.



## Informationen zu diesem Vorgang


---

Nachdem Sie das Paket von einer IBM Download-Site abgerufen haben, müssen Sie die Installationsdateien extrahieren.

## Vorgehensweise

---

Gehen Sie wie folgt vor, um die Installationsdateien für das Operations Center zu extrahieren. In den folgenden Schritten müssen Sie *Versionsnummer* durch die zu installierende Version des Operations Center ersetzen.

 AIX-Betriebssysteme Auf AIX-Systemen:

- a. Laden Sie die folgende Paketdatei in ein beliebiges Verzeichnis herunter:

```
Versionsnummer.000  
-IBM-SPOC-AIX.bin
```


- b. Stellen Sie sicher, dass Sie über die Ausführberechtigung für die Paketdatei verfügen.  
Bei Bedarf können Sie die Dateiberechtigungen mit dem folgenden Befehl ändern:

```
chmod a+x Versionsnummer.000-IBM-SPOC-AIX.bin
```

- c. Geben Sie den folgenden Befehl aus, um die Installationsdateien zu extrahieren:

```
./Versionsnummer.000-IBM-SPOC-AIX.bin
```

Die sich selbst entpackende Paketdatei wird in das Verzeichnis extrahiert.

 Linux-Betriebssysteme Auf Linux-Systemen:

- a. Laden Sie eine der folgenden Paketdateien in ein beliebiges Verzeichnis herunter:

- *Versionsnummer.000-IBM-SPOC-LinuxS390.bin*
- *Versionsnummer.000-IBM-SPOC-Linuxx86\_64.bin*


- b. Stellen Sie sicher, dass Sie über die Ausführberechtigung für die Paketdatei verfügen.  
Bei Bedarf können Sie die Dateiberechtigungen mit dem folgenden Befehl ändern:

```
chmod a+x Paketname.bin
```

- c. Geben Sie den folgenden Befehl aus, um die Installationsdateien zu extrahieren:

```
./Paketname.bin
```

Die sich selbst entpackende Paketdatei wird in das Verzeichnis extrahiert.

 Windows-Betriebssysteme Auf Windows-Systemen:

- a. Laden Sie die folgende Paketdatei in ein beliebiges Verzeichnis herunter:

```
Versionsnummer.000-IBM-SPOC-WindowsX64.exe
```

- b. Klicken Sie im Windows Explorer doppelt auf den Dateinamen, um die Installationsdateien zu extrahieren.

Die sich selbst entpackende Paketdatei wird in das Verzeichnis extrahiert.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Operations Center mit einem grafisch orientierten Assistenten installieren

---

Sie können das Operations Center mithilfe des grafisch orientierten Assistenten von IBM® Installation Manager installieren oder aktualisieren.

 AIX-Betriebssysteme

## Vorbereitende Schritte

---

Wenn die folgenden RPM-Dateien auf dem Computer nicht installiert sind, installieren Sie sie. Anweisungen siehe RPM-Dateien für den grafisch orientierten Assistenten installieren.

- atk-1.12.3-2.aix5.2.ppc.rpm
- cairo-1.8.8-1.aix5.2.ppc.rpm
- expat-2.0.1-1.aix5.2.ppc.rpm
- fontconfig-2.4.2-1.aix5.2.ppc.rpm

- freetype2-2.3.9-1.aix5.2.ppc.rpm
- gettext-0.10.40-6.aix5.1.ppc.rpm
- glib2-2.12.4-2.aix5.2.ppc.rpm
- gtk2-2.10.6-4.aix5.2.ppc.rpm
- libjpeg-6b-6.aix5.1.ppc.rpm
- libpng-1.2.32-2.aix5.2.ppc.rpm
- libtiff-3.8.2-1.aix5.2.ppc.rpm
- pango-1.14.5-4.aix5.2.ppc.rpm
- pixman-0.12.0-3.aix5.2.ppc.rpm
- xcursor-1.1.7-3.aix5.2.ppc.rpm
- xft-2.1.6-5.aix5.1.ppc.rpm
- xrender-0.9.1-3.aix5.2.ppc.rpm
- zlib-1.2.3-3.aix5.1.ppc.rpm

## Vorgehensweise

---

1. Geben Sie in dem Verzeichnis, in dem die Operations Center-Installationspaketdatei extrahiert wurde, den folgenden Befehl aus:
  - Linux-Betriebssysteme./install.sh
  - install.bat
2. Führen Sie die Installation der IBM Installation Manager- und Operations Center-Pakete gemäß den Anweisungen des Assistenten aus.
 

Wenn Ihre Ländereinstellung die UTF-8-Codierung verwendet, kann die folgende Nachricht angezeigt werden und der Installationsassistent kann langsam sein:

Schriftartgruppe kann nicht erstellt werden

Wird diese Nachricht angezeigt, führen Sie einen der folgenden Schritte aus:

- Ersetzen Sie die Ländereinstellung durch eine, die keine UTF-8-Codierung verwendet. Informationen zu Sprachoptionswerten, die keine UTF-8-Codierung verwenden, finden Sie in Voraussetzungen für die Sprache.
- Installieren Sie das Operations Center mithilfe der Befehlszeile im Konsolenmodus.
- Installieren Sie das Operations Center im unbeaufsichtigten Modus.

## Nächste Schritte

---

Siehe Operations Center konfigurieren.

- RPM-Dateien für den grafisch orientierten Assistenten installieren  
Bevor Sie das Operations Center mit dem grafisch orientierten Assistenten von IBM Installation Manager installieren können, müssen bestimmte RPM-Dateien installiert werden.

Linux-Betriebssysteme

## Operations Center im Konsolenmodus installieren

---

Sie können das Operations Center mithilfe der Befehlszeile im Konsolenmodus installieren oder aktualisieren.

### Vorgehensweise

---

1. Führen Sie in dem Verzeichnis, in dem die Installationspaketdatei extrahiert wurde, das folgende Programm aus:

Linux-Betriebssysteme

./install.sh -c

install.bat -c

2. Befolgen Sie die an der Konsole angezeigten Anweisungen, um die Pakete für Installation Manager und das Operations Center zu installieren.

### Nächste Schritte

---

Siehe Operations Center konfigurieren.

Linux-Betriebssysteme

## Operations Center im unbeaufsichtigten Modus installieren

---

Sie können das Operations Center im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlermeldungen in Protokolldateien gespeichert.

### Vorbereitende Schritte

---

Für die Dateneingabe bei Verwendung der unbeaufsichtigten Installation können Sie eine Antwortdatei verwenden. Die folgenden Musterantwortdateien stehen im Verzeichnis `input` zur Verfügung, in dem das Installationspaket extrahiert wird:

`install_response_sample.xml`

Verwenden Sie diese Datei für die Installation des Operations Center.

`update_response_sample.xml`

Verwenden Sie diese Datei für das Upgrade des Operations Center.

Diese Dateien enthalten Standardwerte, die dazu beitragen können, unnötige Warnungen zu vermeiden. Befolgen Sie die in den Dateien enthaltenen Anweisungen zur Verwendung dieser Dateien.

Wenn Sie eine Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

### Vorgehensweise

---

1. Erstellen Sie eine Antwortdatei. Sie können die Musterantwortdatei ändern oder eine eigene Datei erstellen.  
Tipp: Zum Generieren einer Antwortdatei im Rahmen einer Installation im Konsolenmodus wählen Sie die Installationsoptionen im Konsolenmodus aus. Dann geben Sie in der Anzeige Zusammenfassung `G` ein, um die Antwortdatei entsprechend den zuvor ausgewählten Optionen zu generieren.



2. Erstellen Sie in der Antwortdatei ein Kennwort für den Truststore des Operations Center.  
Wenn Sie die Datei `install_response_sample.xml` verwenden, fügen Sie das Kennwort in die folgende Zeile der Datei ein. Hierbei ist `mein_Kennwort` das Kennwort:

```
<variable name='ssl.password' value='mein_Kennwort' />
```


Weitere Informationen zu diesem Kennwort finden Sie in Prüfliste für die Installation.

Tipp: Das Truststore-Kennwort ist nicht erforderlich, wenn Sie das Operations Center mit der Datei `update_response_sample.xml` aktualisieren.

3. Geben Sie den folgenden Befehl in dem Verzeichnis, in dem das Installationspaket extrahiert wurde, aus, um die unbeaufsichtigte Installation zu starten. Der Wert *Antwortdatei* gibt den Pfad und den Namen der Antwortdatei an.

- o    

```
./install.sh -s -input Antwortdatei -acceptLicense
```

- o   

```
install.bat -s -input Antwortdatei -acceptLicense
```

### Nächste Schritte

---

Siehe Operations Center konfigurieren.

## Upgrade des Operations Center

---

Sie können ein Upgrade des Operations Center mit jeder der folgenden Methoden durchführen: grafisch orientierter Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

### Vorbereitende Schritte

---

Bevor Sie ein Upgrade des Operations Center durchführen, lesen Sie die Informationen zu den Systemvoraussetzungen und die Prüfliste für die Installation. Die Voraussetzungen und Anforderungen der neuen Version des Operations Center können von denen der momentan verwendeten Version abweichen.

### Informationen zu diesem Vorgang

---

Die Anweisungen für das Upgrade des Operations Center sind mit Ausnahme der folgenden Punkte mit den Anweisungen für die Installation des Operations Center identisch:

- Sie verwenden nicht die Funktion Installieren von IBM® Installation Manager, sondern die Funktion Aktualisieren.  
Tipp: In IBM Installation Manager bedeutet *aktualisieren* das Erkennen und Installieren von Aktualisierungen und Fixes für installierte Softwarepakete. In diesem Kontext sind *Aktualisierung* und *Upgrade* gleichbedeutend.
- Wenn Sie ein Upgrade des Operations Center im unbeaufsichtigten Modus durchführen, können Sie den Schritt für die Erstellung eines Kennworts für die Truststore-Datei überspringen.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Erste Schritte mit dem Operations Center

Bevor Sie das Operations Center für die Verwaltung Ihrer Speicherumgebung verwenden können, müssen Sie es konfigurieren.

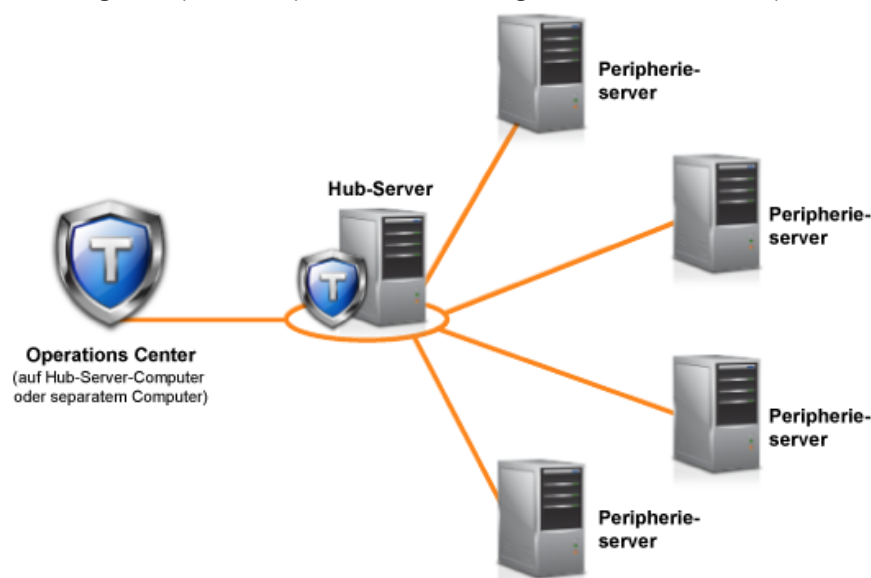
### Informationen zu diesem Vorgang

Führen Sie nach der Installation des Operations Center die folgenden Basiskonfigurationsschritte aus:

1. Legen Sie den Hub-Server fest.
2. Fügen Sie alle Peripherieserver hinzu.
3. Konfigurieren Sie wahlweise E-Mail-Alerts auf den Hub- und Peripherieservern.

Abbildung 1 veranschaulicht eine Operations Center-Konfiguration.

Abbildung 1. Beispiel einer Operations Center-Konfiguration mit Hub- und Peripherieservern



- Operations Center konfigurieren  
Wenn Sie das Operations Center zum ersten Mal öffnen, müssen Sie es für die Verwaltung Ihrer Speicherumgebung konfigurieren. Sie müssen das Operations Center dem IBM Spectrum Protect-Server zuordnen, der als Hub-Server festgelegt ist. Anschließend können Sie weitere IBM Spectrum Protect-Server als Peripherieserver verbinden.
- Sichere Kommunikation konfigurieren  
Das Operations Center verwendet HTTPS (Hypertext Transfer Protocol Secure) für die Kommunikation mit Web-Browsern. Das TLS-Protokoll schützt die Kommunikation zwischen dem Operations Center und dem Hub-Server sowie zwischen dem Hub-Server und den zugeordneten Peripherieservern (TLS = Transport Layer Security).
- Web-Server starten und stoppen  
Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Das Stoppen und Starten des Web-Servers kann z. B. für Konfigurationsänderungen erforderlich sein.
- Operations Center öffnen  
Die Seite 'Übersicht' ist die Standardeingangsansicht im Operations Center. In Ihrem Web-Browser können Sie jedoch für die Seite, die bei der Anmeldung beim Operations Center geöffnet werden soll, ein Lesezeichen setzen.
- Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen  
Der Clientverwaltungsservice erfasst Diagnoseinformationen über Clients für Sichern/Archivieren und stellt diese Informationen dem Operations Center für Basisüberwachungsfunktionen zur Verfügung.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

# Operations Center konfigurieren

---

Wenn Sie das Operations Center zum ersten Mal öffnen, müssen Sie es für die Verwaltung Ihrer Speicherumgebung konfigurieren. Sie müssen das Operations Center dem IBM Spectrum Protect-Server zuordnen, der als Hub-Server festgelegt ist. Anschließend können Sie weitere IBM Spectrum Protect-Server als Peripherieserver verbinden.

- Hub-Server festlegen  
Wenn Sie zum ersten Mal eine Verbindung zum Operations Center herstellen, müssen Sie angeben, welcher IBM Spectrum Protect-Server der Hub-Server ist.
- Peripherieserver hinzufügen  
Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server mindestens einen Peripherieserver hinzufügen.
- E-Mail-Alerts an Administratoren senden  
Ein Alert ist eine Benachrichtigung über ein relevantes Problem auf dem IBM Spectrum Protect-Server und wird durch eine Servernachricht ausgelöst. Alerts können im Operations Center angezeigt und vom Server per E-Mail an Administratoren gesendet werden.
- Angepassten Text in die Anmeldeanzeige einfügen  
Sie können angepassten Text, z. B. die Nutzungsbedingungen Ihres Unternehmens für die Software, zur Anmeldeanzeige des Operations Center hinzufügen, so dass die Benutzer des Operations Center den Text sehen, bevor sie ihren Benutzernamen und ihr Kennwort eingeben.
- REST-Services aktivieren  
Anwendungen, die REST-Services verwenden, können die Speicherumgebung abfragen und verwalten, indem eine Verbindung zum Operations Center hergestellt wird (REST = Representational State Transfer).

## Hub-Server festlegen

---

Wenn Sie zum ersten Mal eine Verbindung zum Operations Center herstellen, müssen Sie angeben, welcher IBM Spectrum Protect-Server der Hub-Server ist.

### Vorbereitende Schritte

---

Für das Operations Center ist die sichere Kommunikation zwischen dem Hub-Server und dem Operations Center erforderlich. Um die Kommunikation zu schützen, müssen Sie das TLS-Zertifikat des Hub-Servers zur Truststore-Datei des Operations Center hinzufügen (TLS = Transport Layer Security). Weitere Informationen finden Sie in Kommunikation zwischen Operations Center und Hub-Server schützen.

### Vorgehensweise

---

Geben Sie die folgende Adresse in einem Web-Browser an. Dabei steht *Hostname* für den Namen des Computers, auf dem das Operations Center installiert ist, und *sicherer\_Anschluss* für die Anschlussnummer, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet:

```
https://Hostname:sicherer_Anschluss/oc
```

Tipps:

- Bei der URL muss die Groß-/Kleinschreibung beachtet werden. Achten Sie beispielsweise darauf, dass Sie "oc" wie gezeigt in Kleinbuchstaben eingeben.
- Weitere Informationen zu der Anschlussnummer finden Sie in Prüfliste für die Installation.
- Wenn Sie zum ersten Mal eine Verbindung zum Operations Center herstellen, müssen Sie folgende Informationen angeben:
  - Verbindungsdaten für den Server, den Sie als Hub-Server festlegen wollen.
  - Berechtigungsnachweise zur Anmeldung für eine Administrator-ID, die für diesen Server definiert ist.
- Ist der Aufbewahrungszeitraum für Ereignisdatensätze des Servers kürzer als 14 Tage, wird der Zeitraum automatisch auf 14 Tage zurückgesetzt, wenn Sie den Server als Hub-Server konfigurieren.

### Nächste Schritte




---

Wenn Ihre Umgebung mehrere IBM Spectrum Protect-Server umfasst, fügen Sie die übrigen Server dem Hub-Server als Peripherieserver hinzu.

Achtung: Nachdem ein Server als Hub- oder Peripherieserver konfiguriert wurde, dürfen Sie seinen Namen nicht mehr ändern.

#### Zugehörige Konzepte:

Voraussetzungen für Hub- und Peripherieserver

Administrator-IDs, die für das Operations Center erforderlich sind  
 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Peripherieserver hinzufügen

---

Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server mindestens einen Peripherieserver hinzufügen.

### Vorbereitende Schritte

---

Die Kommunikation zwischen dem Peripherieserver und dem Hub-Server muss mithilfe des TLS-Protokolls geschützt werden (TLS = Transport Layer Security). Um die Kommunikation zu schützen, müssen Sie das Zertifikat des Peripherieservers zur Truststore-Datei des Hub-Servers hinzufügen.

### Vorgehensweise

---




1. Klicken Sie in der Menüleiste des Operations Center auf Server. Die Seite Server wird geöffnet.

In der Tabelle auf der Seite Server kann ein Server den Status "Nicht überwacht" haben. Dieser Status bedeutet, dass dieser Server zwar durch einen Administrator mit dem Befehl DEFINE SERVER für den Hub-Server definiert, aber noch nicht als Peripherieserver konfiguriert wurde.

2. Führen Sie einen der folgenden Schritte aus:
  - Klicken Sie auf den Server, um ihn hervorzuheben, und klicken Sie in der Menüleiste der Tabelle auf Peripherieserver überwachen.
  - Wenn der Server, den Sie hinzufügen möchten, nicht in der Tabelle angezeigt wird und die sichere Kommunikation über SSL/TSL nicht erforderlich ist, klicken Sie auf + Peripherieserver in der Menüleiste der Tabelle.
3. Stellen Sie die erforderlichen Informationen bereit und führen Sie die Schritte im Konfigurationsassistenten für den Peripherieserver aus.  
Tipp: Ist der Aufbewahrungszeitraum für Ereignisdatensätze des Servers kürzer als 14 Tage, wird der Zeitraum automatisch auf 14 Tage zurückgesetzt, wenn Sie den Server als Peripherieserver konfigurieren.

#### Zugehörige Verweise:

DEFINE SERVER (Server für Übertragung zwischen Servern definieren)

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## E-Mail-Alerts an Administratoren senden

---

Ein Alert ist eine Benachrichtigung über ein relevantes Problem auf dem IBM Spectrum Protect-Server und wird durch eine Servernachricht ausgelöst. Alerts können im Operations Center angezeigt und vom Server per E-Mail an Administratoren gesendet werden.

### Vorbereitende Schritte

---

Bevor Sie die E-Mail-Benachrichtigung für Administratoren wegen Alerts konfigurieren, stellen Sie sicher, dass folgende Anforderungen erfüllt sind:

- Damit Alerts als E-Mail gesendet und empfangen werden können, ist ein SMTP-Server erforderlich und der Server, der die Alerts als E-Mail sendet, muss auf den SMTP-Server zugreifen können.  
Tipp: Wenn das Operations Center auf einem separaten Computer installiert ist, benötigt dieser Computer keinen Zugriff auf den SMTP-Server.
- Ein Administrator benötigt die Systemberechtigung, um die E-Mail-Benachrichtigung konfigurieren zu können.

### Informationen zu diesem Vorgang

---

Eine E-Mail-Benachrichtigung wird nur für das erste Auftreten eines Alerts gesendet. Außerdem wird keine E-Mail-Benachrichtigung für einen Alert gesendet, wenn der Alert vor der Konfiguration der E-Mail-Benachrichtigung generiert wird.

Sie können die E-Mail-Benachrichtigung wie folgt konfigurieren:

- Benachrichtigung für einzelne Alerts senden
- Alertzusammenfassungen senden

Eine Alertzusammenfassung enthält Informationen zu aktuellen Alerts. Die Zusammenfassung beinhaltet die Gesamtzahl der Alerts, die Gesamtzahl der aktiven und inaktiven Alerts, den ältesten Alert, den neuesten Alert und den am häufigsten auftretenden Alert.

Sie können maximal drei Administratoren als Empfänger von Alertzusammenfassungen per E-Mail angeben. Alertzusammenfassungen werden ca. einmal stündlich gesendet.

## Vorgehensweise

---

Gehen Sie auf jedem Hub- und Peripherieserver, von dem Sie E-Mail-Alerts erhalten wollen, wie folgt vor, um die E-Mail-Benachrichtigung für Administratoren wegen Alerts zu konfigurieren:

1. Geben Sie den folgenden Befehl aus, um zu überprüfen, dass die Alertüberwachung aktiviert ist:

```
QUERY MONITORSETTINGS
```

2. Geben Sie den folgenden Befehl aus, wenn die Befehlsausgabe anzeigt, dass die Alertüberwachung inaktiviert ist. Andernfalls fahren Sie mit dem nächsten Schritt fort.

```
SET ALERTMONITOR ON
```

3. Geben Sie den folgenden Befehl aus, um das Senden von E-Mail-Benachrichtigungen zu aktivieren:

```
SET ALERTEMAIL ON
```

4. Geben Sie den folgenden Befehl aus, um den SMTP-Server zu definieren, der zum Senden von E-Mail-Benachrichtigungen verwendet wird:

```
SET ALERTEMAILSMTPHOST Hostname
```

5. Geben Sie den folgenden Befehl aus, um die Anschlussnummer für den SMTP-Server anzugeben:

```
SET ALERTEMAILSMTPPORT Anschlussnummer
```

Die Standardanschlussnummer ist 25.

6. Geben Sie den folgenden Befehl aus, um die E-Mail-Adresse des Absenders der Alerts anzugeben:

```
SET ALERTEMAILFROMADDR E-Mail-Adresse
```

7. Geben Sie für jede Administrator-ID, die E-Mail-Benachrichtigungen empfangen soll, einen der folgenden Befehle aus, um die E-Mail-Benachrichtigung zu aktivieren und um die E-Mail-Adresse anzugeben:

```
REGISTER ADMIN Administratorname ALERT=YES EMAILADDRESS=E-Mail-Adresse
```

```
UPDATE ADMIN Administratorname ALERT=YES EMAILADDRESS=E-Mail-Adresse
```

8. Wählen Sie eine oder beide der folgenden Optionen aus und geben Sie die Administrator-IDs an, die E-Mail-Benachrichtigungen empfangen sollen:

- o Benachrichtigung für einzelne Alerts senden

Geben Sie einen der folgenden Befehle aus, um die Administrator-IDs anzugeben bzw. zu aktualisieren, die E-Mail-Benachrichtigungen für einen einzelnen Alert empfangen sollen:

```
DEFINE ALERTTRIGGER Nachrichtenummer Admin=Administratorname1,Administratorname2
```

```
UPDATE ALERTTRIGGER Nachrichtenummer ADDAdmin=Administratorname3 DELAdmin=Administratorname1
```

Tipp: Auf der Seite Alerts konfigurieren des Operations Center können Sie die Administratoren auswählen, die E-Mail-Benachrichtigungen erhalten sollen.

- o Alertzusammenfassungen senden

Geben Sie den folgenden Befehl aus, um die Administrator-IDs anzugeben bzw. zu aktualisieren, die Alertzusammenfassungen per E-Mail erhalten sollen:

```
SET ALERTSUMMARYTOADMINS Administratorname1,Administratorname2,Administratorname3
```

Gehen Sie wie folgt vor, wenn Sie Alertzusammenfassungen, aber keine Benachrichtigungen über einzelne Alerts empfangen wollen:

- a. Setzen Sie die Benachrichtigung über einzelne Alerts wie in E-Mail-Alerts vorübergehend aussetzen beschrieben aus.
- b. Stellen Sie sicher, dass die betreffende Administrator-ID in dem folgenden Befehl aufgelistet ist:

```
SET ALERTSUMMARYTOADMINS Administratorname1,Administratorname2,Administratorname3
```

## E-Mail-Alerts an mehrere Administratoren senden

---

Das folgende Beispiel zeigt die Befehle, mit denen alle Alerts für Nachricht ANR1075E in einer E-Mail an die Administratoren myadmin, djadmin und csadmin gesendet werden:


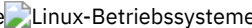

```

SET ALERTMONITOR ON
SET ALERTEMAIL ON
SET ALERTEMAILSMTPHOST mymailserver.domain.com
SET ALERTEMAILSMTPPORT 450
SET ALERTEMAILFROMADDR srvadmin@mydomain.com
UPDATE ADMIN myadmin ALERT=YES EMAILADDRESS=myaddr@anycompany.com
UPDATE ADMIN djadmin ALERT=YES EMAILADDRESS=djaddr@anycompany.com
UPDATE ADMIN csadmin ALERT=YES EMAILADDRESS=csaddr@anycompany.com
DEFINE ALERTTRIGGER anr0175e ADMIN=myadmin,djadmin,csadmin

```

- E-Mail-Alerts vorübergehend aussetzen  
E-Mail-Alerts können vorübergehend ausgesetzt werden, wenn bestimmte Situationen dies erforderlich machen. Sie möchten z. B. Alertzusammenfassungen erhalten, aber die Benachrichtigung über einzelne Alerts aussetzen oder Sie möchten die E-Mail-Benachrichtigung aussetzen, wenn ein Administrator im Urlaub ist.

#### Zugehörige Verweise:

DEFINE ALERTTRIGGER (Alertauslöser definieren)  
 QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)  
 REGISTER ADMIN (Administrator-ID registrieren)  
 SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren)  
 SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)  
 SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)  
 SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)  
 SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)  
 SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren)  
 UPDATE ADMIN (Administrator aktualisieren)  
 UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)  
  




## Angepassten Text in die Anmeldeanzeige einfügen

Sie können angepassten Text, z. B. die Nutzungsbedingungen Ihres Unternehmens für die Software, zur Anmeldeanzeige des Operations Center hinzufügen, so dass die Benutzer des Operations Center den Text sehen, bevor sie ihren Benutzernamen und ihr Kennwort eingeben.

### Vorgehensweise

Gehen Sie wie folgt vor, um angepassten Text zur Anmeldeanzeige hinzuzufügen:

1. Wechseln Sie auf dem Computer, auf dem das Operations Center installiert ist, in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):

  *Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer  
 *Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer

2. Erstellen Sie in dem Verzeichnis eine Datei mit dem Namen loginText.html, die den Text enthält, den Sie zur Anmeldeanzeige hinzufügen wollen. Text mit Sonderzeichen, die keine ASCII-Zeichen sind, muss UTF-8-codiert sein.  
Tipp: Sie können den Text mit HTML-Tags formatieren.
3. Überprüfen Sie den hinzugefügten Text in der Anmeldeanzeige des Operations Center.  
Geben Sie die folgende Adresse in einem Web-Browser an, um das Operations Center zu öffnen. Dabei steht *Hostname* für den Namen des Computers, auf dem das Operations Center installiert ist, und *sicherer\_Anschluss* für die Anschlussnummer, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet:

`https://Hostname:sicherer_Anschluss/oc`

## REST-Services aktivieren

Anwendungen, die REST-Services verwenden, können die Speicherumgebung abfragen und verwalten, indem eine Verbindung zum Operations Center hergestellt wird (REST = Representational State Transfer).

### Informationen zu diesem Vorgang

Aktivieren Sie dieses Feature, um REST-Services eine Interaktion mit Hub- und Peripherieservern zu ermöglichen. Dabei werden Aufrufe an die folgende Adresse gesendet:

`https://OC-Hostname:Anschluss/oc/api`




Hierbei steht *OC-Hostname* für den Netznamen oder die IP-Adresse des Hostsystems des Operations Center und *Anschluss* für die Anschlussnummer des Operations Center. Die Standardanschlussnummer ist 11090.

Informationen zu den für das Operations Center verfügbaren REST-Services finden Sie in Technote <http://www.ibm.com/support/docview.wss?uid=swg21973011> oder geben Sie den folgenden REST-Aufruf aus:

`https://OC-Hostname:Anschluss/oc/api/help`

## Vorgehensweise

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für die Einstellungen  und klicken Sie auf Einstellungen.
2. Wählen Sie auf der Seite 'Allgemein' das Kontrollkästchen Verwaltungs-REST-API aktivieren aus.
3. Klicken Sie auf Speichern.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Sichere Kommunikation konfigurieren

Das Operations Center verwendet HTTPS (Hypertext Transfer Protocol Secure) für die Kommunikation mit Web-Browsern. Das TLS-Protokoll schützt die Kommunikation zwischen dem Operations Center und dem Hub-Server sowie zwischen dem Hub-Server und den zugeordneten Peripherieservern (TLS = Transport Layer Security).

### Informationen zu diesem Vorgang

TLS 1.2 ist für die sichere Kommunikation zwischen dem IBM Spectrum Protect-Server und dem Operations Center sowie zwischen dem Hub-Server und den Peripherieservern erforderlich.

- Kommunikation zwischen Operations Center und Hub-Server schützen  
Um die Kommunikation zwischen dem Operations Center und dem Hub-Server zu schützen, müssen Sie das TLS-Zertifikat (Transport Layer Security) des Hub-Servers der Truststore-Datei des Operations Center hinzufügen.
- Kommunikation zwischen Hub-Server und Peripherieservern schützen  
Sie müssen das Zertifikat des Peripherieservers im Hub-Server und das Zertifikat des Hub-Servers im Peripherieserver definieren, um die Kommunikation zwischen dem Hub-Server und einem Peripherieserver mithilfe des TLS-Protokolls zu schützen (TLS = Transport Layer Security). Außerdem müssen Sie im Operations Center die Überwachung des Peripherieservers konfigurieren.
- Kennwort für die Truststore-Datei des Operations Center zurücksetzen  
Um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server einrichten zu können, müssen Sie das Kennwort für die Truststore-Datei des Operations Center kennen. Sie erstellen dieses Kennwort während der Installation des Operations Center. Wenn Sie das Kennwort nicht kennen, können Sie es zurücksetzen.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Kommunikation zwischen Operations Center und Hub-Server schützen

Um die Kommunikation zwischen dem Operations Center und dem Hub-Server zu schützen, müssen Sie das TLS-Zertifikat (Transport Layer Security) des Hub-Servers der Truststore-Datei des Operations Center hinzufügen.

### Vorbereitende Schritte

Die Truststore-Datei des Operations Center ist ein Container für Zertifikate, auf den das Operations Center zugreifen kann. Die Truststore-Datei enthält das Zertifikat, das das Operations Center für die HTTPS-Kommunikation mit Web-Browsern verwendet.

Während der Installation des Operations Center erstellen Sie ein Kennwort für die Truststore-Datei. Um die Kommunikation zwischen dem Operations Center und dem Hub-Server zu schützen, müssen Sie dasselbe Kennwort verwenden, um das Zertifikat des Hub-Servers der Truststore-Datei hinzuzufügen. Wenn Sie dieses Kennwort vergessen haben, können Sie es zurücksetzen. Siehe Kennwort für die Truststore-Datei des Operations Center zurücksetzen.

## Vorgehensweise

1. Geben Sie das Zertifikat `cert256.arm` als Standardzertifikat in der Schlüsseldatenbankdatei des Hub-Servers an.

Gehen Sie wie folgt vor, um `cert256.arm` als Standardzertifikat anzugeben:

- a. Geben Sie den folgenden Befehl im Verzeichnis der Hub-Server-Instanz aus:


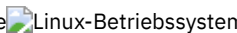
```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
-label "TSM Server SelfSigned SHA Key"
```


- b. Starten Sie den Hub-Server erneut, damit er die Änderungen der Schlüsseldatenbankdatei übernehmen kann.
2. Geben Sie den folgenden Befehl aus, um zu überprüfen, ob das Zertifikat cert256.arm als Standardzertifikat in der Schlüsseldatenbankdatei des Hub-Servers definiert ist:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

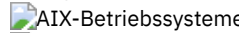
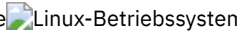
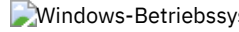
3. Stoppen Sie den Web-Server des Operations Center.
4. Rufen Sie die Befehlszeile des Betriebssystems auf, auf dem das Operations Center installiert ist.
5. Verwenden Sie das Dienstprogramm iKeycmd oder iKeyman, um das Zertifikat der Truststore-Datei des Operations Center hinzuzufügen.

Das Dienstprogramm iKeycmd ist eine Befehlszeilenschnittstelle und das Dienstprogramm iKeyman ist die grafische Benutzerschnittstelle von IBM® Key Management.

  Die Dienstprogramme iKeycmd und iKeyman müssen als Rootbenutzer ausgeführt werden.

 Die Dienstprogramme iKeycmd und iKeyman müssen von einem Administratorkonto ausgeführt werden.

Gehen Sie wie folgt vor, um das TLS-Zertifikat mithilfe der Befehlszeilenschnittstelle hinzuzufügen:

- a. Wechseln Sie in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):
  -   *Installationsverzeichnis*/ui/jre/bin
  -  *Installationsverzeichnis*\ui\jre\bin
- b. Geben Sie den Befehl iKeycmd aus, um das Zertifikat cert256.arm als Standardzertifikat in der Schlüsseldatenbankdatei des Hub-Servers hinzuzufügen:

```
ikeycmd -cert -add
-db /Installationsverzeichnis/Liberty/usr/servers/guiServer/gui-truststore.jks
-file /fvt/comfrey/srv/cert256.arm
-label 'Kennsatzbeschreibung'
-pw 'Kennwort' -type jks -format ascii -trust enable
```

Hierbei gilt Folgendes:

**Installationsverzeichnis**

Das Verzeichnis, in dem das Operations Center installiert ist.



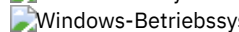
**Kennsatzbeschreibung**

Die Beschreibung, die Sie dem Kennsatz zuordnen.

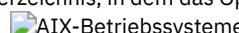
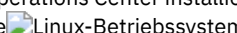
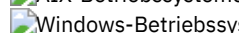
**Kennwort**

Das Kennwort, das Sie bei der Installation des Operations Center erstellt haben. Wenn Sie das Kennwort zurücksetzen wollen, deinstallieren Sie das Operations Center, löschen Sie die Datei .jks und installieren Sie das Operations Center erneut.



Gehen Sie wie folgt vor, um das Zertifikat mithilfe des Fensters 'IBM Key Management' hinzuzufügen:

- a. Wechseln Sie in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):
  -   *Installationsverzeichnis*/ui/jre/bin
  -  *Installationsverzeichnis*\ui\jre\bin
- b. Geben Sie den folgenden Befehl aus, um das Fenster IBM Key Management zu öffnen:

```
ikeyman
```

- c. Klicken Sie auf Schlüsseldatenbankdatei > Öffnen.
- d. Klicken Sie im Fenster Öffnen auf Durchsuchen und wechseln Sie in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):
  -   *Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer
  -  *Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer
- e. Wählen Sie im Verzeichnis guiServer die Datei gui-truststore.jks aus.
- f. Klicken Sie auf Öffnen und dann auf OK.
- g. Geben Sie das Kennwort für die Truststore-Datei ein und klicken Sie auf OK.
- h. Klicken Sie im Bereich Schlüsseldatenbankinhalt des Fensters IBM Key Management auf den Pfeil und wählen Sie Zertifikate des Unterzeichners in der Liste aus.
- i. Klicken Sie auf Hinzufügen.



j. Klicken Sie im Fenster Öffnen auf Durchsuchen und wechseln Sie in das Verzeichnis der Hub-Server-Instanz (siehe das folgende Beispiel).

-  Linux-Betriebssysteme/opt/tivoli/tsm/server/bin
-  c:\Programme\Tivoli\TSM\server1

Das Verzeichnis enthält das Zertifikat cert256.arm.

Wenn Sie im Fenster Öffnen nicht auf das Verzeichnis der Hub-Server-Instanz zugreifen können, gehen Sie wie folgt vor:

i. Kopieren Sie die Datei cert256.arm mithilfe von FTP oder einer anderen Dateiübertragungsmethode vom Hub-Server in das folgende Verzeichnis auf dem Computer, auf dem das Operations Center installiert ist:

-  Linux-BetriebssystemeInstallationsverzeichnis/ui/Liberty/usr/servers/guiServer
-  Installationsverzeichnis\ui\Liberty\usr\servers\guiServer

ii. Wechseln Sie im Fenster Öffnen in das Verzeichnis guiServer.

k. Wählen Sie das Zertifikat cert256.arm aus.

Tipp: Das von Ihnen ausgewählte Zertifikat muss als Standardzertifikat in der Schlüsseldatenbankdatei des Hub-Servers definiert sein. Weitere Informationen finden Sie unter Schritt 1 und 2.

l. Klicken Sie auf Öffnen und dann auf OK.

m. Geben Sie eine Bezeichnung für das Zertifikat ein. Geben Sie beispielsweise den Namen des Hub-Servers ein.



n. Klicken Sie auf OK. Das SSL-Zertifikat des Hub-Servers wird der Truststore-Datei hinzugefügt und die Bezeichnung im Bereich Schlüsseldatenbankinhalt des Fensters IBM Key Management angezeigt.

o. Schließen Sie das Fenster IBM Key Management.

6. Starten Sie den Web-Server des Operations Center.

7. Wenn Sie zum ersten Mal eine Verbindung zum Operations Center herstellen, müssen Sie die IP-Adresse oder den Netznamen des Hub-Servers und die Anschlussnummer für die Kommunikation mit dem Hub-Server angeben. Ist die Serveroption ADMINONCLIENTPORT für den IBM Spectrum Protect-Server aktiviert, geben Sie die durch die Serveroption TCPADMINPORT angegebene Anschlussnummer ein. Ist die Serveroption ADMINONCLIENTPORT nicht aktiviert, geben Sie die durch die Serveroption TCPPORT angegebene Anschlussnummer ein.

Wenn das Operations Center bereits konfiguriert wurde, können Sie den Inhalt der Datei serverConnection.properties überprüfen, um die Verbindungsdaten zu verifizieren. Die Datei serverConnection.properties befindet sich in dem folgenden Verzeichnis auf dem Computer, auf dem das Operations Center installiert ist:

-  Linux-BetriebssystemeInstallationsverzeichnis/ui/Liberty/usr/servers/guiServer
-  Installationsverzeichnis\ui\Liberty\usr\servers\guiServer




## Nächste Schritte

---

Informationen zur Konfiguration der TLS-Kommunikation zwischen dem Hub-Server und einem Peripherieserver finden Sie in Kommunikation zwischen Hub-Server und Peripherieserver schützen.

### Zugehörige Verweise:

QUERY OPTION (Serveroptionen abfragen)

## Kommunikation zwischen Hub-Server und Peripherieserver schützen

---

Sie müssen das Zertifikat des Peripherieservers im Hub-Server und das Zertifikat des Hub-Servers im Peripherieserver definieren, um die Kommunikation zwischen dem Hub-Server und einem Peripherieserver mithilfe des TLS-Protokolls zu schützen (TLS = Transport Layer Security). Außerdem müssen Sie im Operations Center die Überwachung des Peripherieservers konfigurieren.

## Informationen zu diesem Vorgang

---

Der Hub-Server empfängt Status- und Alertinformationen vom Peripherieserver und zeigt diese Informationen im Operations Center an. Damit die Status- und Alertinformationen vom Peripherieserver empfangen werden können, muss das Zertifikat des Peripherieservers zur Truststore-Datei des Hub-Servers hinzugefügt werden. Außerdem müssen Sie im Operations Center die Überwachung des Peripherieservers konfigurieren.

Damit andere Funktionen des Operations Center aktiviert werden, z. B. die automatische Implementierung von Clientaktualisierungen, muss das Zertifikat des Hub-Servers zur Truststore-Datei des Peripherieservers hinzugefügt werden.

## Vorgehensweise

---

1. Führen Sie die folgenden Schritte aus, um das Zertifikat des Peripherieservers im Hub-Server zu definieren:

a. Wechseln Sie auf dem Peripherieserver in das Verzeichnis der Peripherieserverinstanz.

b. Geben Sie das erforderliche Zertifikat cert256.arm als Standardzertifikat in der Schlüsseldatenbankdatei des Peripherieservers an. Geben Sie den folgenden Befehl aus:

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
-label "TSM Server SelfSigned SHA Key"
```

- c. Überprüfen Sie die Zertifikate in der Schlüsseldatenbankdatei des Peripherieservers. Geben Sie den folgenden Befehl aus:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

- d. Übertragen Sie die Datei cert256.arm des Peripherieservers sicher an den Hub-Server.  
e. Wechseln Sie auf dem Hub-Server in das Verzeichnis der Hub-Server-Instanz.  
f. Definieren Sie das Zertifikat des Peripherieservers im Hub-Server. Geben Sie den folgenden Befehl im Verzeichnis der Hub-Server-Instanz aus. Hierbei steht *Peripherieservername* für den Namen des Peripherieservers und *Peripherie\_cert256.arm* für den Dateinamen des Zertifikats des Peripherieservers.

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
-label Peripherieservername -file Peripherie_cert256.arm
```

2. Führen Sie die folgenden Schritte aus, um das Zertifikat des Hub-Servers im Peripherieserver zu definieren:

- a. Wechseln Sie auf dem Hub-Server in das Verzeichnis der Hub-Server-Instanz.  
b. Geben Sie das erforderliche Zertifikat cert256.arm als Standardzertifikat in der Schlüsseldatenbankdatei des Hub-Servers an. Geben Sie den folgenden Befehl aus:

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
-label "TSM Server SelfSigned SHA Key"
```

- c. Überprüfen Sie die Zertifikate in der Schlüsseldatenbankdatei des Peripherieservers. Geben Sie den folgenden Befehl aus:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

- d. Übertragen Sie die Datei cert256.arm des Hub-Servers sicher an den Peripherieserver.  
e. Wechseln Sie auf dem Peripherieserver in das Verzeichnis der Peripherieserverinstanz.  
f. Definieren Sie das Zertifikat des Hub-Servers im Peripherieserver. Geben Sie den folgenden Befehl im Verzeichnis der Peripherieserverinstanz aus. Hierbei steht *Name\_des\_Hub-Servers* für den Namen des Hub-Servers und *Hub\_cert256.arm* für den Dateinamen des Zertifikats des Hub-Servers.

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
-label Name_des_Hub-Servers -file Hub_cert256.arm
```

3. Starten Sie den Hub-Server und den Peripherieserver neu.

4. Führen Sie die folgenden Schritte aus, um den Peripherieserver im Hub-Server und den Hub-Server im Peripherieserver zu definieren.

- a. Geben Sie die folgenden Befehle sowohl auf dem Hub-Server als auch auf dem Peripherieserver aus:

```
SET SERVERPASSWORD Serverkennwort
SET SERVERHLADDRESS IP-Adresse
SET SERVERLLADDRESS TCP-Port
```

- b. Geben Sie auf dem Hub-Server den Befehl DEFINE SERVER gemäß dem folgenden Beispiel aus:

```
DEFINE SERVER Peripherieservername HLA=Peripherieserveradresse
LLA=spoke_SSLTCPADMINPort SERVERPA=Peripherieserverkennwort
```

- c. Geben Sie auf dem Peripherieserver den Befehl DEFINE SERVER gemäß dem folgenden Beispiel aus:

```
DEFINE SERVER Name_des_Hub-Servers HLA=Hub-Server-Adresse
LLA=hub_SSLTCPADMINPort SERVERPA=Hub-Server-Kennwort
```

Tipp: Außer beim Senden oder Empfangen von Objektdaten durch den Server ist die Serverkommunikation standardmäßig verschlüsselt. Objektdaten werden mithilfe von TCP/IP gesendet und empfangen. Durch die Nichtverschlüsselung von Objektdaten entspricht die Serverleistung in etwa der Kommunikation über eine TCP/IP-Sitzung und die Sitzung ist sicher. Soll die gesamte Kommunikation mit dem angegebenen Server verschlüsselt werden, auch wenn der Server Objektdaten sendet und empfängt, müssen Sie im Befehl DEFINE SERVER den Parameter SSL=YES angeben.




5. Führen Sie die folgenden Schritte aus, um im Operations Center die Überwachung des Peripherieservers konfigurieren:

- a. Klicken Sie in der Menüleiste des Operations Center auf Server. Der Peripherieserver hat den Status "Nicht überwacht". Dieser Status bedeutet, dass dieser Server zwar mit dem Befehl DEFINE SERVER für den Hub-Server definiert, aber noch nicht als Peripherieserver konfiguriert wurde.  
b. Klicken Sie auf den Peripherieserver, um den Eintrag hervorzuheben, und auf Peripherieserver überwachen.

#### Zugehörige Verweise:

DEFINE SERVER (Server für Übertragung zwischen Servern definieren)

QUERY OPTION (Serveroptionen abfragen)

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme



# Kennwort für die Truststore-Datei des Operations Center zurücksetzen

Um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server einrichten zu können, müssen Sie das Kennwort für die Truststore-Datei des Operations Center kennen. Sie erstellen dieses Kennwort während der Installation des Operations Center. Wenn Sie das Kennwort nicht kennen, können Sie es zurücksetzen.

## Informationen zu diesem Vorgang

Um das Kennwort zurückzusetzen, müssen Sie ein neues Kennwort erstellen, die Truststore-Datei des Operations Center löschen und den Web-Server des Operations Center erneut starten.

## Vorgehensweise

1. Stoppen Sie den Web-Server des Operations Center.
2. Wechseln Sie in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):
  - o Linux-Betriebssysteme *Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer
  - o  *Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer
3. Öffnen Sie die Datei `bootstrap.properties`, die das Kennwort für die Truststore-Datei enthält. Wenn das Kennwort nicht verschlüsselt ist, können Sie damit die Truststore-Datei öffnen, ohne es zurücksetzen zu müssen. Die folgenden Beispiele zeigen den Unterschied zwischen einem verschlüsselten und einem nicht verschlüsselten Kennwort:

Beispiel eines verschlüsselten Kennworts

Verschlüsselte Kennwörter beginnen mit der Zeichenfolge `{xor}`.

Das folgende Beispiel zeigt das verschlüsselte Kennwort als Wert des Parameters `tsm.truststore.pswd`:

```
tsm.truststore.pswd={xor}MiYPPiwsKDatOw==
```

Beispiel eines nicht verschlüsselten Kennworts

Das folgende Beispiel zeigt das nicht verschlüsselte Kennwort als Wert des Parameters `tsm.truststore.pswd`:

```
tsm.truststore.pswd=J8b%^B
```

4. Sie setzen das Kennwort zurück, indem Sie das Kennwort in der Datei `bootstrap.properties` durch ein neues Kennwort ersetzen. Sie können das Kennwort durch ein verschlüsseltes Kennwort oder durch ein nicht verschlüsseltes Kennwort ersetzen. Merken Sie sich das nicht verschlüsselte Kennwort für eine spätere Verwendung.

Gehen Sie wie folgt vor, um ein verschlüsseltes Kennwort zu erstellen:



- a. Erstellen Sie ein nicht verschlüsseltes Kennwort.

Das Kennwort für die Truststore-Datei muss die folgenden Kriterien erfüllen:



- Das Kennwort darf mindestens 6 Zeichen und maximal 64 Zeichen enthalten.
- Das Kennwort muss mindestens die folgenden Zeichen enthalten:
  - Einen Großbuchstaben (A – Z)
  - Einen Kleinbuchstaben (a – z)
  - Eine Ziffer (0 – 9)
  - Zwei der nachfolgend aufgelisteten nicht alphanumerischen Zeichen:


```
~ ! @ # $ % ^ & * _ - + = ` |  
( ) { } [ ] : ; < > , . ? /
```

- b. Wechseln Sie über die Befehlszeile des Betriebssystems in das folgende Verzeichnis:

- Linux-Betriebssysteme *Installationsverzeichnis*/ui/Liberty/bin
-  *Installationsverzeichnis*\ui\Liberty\bin

- c. Geben Sie den folgenden Befehl aus, um das Kennwort zu verschlüsseln (*mein\_Kennwort* ist das nicht verschlüsselte Kennwort):

- Linux-Betriebssysteme `securityUtility encode mein_Kennwort`
-  `securityUtility.bat encode mein_Kennwort`

 Die folgende Nachricht könnte angezeigt werden:

```
! Der Befehl "java" ist entweder falsch geschrieben  
oder konnte nicht gefunden werden.
```

Wenn diese Nachricht angezeigt wird, führen Sie folgende Schritte aus:

- i. Geben Sie den folgenden Befehl aus (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):

```
set JAVA_HOME="Installationsverzeichnis\jre"
```

- ii. Geben Sie den folgenden Befehl erneut aus, um das Kennwort zu verschlüsseln:

```
securityUtility.bat encode mein_Kennwort
```

- Schließen Sie die Datei bootstrap.properties.
- Wechseln Sie in das folgende Verzeichnis:
  - Linux-Betriebssysteme `Installationsverzeichnis/ui/Liberty/usr/servers/guiServer`
  - `Installationsverzeichnis\ui\Liberty\usr\servers\guiServer`
- Löschen Sie die Truststore-Datei gui-truststore.jks des Operations Center.
- Starten Sie den Web-Server des Operations Center.

## Ergebnisse

---

Eine neue Truststore-Datei wird automatisch für das Operations Center erstellt und das TLS-Zertifikat des Operations Center wird automatisch in die Truststore-Datei eingefügt.

## Web-Server starten und stoppen

---

Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Das Stoppen und Starten des Web-Servers kann z. B. für Konfigurationsänderungen erforderlich sein.

## Vorgehensweise

---

Stoppen Sie den Web-Server und starten Sie ihn erneut.

- Geben Sie im Verzeichnis `/Installationsverzeichnis/ui/utills` die folgenden Befehle aus (`Installationsverzeichnis` ist das Verzeichnis, in dem das Operations Center installiert ist):

- Zum Stoppen des Servers:

```
./stopserver.sh
```

- Zum Starten des Servers:

```
./startserver.sh
```

- Geben Sie die folgenden Befehle aus:

- Zum Stoppen des Servers:

```
service opscenter.rc stop
```

- Zum Starten des Servers:

```
service opscenter.rc start
```

- Zum erneuten Starten des Servers:

```
service opscenter.rc restart
```

Geben Sie den folgenden Befehl aus, um festzustellen, ob der Server ausgeführt wird:

```
service opscenter.rc status
```

- Im Fenster Dienste stoppen bzw. starten Sie den Dienst 'Operations Center'.

## Operations Center öffnen

---

Die Seite 'Übersicht' ist die Standardeingangsseite im Operations Center. In Ihrem Web-Browser können Sie jedoch für die Seite, die bei der Anmeldung beim Operations Center geöffnet werden soll, ein Lesezeichen setzen.

## Vorgehensweise

---

- Geben Sie die folgende Adresse in einem Web-Browser an. Dabei steht *Hostname* für den Namen des Computers, auf dem das Operations Center installiert ist, und *sicherer\_Anschluss* für die Anschlussnummer, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet:


```
https://Hostname:sicherer_Anschluss/oc
```

Tipps:

- Bei der URL muss die Groß-/Kleinschreibung beachtet werden. Achten Sie beispielsweise darauf, dass Sie "oc" wie gezeigt in Kleinbuchstaben eingeben.
  - Die Standardanschlussnummer für HTTPS-Kommunikation lautet 11090. Während der Installation des Operations Center kann jedoch eine andere Anschlussnummer angegeben werden.
2. Melden Sie sich unter Verwendung einer Administrator-ID an, die auf dem Hub-Server registriert ist.

Auf der Seite 'Übersicht' können Sie Übersichtsdaten für Clients, Services, Server, Speicherpools und Speichereinheiten anzeigen. Sie können weitere Details anzeigen, indem Sie auf die Elemente klicken oder indem Sie die Menüleiste des Operations Center verwenden.

Überwachung über eine mobile Einheit: Um die Speicherumgebung über Fernzugriff zu überwachen, können Sie die Seite 'Übersicht' des Operations Center im Web-Browser einer mobilen Einheit anzeigen. Das Operations Center unterstützt den Apple Safari-Web-Browser auf dem iPad. Es können auch andere mobile Einheiten verwendet werden.

## Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen

---

Der Clientverwaltungsservice erfasst Diagnoseinformationen über Clients für Sichern/Archivieren und stellt diese Informationen dem Operations Center für Basisüberwachungsfunktionen zur Verfügung.

### Informationen zu diesem Vorgang

---

Nach der Installation des Clientverwaltungsservice können Sie die Diagnosesseite im Operations Center aufrufen, um Fehlerbehebungsinformationen für Clients für Sichern/Archivieren anzuzeigen.

Diagnoseinformationen können nur von Linux- und Windows-Clients erfasst werden. Administratoren können jedoch die Diagnoseinformationen unter AIX, Linux oder Windows im Operations Center anzeigen.

Sie können den Clientverwaltungsservice auch auf Knoten mit Einheiten zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware installieren, um Diagnoseinformationen über die Einheiten zum Versetzen von Daten zu erfassen.

Tipp: In der Dokumentation für den Clientverwaltungsservice ist *Clientsystem* das System, in dem der Client für Sichern/Archivieren installiert ist.

- Clientverwaltungsservice mit einem grafisch orientierten Assistenten installieren  
Sie müssen den Clientverwaltungsservice auf den von Ihnen verwalteten Clientsystemen installieren, um Diagnoseinformationen über Clients für Sichern/Archivieren (z. B. Clientprotokolldateien) zu erfassen.
- Clientverwaltungsservice im unbeaufsichtigten Modus installieren  
Sie können den Clientverwaltungsservice im unbeaufsichtigten Modus installieren. Im unbeaufsichtigten Modus geben Sie die Installationswerte in einer Antwortdatei an und führen anschließend einen Installationsbefehl aus.
- Überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert wurde  
Bevor Sie Diagnoseinformationen über einen Client für Sichern/Archivieren mit dem Clientverwaltungsservice erfassen, können Sie überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert wurde.
- Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren  
Wenn Sie nicht die Standardkonfiguration für den Clientverwaltungsservice verwenden, müssen Sie das Operations Center für den Zugriff auf den Clientverwaltungsservice konfigurieren.
- Clientverwaltungsservice starten und stoppen  
Der Clientverwaltungsservice wird nach seiner Installation auf dem Clientsystem automatisch gestartet. Sie müssen den Service in bestimmten Situationen möglicherweise stoppen und starten.
- Clientverwaltungsservice deinstallieren  
Wenn Sie keine Clientdiagnoseinformationen mehr erfassen müssen, können Sie den Clientverwaltungsservice im Clientsystem deinstallieren.
- Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren  
Der Clientverwaltungsservice verwendet Informationen in der Clientkonfigurationsdatei (client-configuration.xml), um Diagnoseinformationen zu erkennen. Wenn der Clientverwaltungsservice die Position der Protokolldateien nicht erkennen kann, müssen Sie das Dienstprogramm CmsConfig ausführen, um die Position der Protokolldateien zur Datei client-configuration.xml hinzuzufügen.

# Clientverwaltungsservice mit einem grafisch orientierten Assistenten installieren

Sie müssen den Clientverwaltungsservice auf den von Ihnen verwalteten Clientsystemen installieren, um Diagnoseinformationen über Clients für Sichern/Archivieren (z. B. Clientprotokolldateien) zu erfassen.

## Vorbereitende Schritte

Lesen Sie den Abschnitt Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices.

## Informationen zu diesem Vorgang

Sie müssen den Clientverwaltungsservice auf demselben Computer wie den Client für Sichern/Archivieren installieren.

## Vorgehensweise

1. Laden Sie das Installationspaket für den Clientverwaltungsservice von einer IBM® Download-Site, z. B. IBM Passport Advantage oder IBM Fix Central, herunter. Suchen Sie nach einem Dateinamen, der etwa wie folgt lautet: `<Version>-IBM-SPCMS-<Betriebssystem>.bin`.

Die folgende Tabelle enthält die Namen der Installationspakete.

| Clientbetriebssystem | Installationspaketname            |
|----------------------|-----------------------------------|
| Linux x86 64-Bit     | 8.1.x.000-IBM-SPCMS-Linuxx64.bin  |
| Windows 32-Bit       | 8.1.x.000-IBM-SPCMS-Windows32.exe |
| Windows 64-Bit       | 8.1.x.000-IBM-SPCMS-Windows64.exe |

2. Erstellen Sie ein Verzeichnis auf dem Clientsystem, das Sie verwalten wollen, und kopieren Sie das Installationspaket dorthin.
3. Extrahieren Sie den Inhalt der Installationspaketdatei.

- o Gehen Sie in Linux-Clientsystemen wie folgt vor:

- a. Geben Sie den folgenden Befehl aus, um aus der Datei eine ausführbare Datei zu machen:

```
chmod +x 8.1.x.000-IBM-SPCMS-Linuxx64.bin
```

- b. Geben Sie den folgenden Befehl aus:

```
./8.1.x.000-IBM-SPCMS-Linuxx64.bin
```

- o In Windows-Clientsystemen klicken Sie doppelt auf den Namen des Installationspakets in Windows Explorer.

Tipp: Wenn Sie das Paket zuvor bereits installiert und deinstalliert haben, wählen Sie bei der Aufforderung, die vorhandenen Installationsdateien zu ersetzen, Alle aus.

4. Führen Sie die Installationsstapeldatei in dem Verzeichnis aus, in dem Sie die Installationsdateien und zugehörige Dateien extrahiert haben. Dies ist das Verzeichnis, das Sie in Schritt 2 erstellt haben.

- o Geben Sie auf Linux-Clientsystemen den folgenden Befehl aus:

```
./install.sh
```

- o In Windows-Clientsystemen klicken Sie doppelt auf install.bat.

5. Befolgen Sie die Anweisungen im Assistenten von IBM Installation Manager, um den Clientverwaltungsservice zu installieren.

Ist IBM Installation Manager auf dem Clientsystem noch nicht installiert, müssen Sie sowohl IBM Installation Manager als auch IBM Spectrum Protect-Clientverwaltungsservices auswählen.

Tipp: Sie können die Standardposition für das Verzeichnis für gemeinsam genutzte Ressourcen und für das Installationsverzeichnis von IBM Installation Manager übernehmen.

## Nächste Schritte

Befolgen Sie die Anweisungen in Überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert wurde.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Clientverwaltungsservice im unbeaufsichtigten Modus installieren



Sie können den Clientverwaltungsservice im unbeaufsichtigten Modus installieren. Im unbeaufsichtigten Modus geben Sie die Installationswerte in einer Antwortdatei an und führen anschließend einen Installationsbefehl aus.

## Vorbereitende Schritte

---

Lesen Sie den Abschnitt Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices.

Extrahieren Sie das Installationspaket gemäß den Anweisungen in Clientverwaltungsservice mit einem grafisch orientierten Assistenten installieren.

## Informationen zu diesem Vorgang

---

Sie müssen den Clientverwaltungsservice auf demselben Computer wie den Client für Sichern/Archivieren installieren.

Das Verzeichnis input, das sich in dem Verzeichnis befindet, in dem das Installationspaket extrahiert wird, enthält die folgende Musterantwortdatei:

install\_response\_sample.xml

Sie können die Musterdatei mit den Standardwerten verwenden oder diese Datei anpassen.

Tipp: Wenn Sie die Musterdatei anpassen wollen, müssen Sie eine Kopie der Musterdatei erstellen, die Kopie umbenennen und bearbeiten.

## Vorgehensweise

---

1. Erstellen Sie eine auf der Musterdatei basierende Antwortdatei oder verwenden Sie die Musterdatei install\_response\_sample.xml. In beiden Fällen müssen Sie sicherstellen, dass in der Antwortdatei die Anschlussnummer für den Clientverwaltungsservice angegeben ist. Der Standardanschluss ist 9028. Beispiel:

```
<variable name='port' value='9028' />
```

2. Führen Sie den Installationsbefehl für den Clientverwaltungsservice aus und akzeptieren Sie die Lizenz. Geben Sie in dem Verzeichnis, in dem die Installationspaketdatei extrahiert wurde, den folgenden Befehl aus (*Antwortdatei* steht für den Pfad der Antwortdatei einschließlich des Dateinamens):

Auf einem Linux-Clientsystem:

```
./install.sh -s -input Antwortdatei -acceptLicense
```

Beispiel:

```
./install.sh -s -input /cms_install/input/install_response.xml -acceptLicense
```

Auf einem Windows-Clientsystem:

```
install.bat -s -input Antwortdatei -acceptLicense
```

Beispiel:

```
install.bat -s -input c:\cms_install\input\install_response.xml -acceptLicense
```

## Nächste Schritte

---

Befolgen Sie die Anweisungen in Überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert wurde.

## Überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert wurde

---

Bevor Sie Diagnoseinformationen über einen Client für Sichern/Archivieren mit dem Clientverwaltungsservice erfassen, können Sie überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert wurde.

## Vorgehensweise

---

Geben Sie auf dem Clientsystem die folgenden Befehle in die Befehlszeile ein, um die Konfiguration des Clientverwaltungsservice anzuzeigen:

- Geben Sie auf Linux-Clientsystemen den folgenden Befehl aus:

```
Clientinstallationsverzeichnis/cms/bin/CmsConfig.sh list
```

*Clientinstallationsverzeichnis* ist das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist. Geben Sie bei einer Standardclientinstallation beispielsweise den folgenden Befehl aus:

```
/opt/tivoli/tsm/cms/bin/CmsConfig.sh list
```

Die Ausgabe kann wie in dem folgenden Beispiel aussehen:

```
CMS-Konfiguration auflisten

server1.example.com:1500 NO_SSL HOSTNAME
  Funktionen: [LOG_QUERY]
  Optionsdateipfad: /opt/tivoli/tsm/client/ba/bin/dsm.sys

  Protokolldatei: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
    en_US MM/dd/yyyy HH:mm:ss Windows-1252
  Protokolldatei: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
    en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

- Geben Sie auf Windows-Clientsystemen den folgenden Befehl aus:

```
Clientinstallationsverzeichnis\cms\bin\CmsConfig.bat list
```

*Clientinstallationsverzeichnis* ist das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist. Geben Sie bei einer Standardclientinstallation beispielsweise den folgenden Befehl aus:

```
C:"Program Files"\Tivoli\TSM\cms\bin\CmsConfig.bat list
```

Die Ausgabe kann wie in dem folgenden Beispiel aussehen:

```
CMS-Konfiguration auflisten

server1.example.com:1500 NO_SSL HOSTNAME
  Funktionen: [LOG_QUERY]
  Optionsdateipfad: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

  Protokolldatei: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
    en_US MM/dd/yyyy HH:mm:ss Windows-1252
  Protokolldatei: C:\Program Files\Tivoli\TSM\baclient\dmsched.log
    en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

Wenn der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist, zeigt die Ausgabe die Position der Fehlerprotokolldatei an.

Der Ausgabebetext wird aus der folgenden Konfigurationsdatei extrahiert:

- Auf Linux-Clientsystemen:

```
Clientinstallationsverzeichnis/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
```

- Auf Windows-Clientsystemen:

```
Clientinstallationsverzeichnis\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
```

Wenn die Ausgabe keine Einträge enthält, müssen Sie die Datei *client-configuration.xml* konfigurieren. Anweisungen zur Konfiguration dieser Datei finden Sie in Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren. Mit dem Befehl *CmsConfig verify* können Sie überprüfen, ob eine Knotendefinition in der Datei *client-configuration.xml* ordnungsgemäß erstellt wurde.

## Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren

---

Wenn Sie nicht die Standardkonfiguration für den Clientverwaltungsservice verwenden, müssen Sie das Operations Center für den Zugriff auf den Clientverwaltungsservice konfigurieren.

### Vorbereitende Schritte

---

Stellen Sie sicher, dass der Clientverwaltungsservice auf dem Clientsystem installiert und gestartet wird.

Überprüfen Sie, ob die Standardkonfiguration verwendet wird. Die Standardkonfiguration wird nicht verwendet, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Clientverwaltungsservice verwendet nicht die Standardanschlussnummer 9028.
- Für den Zugriff auf den Client für Sichern/Archivieren wird nicht dieselbe IP-Adresse wie für das Clientsystem verwendet, in dem der Client für Sichern/Archivieren installiert ist. Eine andere IP-Adresse könnte beispielsweise in den folgenden Situationen verwendet werden:
  - Das Computersystem verfügt über zwei Netzwerke. Der Client für Sichern/Archivieren ist für die Kommunikation in einem Netz konfiguriert, während der Clientverwaltungsservice in dem anderen Netz kommuniziert.
  - Das Clientsystem ist mit DHCP (Dynamic Host Configuration Protocol) konfiguriert. Folglich wird dem Clientsystem eine IP-Adresse dynamisch zugeordnet, die während der vorherigen Operation des Clients für Sichern/Archivieren auf dem IBM Spectrum Protect-Server gespeichert wird. Wenn das Clientsystem neu gestartet wird, kann ihm eine andere IP-Adresse zugeordnet werden. Um sicherzustellen, dass das Operations Center das Clientsystem immer finden kann, geben Sie einen vollständig qualifizierten Domännennamen an.

## Vorgehensweise

Gehen Sie wie folgt vor, um das Operations Center für die Verwendung des Clientverwaltungsservice zu konfigurieren:

1. Wählen Sie auf der Seite Clients des Operations Center den Client aus.
2. Klicken Sie auf Details.
3. Klicken Sie auf die Registerkarte Eigenschaften.
4. Geben Sie im Feld URL für Ferndiagnose im Abschnitt Allgemein die URL für den Clientverwaltungsservice im Clientsystem an.

Die Adresse muss mit `https` beginnen. Die folgende Tabelle enthält Beispiele der URL für Ferndiagnose.

| URL-Typ                                      | Beispiel                                     |
|--|--|
| Mit DNS-Hostnamen und Standardanschluss 9028 | <code>https://server.example.com</code>      |
| Mit DNS-Hostnamen und ohne Standardanschluss | <code>https://server.example.com:1599</code> |
| Mit IP-Adresse und ohne Standardanschluss    | <code>https://192.0.2.0:1599</code>          |

5. Klicken Sie auf Speichern.

## Nächste Schritte

Auf Clientdiagnoseinformationen (z. B. Clientprotokolldateien) können Sie über die Registerkarte Diagnose im Operations Center zugreifen.

## Clientverwaltungsservice starten und stoppen

Der Clientverwaltungsservice wird nach seiner Installation auf dem Clientsystem automatisch gestartet. Sie müssen den Service in bestimmten Situationen möglicherweise stoppen und starten.

## Vorgehensweise

- Geben Sie die folgenden Befehle aus, um den Clientverwaltungsservice auf Linux-Clientsystemen zu stoppen, zu starten oder erneut zu starten:
  - Zum Stoppen des Service:

```
service cms.rc stop
```
  - Zum Starten des Service:

```
service cms.rc start
```
  - Zum erneuten Starten des Service:

```
service cms.rc restart
```
- Auf Windows-Clientsystemen öffnen Sie das Fenster Dienste, wo Sie den Dienst 'IBM Spectrum Protect-Clientverwaltungsservices' stoppen, starten oder erneut starten können.

## Clientverwaltungsservice deinstallieren

---

Wenn Sie keine Clientdiagnoseinformationen mehr erfassen müssen, können Sie den Clientverwaltungsservice im Clientsystem deinstallieren.

### Informationen zu diesem Vorgang

---

Sie müssen den Clientverwaltungsservice mit IBM® Installation Manager deinstallieren. Falls nicht mehr benötigt, können Sie auch IBM Installation Manager deinstallieren.

### Vorgehensweise

---

1. Deinstallieren Sie den Clientverwaltungsservice wie folgt auf dem Clientsystem:
  - a. Öffnen Sie IBM Installation Manager:
    - Wechseln Sie im Linux-Clientsystem in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das Unterverzeichnis eclipse (z. B. /opt/IBM/InstallationManager/eclipse) und geben Sie folgenden Befehl aus:

```
./IBMIM
```
    - Im Windows-Clientsystem öffnen Sie IBM Installation Manager über das Menü Start.
  - b. Klicken Sie auf Deinstallieren.
  - c. Wählen Sie IBM Spectrum Protect-Clientverwaltungsservices aus und klicken Sie auf Weiter.
  - d. Klicken Sie auf Deinstallieren und dann auf Fertigstellen.
  - e. Schließen Sie das IBM Installation Manager-Fenster.
2. Falls Sie IBM Installation Manager nicht mehr benötigen, deinstallieren Sie es im Clientsystem:
  - a. Öffnen Sie den Deinstallationsassistenten von IBM Installation Manager:
    - Wechseln Sie im Linux-Clientsystem in das Deinstallationsverzeichnis von IBM Installation Manager (z. B. /var/ibm/InstallationManager/uninstall) und geben Sie den folgenden Befehl aus:

```
./uninstall
```
    - Im Windows-Clientsystem klicken Sie auf Start > Systemsteuerung. Dann klicken Sie auf Programm deinstallieren > IBM Installation Manager > Deinstallieren.
  - b. Wählen Sie IBM Installation Manager im Fenster IBM Installation Manager aus (falls noch nicht ausgewählt) und klicken Sie auf Weiter.
  - c. Klicken Sie auf Deinstallieren und dann auf Fertigstellen.

## Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren

---

Der Clientverwaltungsservice verwendet Informationen in der Clientkonfigurationsdatei (client-configuration.xml), um Diagnoseinformationen zu erkennen. Wenn der Clientverwaltungsservice die Position der Protokolldateien nicht erkennen kann, müssen Sie das Dienstprogramm CmsConfig ausführen, um die Position der Protokolldateien zur Datei client-configuration.xml hinzuzufügen.



- Dienstprogramm CmsConfig  
Wenn Sie nicht die Standardclientkonfiguration verwenden, können Sie das Dienstprogramm CmsConfig auf dem Clientsystem ausführen, um die Position der Clientprotokolldateien zu erkennen und zur Datei client-configuration.xml hinzuzufügen. Nach Abschluss der Konfiguration kann der Clientverwaltungsservice auf die Clientprotokolldateien zugreifen und sie für Basisdiagnosefunktionen im Operations Center zur Verfügung stellen.

## Fehlerbehebung für die Operations Center-Installation

---

Wenn bei der Installation des Operations Center ein Problem auftritt, das Sie nicht lösen können, können Sie in den Beschreibungen der bekannten Probleme nach einer Lösungsmöglichkeit suchen.

-  Grafisch orientierter Installationsassistent kann auf einem AIX-System nicht gestartet werden  
Sie installieren das Operations Center auf einem AIX-System mithilfe des grafisch orientierten Assistenten und das Installationsprogramm startet nicht.
-  Chinesische, japanische oder koreanische Schriftarten werden nicht ordnungsgemäß angezeigt  
Chinesische, japanische oder koreanische Schriftarten werden im Operations Center unter Red Hat Enterprise Linux 5 nicht ordnungsgemäß angezeigt.

## Grafisch orientierter Installationsassistent kann auf einem AIX-System nicht gestartet werden


---

Sie installieren das Operations Center auf einem AIX-System mithilfe des grafisch orientierten Assistenten und das Installationsprogramm startet nicht.

### Lösung

---

Die in Operations Center mit einem grafisch orientierten Assistenten installierten aufgelisteten RPM-Dateien müssen auf dem Computer installiert sein. Überprüfen Sie, ob die RPM-Dateien installiert sind.

 Linux-Betriebssysteme

## Chinesische, japanische oder koreanische Schriftarten werden nicht ordnungsgemäß angezeigt

---

Chinesische, japanische oder koreanische Schriftarten werden im Operations Center unter Red Hat Enterprise Linux 5 nicht ordnungsgemäß angezeigt.

### Lösung

---

Installieren Sie die folgenden Schriftartpakete, die von Red Hat verfügbar sind:

- fonts-chinese
- fonts-japanese
- fonts-korean

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Operations Center deinstallieren

---

Sie können das Operations Center mit jeder der folgenden Methoden deinstallieren: grafischer Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

- Operations Center mit einem grafisch orientierten Assistenten deinstallieren  
Sie können das Operations Center mithilfe des grafisch orientierten Assistenten von IBM® Installation Manager deinstallieren.
- Operations Center im Konsolenmodus deinstallieren  
Zum Deinstallieren des Operations Center mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.
- Operations Center im unbeaufsichtigten Modus deinstallieren  
Zum Deinstallieren des Operations Center im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Operations Center mit einem grafisch orientierten Assistenten deinstallieren



---

Sie können das Operations Center mithilfe des grafisch orientierten Assistenten von IBM® Installation Manager deinstallieren.


### Vorgehensweise

---

1. Öffnen Sie IBM Installation Manager.

 AIX-Betriebssysteme  Linux-Betriebssysteme In dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das Unterverzeichnis eclipse (z. B. /opt/IBM/InstallationManager/eclipse) und geben Sie folgenden Befehl aus:

```
./IBMIM
```

 Windows-Betriebssysteme Sie können IBM Installation Manager über das Menü Start öffnen.

2. Klicken Sie auf Deinstallieren.

3. Wählen Sie die Option für das Operations Center aus und klicken Sie auf Weiter.
4. Klicken Sie auf Deinstallieren.
5. Klicken Sie auf Fertigstellen.



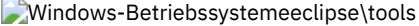
## Operations Center im Konsolenmodus deinstallieren

---


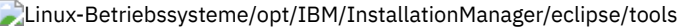
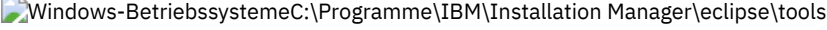
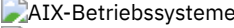
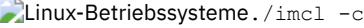
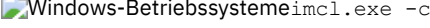
Zum Deinstallieren des Operations Center mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.

### Vorgehensweise

---

1. In dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das folgende Unterverzeichnis:
  -   eclipse/tools
  -  eclipse\tools

Beispiel:

-   /opt/IBM/InstallationManager/eclipse/tools
  -  C:\Programme\IBM\Installation Manager\eclipse\tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus:
    -   ./imcl -c
    -  imcl.exe -c
  3. Für die Deinstallation geben Sie **5** ein.
  4. Wählen Sie die Deinstallation aus der IBM Spectrum Protect-Paketgruppe aus.
  5. Geben Sie **N** für 'Next' (Weiter) ein.
  6. Wählen Sie die Deinstallation des Operations Center-Pakets aus.
  7. Geben Sie **N** für 'Next' (Weiter) ein.
  8. Geben Sie **U** für 'Uninstall' (Deinstallieren) ein.
  9. Geben Sie **F** für 'Finish' (Fertigstellen) ein.

## Operations Center im unbeaufsichtigten Modus deinstallieren

---

Zum Deinstallieren des Operations Center im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.

### Vorbereitende Schritte

---


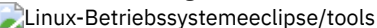
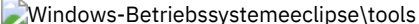
Sie können die Dateneingabe für eine unbeaufsichtigte Deinstallation des Operations Center-Servers mithilfe einer Antwortdatei bereitstellen. IBM Spectrum Protect enthält eine Musterantwortdatei, `uninstall_response_sample.xml`, im Verzeichnis `input`, in dem das Installationspaket extrahiert wird. Diese Datei enthält Standardwerte, durch die Sie unnötige Warnungen vermeiden können.

Wenn Sie das Operations Center deinstallieren wollen, lassen Sie die Einstellung `modify="false"` für den Operations Center-Eintrag in der Antwortdatei unverändert.


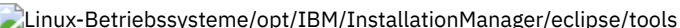
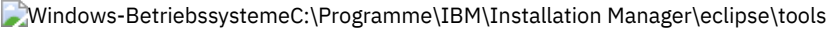
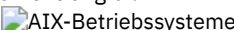
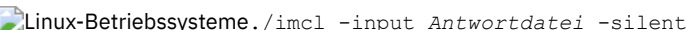
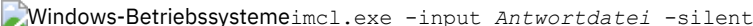
Wenn Sie die Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

### Vorgehensweise




---




1. In dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das folgende Unterverzeichnis:
  -   eclipse/tools
  -  eclipse\tools

Beispiel:

-   /opt/IBM/InstallationManager/eclipse/tools
  -  C:\Programme\IBM\Installation Manager\eclipse\tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus, wobei *Antwortdatei* den Pfad der Antwortdatei einschließlich des Dateinamens angibt:
    -   ./imcl -input *Antwortdatei* -silent
    -  imcl.exe -input *Antwortdatei* -silent

Der folgende Befehl ist ein Beispiel:

- o   Linux-Betriebssysteme `./imcl -input /tmp/input/uninstall_response.xml -silent`
- o  Windows-Betriebssysteme `imcl.exe -input C:\tmp\input\uninstall_response.xml -silent`

## Rollback zu einer vorherigen Version des Operations Center durchführen

Standardmäßig speichert IBM® Installation Manager ältere Versionen eines Pakets, damit ein Rollback ausgeführt werden kann, falls Probleme mit neueren Versionen von Updates, Fixes oder Paketen auftreten.

### Vorbereitende Schritte

Die Rollback-Funktion ist erst verfügbar, nachdem das Operations Center aktualisiert wurde.

### Informationen zu diesem Vorgang

Wenn IBM Installation Manager ein Rollback zu einer vorherigen Version durchführt, wird die aktuelle Version der Paketdateien deinstalliert und die frühere Version erneut installiert.

Um ein Rollback zu einer vorherigen Version durchführen zu können, muss IBM Installation Manager auf Dateien für diese Version zugreifen. Diese Dateien werden standardmäßig während jeder aufeinanderfolgenden Installation gespeichert. Da die Anzahl der gespeicherten Dateien bei jeder installierten Version zunimmt, sollten Sie diese Dateien regelmäßig aus Ihrem System löschen. Wenn Sie die Dateien löschen, können Sie jedoch kein Rollback zu einer vorherigen Version durchführen.

Gehen Sie wie folgt vor, um gespeicherte Dateien zu löschen oder um Ihre Einstellung für die Speicherung dieser Dateien bei zukünftigen Installationen zu aktualisieren:

1. Klicken Sie in IBM Installation Manager auf Datei > Benutzervorgaben.
2. Klicken Sie auf der Seite mit den Benutzervorgaben auf Dateien für Rollback und geben Sie Ihre Vorgaben an.

### Vorgehensweise

Wenn Sie ein Rollback zu einer vorherigen Version des Operations Center ausführen möchten, verwenden Sie die Funktion Rollback durchführen von IBM Installation Manager.

## Server konfigurieren

Um Konfigurationstasks für den IBM Spectrum Protect-Server auszuführen, lesen Sie die verfügbare Dokumentation.

### Informationen zu diesem Vorgang

Berücksichtigen Sie für eine bestehende Lösung die folgenden Aktionen.

Führen Sie zur Planung, Implementierung, Überwachung und Ausführung einer neuen Lösung die Anweisungen in IBM Spectrum Protect-Datenschutzlösungen aus.

Tipp: Ab IBM Spectrum Protect Version 7.1.3 ist das *Administratorhandbuch* veraltet.

| Aktion                                   | Details  | Dokumentation               |
|--|--|-----------------------------|
| Überwachen einer Speicherlösung          | Überwachen Sie die Speicherlösung, um vorhandene und potenzielle Probleme zu ermitteln. Auf diese Art und Weise können Sie Fehler beheben und die Systemleistung optimieren. | Speicherlösungen überwachen |
| Auswählen und Konfigurieren von Speicher | Wählen Sie Speicher auf der Basis Ihrer Geschäftsanforderungen aus und führen Sie dann die Tasks für die Konfiguration aus.  | Speicher konfigurieren      |

| Aktion  | Details   | Dokumentation   |
|---|---|---|
| Eliminieren doppelter Daten   | <p>Verwenden Sie die Datendeduplizierung, um redundante Daten in Speicherpools zu eliminieren. Die Datendeduplizierung reduziert den zum Aufbewahren der Daten erforderlichen Speicher. Es wird nur eine einzige Instanz der Daten in einem deduplizierten Speicherpool aufbewahrt.</p> <p>Ab IBM Spectrum Protect Version 7.1.3 können Sie die Inline-Datendeduplizierung verwenden.</p> | <p>Weitere Informationen zu den Unterschieden zwischen Inline-Datendeduplizierung und nachgeordneter Datendeduplizierung sowie Informationen zur Konfiguration der Best-Practice-Lösung für die Datendeduplizierung finden Sie in Datendeduplizierungsoptionen.</p>   |
| Replizieren von Daten   | <p>Sie können Clientknotendaten von einem Quellenreplikationsserver auf einen Zielreplikationsserver replizieren. Wenn ein Katastrophenfall eintritt und der Quellenserver vorübergehend nicht verfügbar ist, können Clientknoten ihre Daten vom Zielreplikationsserver wiederherstellen.</p>   | <p>Informationen zur Implementierung einer Best-Practice-Lösung, die IBM Spectrum Protect-Replikation und automatische Übernahme verwendet, finden Sie in Plattenspeicherlösung für mehrere Standorte.</p> <p>Allgemeine Informationen zur Replikation, einschließlich Konfigurationsschritten, finden Sie in Clientdaten auf einen anderen Server replizieren.</p>   |
| Verwalten der Datenbank und des Wiederherstellungsprotokolls                            | <p>Die Datenbank und das Wiederherstellungsprotokoll (der Serverbestand) speichern Informationen zu Clientdaten und sind für den Betrieb des Servers kritisch.</p>  | <ul style="list-style-type: none"> <li>• Allgemeine Informationen zur Datenbank und zum Wiederherstellungsprotokoll finden Sie in Datenbank und Wiederherstellungsprotokoll verwalten (Version 7.1.1).</li> <li>• Informationen zum Optimieren der Index- und Tabellenreorganisation für die Serverdatenbank und zum Verhindern und Beheben von Problemen, die das Datenbankwachstum betreffen, und von Leistungsproblemen finden Sie in Technote 1683633.</li> </ul> |
| Server schützen   | <p>Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.</p>  | <p>IBM Spectrum Protect-Server schützen</p>   |
| Konfigurieren von SSL für Lightweight Directory Access Protocol (LDAP)                  | <p>Sie können SSL für LDAP-Verzeichnisserver konfigurieren und Kennwörter und Anmeldeverfahren verwalten.</p>   | <p>Informationen zu LDAP finden Sie in:</p> <ul style="list-style-type: none"> <li>• Benutzer mithilfe eines LDAP-Servers authentifizieren</li> <li>• SSL oder TLS für LDAP-Verzeichnisserver konfigurieren (Version 7.1.1)</li> </ul>  |
| Informationen zu Maßnahmen für die Datenaufbewahrung und Konfigurieren dieser Maßnahmen | <p>IBM Spectrum Protect-Maßnahmen definieren die Regeln zur Verwaltung Ihrer Daten.</p>   | <p>Verwenden Sie das Operations Center, um Maßnahmen zu aktualisieren.</p> <p>Weitere Informationen zu Maßnahmen und zum Erstellen von Maßnahmen finden Sie in Maßnahmen anpassen.</p>  |



| Aktion  | Details  | Dokumentation  |
|---|--|--|
| Schützen des Servers und Wiederherstellen des Servers nach einem Katastrophenfall | Schützen Sie Ihre Systeminfrastruktur und Ihre Daten, damit eine Wiederherstellung nach einem Katastrophenfall möglich ist. Verwenden Sie die von IBM Spectrum Protect bereitgestellten Tools und Prozeduren zur Erstellung eines Plans zur Wiederherstellung nach einem Katastrophenfall. | Informationen zum Schützen und Wiederherstellen des Servers finden Sie in: <ul style="list-style-type: none"> <li>• Datenbank und Infrastrukturkonfigurationsdateien schützen (Version 7.1.1)</li> <li>• Disaster Recovery Manager für Bandumgebungen verwenden (Version 7.1.1)</li> </ul> |
| Schützen von NAS-Dateiservern   | Sie können eine Sicherungsumgebung, die Ihren NAS-Dateiserver schützt, planen, konfigurieren und verwalten.  | NAS-Dateiserver schützen   |
| Konfigurieren einer Clusterumgebung   | Konfigurieren Sie eine Clusterumgebung unter AIX, Linux oder Windows, um eine höhere Serververfügbarkeit und eine möglichst kurze Ausfallzeit zu gewährleisten.  | Clusterumgebungen konfigurieren  |
| Überprüfen der Lizenzeinhaltung   | Stellen Sie sicher, dass die Bedingungen Ihrer Lizenzvereinbarung von Ihrer IBM Spectrum Protect-Lösung eingehalten werden. Indem die Einhaltung regelmäßig überprüft wird, können Sie Trends beim Datenwachstum oder der PVU-Nutzung verfolgen.   | Lizenzeinhaltung überprüfen  |

- IBM Spectrum Protect-Server schützen  
Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.
- Clientdaten auf einen anderen Server replizieren  
Mithilfe der Replikation von Clientdaten von einem Quellenserver auf einen anderen Server kann sichergestellt werden, dass gesicherte Clientdaten für die Wiederherstellung verfügbar sind, wenn der Quellenserver beschädigt ist. Bei der Replikation werden Daten inkrementell vom Quellenserver auf den Zielserverserver kopiert, um Übernahme- und Rückübertragungsfunktionalität bereitzustellen.
- Clusterumgebungen konfigurieren  
Sie können den IBM Spectrum Protect-Server für das Clustering auf AIX-, Linux- oder Windows-Systemen konfigurieren.

## IBM Spectrum Protect-Server schützen

Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.

- Sicherheitskonzepte  
Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.
- Administratoren verwalten  
Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.
- Kennwortanforderungen ändern  
Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.
- IBM Spectrum Protect auf dem System schützen  
Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.
- Speicherumgebung vor Ransomware-Attacken schützen  
Speicherumgebungen, die mit dem Internet verbunden sind, können das Ziel von Ransomware-Attacken sein. Sie können

Maßnahmen ergreifen, um Ihre Speicherumgebung vor Ransomware zu schützen und Ihre Server und Clients im Fall einer Attacke wiederherstellen zu können.

- Kommunikation schützen  
Ihre Daten und Kennwörter sind sicherer, wenn Sie mithilfe von Secure Sockets Layer (SSL) oder Transport Layer Security (TLS), einer Form von SSL, geschützt werden.
- IBM Spectrum Protect-Benutzer mithilfe eines LDAP-Servers authentifizieren  
In einem IBM Spectrum Protect-System müssen sich Benutzer beim Server durch die Angabe einer Benutzer-ID und eines Kennworts authentifizieren. Wenn Ihr Unternehmen einen Lightweight Directory Access Protocol-Server (LDAP-Server) zur Verwaltung von Benutzer-IDs verwendet, können Sie den LDAP-Server für die Authentifizierung von IBM Spectrum Protect-Benutzer-IDs verwenden.

## Sicherheitskonzepte

---

Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.

### Transport Layer Security

---

Mithilfe des Protokolls Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) können Sie Transportschichtersicherheit für eine sichere Verbindung zwischen Servern, Clients und Speicheragenten bereitstellen. Wenn Sie Daten zwischen dem Server, dem Client und dem Speicheragenten austauschen, verwenden Sie SSL oder TLS zum Verschlüsseln der Daten.

Tipp: In der gesamten IBM Spectrum Protect-Dokumentation gilt jede Angabe von "SSL" oder zum "Auswählen von SSL" für TLS.

SSL wird von Global Security Kit (GSKit) bereitgestellt, das zusammen mit dem IBM Spectrum Protect-Server installiert wird, der vom Server, vom Client und vom Speicheragenten verwendet wird.

Einschränkung: Sie dürfen die SSL- oder TLS-Protokolle nicht für die Kommunikation mit einer DB2-Datenbankinstanz verwenden, die von IBM Spectrum Protect-Servern verwendet wird.

Jeder Server, Client oder Speicheragent, der SSL ermöglicht, muss ein vertrauenswürdigen selbst signiertes Zertifikat verwenden oder ein eindeutiges Zertifikat anfordern, das von einer Zertifizierungsstelle (CA) signiert ist. Sie können Ihre eigenen Zertifikate verwenden oder Zertifikate bei einer Zertifizierungsstelle (CA) kaufen. Jedes der Zertifikate muss installiert und der Schlüsseldatenbank auf dem IBM Spectrum Protect-Server, -Client oder -Speicheragenten hinzugefügt werden. Das Zertifikat wird von dem SSL-Client oder -Server geprüft, der die SSL-Kommunikation anfordert oder einleitet. Einige CA-Zertifikate sind in der Schlüsseldatenbank standardmäßig vorinstalliert.

SSL wird auf dem IBM Spectrum Protect-Server, -Client und -Speicheragenten unabhängig voneinander konfiguriert.

### Berechtigungsstufen

---

Für jeden IBM Spectrum Protect-Server sind verschiedene Administratorberechtigungsstufen verfügbar, die die Tasks festlegen, die ein Administrator ausführen kann.

Nach der Registrierung muss einem Administrator Berechtigung erteilt werden, indem ihm eine oder mehrere Administratorberechtigungsstufen zugeordnet werden. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen und anderen Administratoren über den Befehl GRANT AUTHORITY Berechtigungsstufen zuordnen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

Ein Administrator kann andere Administrator-IDs registrieren, den IDs Berechtigungsstufen zuordnen, IDs umbenennen, IDs entfernen und IDs für den Server sperren oder entsperren.

Ein Administrator kann den Zugriff auf bestimmte Clientknoten für Rootbenutzer-IDs und Nicht-Rootbenutzer-IDs steuern. Standardmäßig kann eine Nicht-Rootbenutzer-ID keine Daten auf dem Knoten sichern. Ändern Sie mit dem Befehl UPDATE NODE die Knoteneinstellungen, um Sicherungen zu ermöglichen.

### Kennwörter

---

Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer beim Zugriff auf den Server ein Kennwort eingeben.

Verwenden Sie LDAP (Lightweight Directory Access Protocol), um striktere Anforderungen für Kennwörter anzuwenden. Weitere Informationen finden Sie in Benutzer mithilfe eines LDAP-Servers authentifizieren.

Tabelle 1. Merkmale der Kennwortauthentifizierung

| Merkmale | Weitere Informationen |
|----------|-----------------------|
|----------|-----------------------|

| Merkmale                                   | Weitere Informationen  |
|--|--|
| Abhängigkeit von der Groß-/Kleinschreibung | Nicht von der Groß-/Kleinschreibung abhängig.  |
| Standardwert für Kennwortablauf            | 90 Tage.<br>Der Ablaufzeitraum beginnt mit der ersten Registrierung einer Administrator-ID oder eines Clientknotens beim Server. Wenn das Kennwort innerhalb dieses Zeitraums nicht geändert wird, muss das Kennwort beim nächsten Zugriff des Benutzers auf den Server geändert werden. |
| Ungültige Kennworteingabeversuche          | Sie können einen Grenzwert für aufeinanderfolgende ungültige Kennworteingabeversuche für alle Clientknoten definieren. Wenn der Grenzwert überschritten wird, sperrt der Server den Knoten.  |
| Kennwortlänge                              | Der Administrator kann eine Mindestlänge angeben.  |

## Sitzungssicherheit

Die Sitzungssicherheit ist die Sicherheitsstufe, die für die Kommunikation zwischen IBM Spectrum Protect-Clientknoten, -Verwaltungsclients und -Servern verwendet wird und mit dem Parameter SESSIONSECURITY festgelegt wird.

Der Parameter SESSIONSECURITY kann auf einen der folgenden Werte gesetzt werden:

- Mit dem Wert STRICT wird die höchste Sicherheitsstufe für die Kommunikation zwischen IBM Spectrum Protect-Servern, -Knoten und -Administratoren durchgesetzt.
- Der Wert TRANSITIONAL gibt an, dass das vorhandene Kommunikationsprotokoll verwendet wird, wenn Sie Ihre IBM Spectrum Protect-Software auf Version 8.1.2 oder höher aktualisieren. Dies ist der Standardwert. Wenn SESSIONSECURITY=TRANSITIONAL angegeben ist, werden strengere Sicherheitseinstellungen automatisch durchgesetzt, da höhere Versionen des TLS-Protokolls verwendet werden, wenn die Software auf Version 8.1.2 oder höher aktualisiert wird. Nachdem ein Knoten, Administrator oder Server die Anforderungen für den Wert STRICT erfüllt, wird die Sitzungssicherheit automatisch in den Wert STRICT geändert und die Entität kann sich nicht mehr unter Verwendung einer Vorgängerversion des Clients oder unter Verwendung früherer TLS-Protokolle authentifizieren.

Weitere Informationen zu den Werten für den Parameter SESSIONSECURITY enthalten die Beschreibungen der folgenden Befehle.

Tabelle 2. Befehle zum Festlegen des Parameters SESSIONSECURITY

| Entität         | Befehl   |
|-----------------|--|
| Clientknoten    | <ul style="list-style-type: none"> <li>• REGISTER NODE</li> <li>• UPDATE NODE</li> </ul>   |
| Administratoren | <ul style="list-style-type: none"> <li>• REGISTER ADMIN</li> <li>• UPDATE ADMIN</li> </ul> |
| Server          | <ul style="list-style-type: none"> <li>• DEFINE SERVER</li> <li>• UPDATE SERVER</li> </ul> |

Administratoren, die sich unter Verwendung des Befehls DSMADMC, des Befehls DSMC oder des Programms dsm authentifizieren, können sich nach der Authentifizierung unter Verwendung von Version 8.1.2 oder höher nicht unter Verwendung einer früheren Version authentifizieren. Die folgenden Tipps liefern Informationen zur Behebung von Authentifizierungsproblemen für Administratoren:  
Tipps:

- Stellen Sie sicher, dass für die gesamte IBM Spectrum Protect-Software, die das Administratorkonto für die Anmeldung verwendet, ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird. Wenn sich ein Administratorkonto über mehrere Systeme anmeldet, stellen Sie sicher, dass das Zertifikat des Servers auf jedem System installiert ist.
- Nachdem sich ein Administrator bei einem Server der Version 8.1.2 oder höher unter Verwendung eines Clients der Version 8.1.2 oder höher authentifiziert hat, kann sich der Administrator nur auf Clients oder Servern authentifizieren, die Version 8.1.2 oder höher verwenden. Ein Administratorbefehl kann von jedem beliebigen System ausgegeben werden.
- Erstellen Sie, falls erforderlich, ein separates Administratorkonto, das nur mit Clients und Servern verwendet wird, die Software der Version 8.1.1 oder früher verwenden.

Setzen Sie die höchste Sicherheitsstufe für die Kommunikation mit dem IBM Spectrum Protect-Server durch, indem Sie sicherstellen, dass alle Knoten, Administratoren und Server die Sitzungssicherheit STRICT verwenden. Mithilfe des Befehls SELECT können Sie feststellen, welche Server, Knoten und Administratoren die Sitzungssicherheit TRANSITIONAL verwenden und für die Verwendung der Sitzungssicherheit STRICT aktualisiert werden sollten.

### Zugehörige Verweise:

Kommunikation schützen

SELECT (SQL-Abfrage für die Datenbank ausführen)

## Administratoren verwalten

Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.

### Vorgehensweise

Führen Sie die folgenden Tasks aus, um Administratoreinstellungen zu ändern.

| Task  | Prozedur  |
|---|---|
| Administrator hinzufügen                        | Um einen Administrator, ADMIN1, mit Systemberechtigung hinzuzufügen und ein Kennwort anzugeben, führen Sie die folgenden Schritte aus:<br><br>a. Registrieren Sie den Administrator und geben Sie Pa\$#\$twO als Kennwort an, indem Sie den folgenden Befehl ausgeben:<br><br><code>register admin admin1 Pa\$#\$twO</code><br><br>b. Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben:<br><br><code>grant authority admin1 classes=system</code> |
| Administratorberechtigung ändern                | Ändern Sie die Berechtigungsstufe für einen Administrator, ADMIN1.<br><br><ul style="list-style-type: none"><li>• Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben:<br/><br/><code>grant authority admin1 classes=system</code></li><li>• Entziehen Sie dem Administrator die Systemberechtigung, indem Sie den folgenden Befehl ausgeben:<br/><br/><code>revoke authority admin1 classes=system</code></li></ul>                                 |
| Administratoren entfernen                       | Entfernen Sie einen Administrator, ADMIN1, sodass er nicht mehr auf den IBM Spectrum Protect-Server zugreifen kann, indem Sie den folgenden Befehl ausgeben:<br><br><code>remove admin admin1</code>  |
| Zugriff auf den Server vorübergehend verhindern | Sperren oder entsperren Sie einen Administrator, indem Sie den Befehl LOCK ADMIN bzw. UNLOCK ADMIN verwenden.   |

## Kennwortanforderungen ändern

Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.

### Informationen zu diesem Vorgang

Indem Sie die Kennwortauthentifizierung durchsetzen und Kennworteinschränkungen verwalten, können Sie Ihre Daten und Ihre Server vor möglichen Sicherheitsrisiken schützen.

### Vorgehensweise

Führen Sie die folgenden Tasks aus, um Kennwortanforderungen für IBM Spectrum Protect-Server zu ändern.

Tabelle 1. Authentifizierungstasks für IBM Spectrum Protect-Server

| Task  | Prozedur   |
|---|--|
| Grenzwert für ungültige Kennworteingabeversuche festlegen | <p>a. Wählen Sie auf der Seite Server im Operations Center den Server aus.</p> <p>b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale.</p> <p>c. Geben Sie die Anzahl ungültiger Versuche im Feld Grenzwert für ungültige Anmeldeversuche an.</p> <p>Der Standardwert bei der Installation ist 0.</p>   |
| Mindestlänge für Kennwörter festlegen                     | <p>a. Wählen Sie auf der Seite Server im Operations Center den Server aus.</p> <p>b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale.</p> <p>c. Geben Sie die Anzahl Zeichen im Feld Mindestlänge für Kennwort an.</p>   |
| Ablaufzeitraum für Kennwörter festlegen                   | <p>a. Wählen Sie auf der Seite Server im Operations Center den Server aus.</p> <p>b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale.</p> <p>c. Geben Sie die Anzahl Tage im Feld Allgemeine Kennwortablaufdauer an.</p>   |
| Kennwortauthentifizierung inaktivieren                    | <p>Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer ein Kennwort eingeben, um auf den Server zugreifen zu können.</p> <p>Sie können die Kennwortauthentifizierung nur für Kennwörter inaktivieren, die mit dem Server (LOCAL) authentifiziert werden. Durch das Inaktivieren der Kennwortauthentifizierung erhöht sich das Sicherheitsrisiko für den Server.</p> |
| Standardauthentifizierungsmethode festlegen               | <p>Geben Sie den Befehl SET DEFAULTAUTHENTICATION aus. Um beispielsweise den Server als die Standardauthentifizierungsmethode zu verwenden, geben Sie den folgenden Befehl aus:</p> <pre>set defaultauthentication local</pre> <p>Um einen Clientknoten für die Authentifizierung mit dem Server zu aktualisieren, schließen Sie AUTHENTICATION=LOCAL in den Befehl UPDATE NODE ein:</p> <pre>update node authentication=local</pre>                 |

## IBM Spectrum Protect auf dem System schützen

Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

### Vorgehensweise

Stellen Sie sicher, dass nicht berechtigte Benutzer nicht auf die Verzeichnisse für die Serverdatenbank und die Serverinstanz zugreifen können. Behalten Sie die Zugriffseinstellungen für diese Verzeichnisse bei, die Sie während der Implementierung konfiguriert haben.

- Benutzerzugriff auf den Server einschränken  
Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.
- Zugriff über Porteinschränkungen einschränken  
Schränken Sie den Zugriff auf den Server ein, indem Sie Porteinschränkungen anwenden.

## Benutzerzugriff auf den Server einschränken

Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

## Vorgehensweise

- Nachdem Sie einen Administrator mit dem Befehl REGISTER ADMIN registriert haben, legen Sie die Berechtigungsstufe des Administrators mithilfe des Befehls GRANT AUTHORITY fest. Ausführliche Informationen zum Festlegen und Ändern der Berechtigung finden Sie in Administratoren verwalten.
- Um die Berechtigung eines Administrators zur Ausführung bestimmter Tasks zu steuern, verwenden Sie die beiden folgenden Serveroptionen:
  - Über die Serveroption QUERYAUTH können Sie die Berechtigungsstufe auswählen, die ein Administrator haben muss, um Befehle QUERY und SELECT ausgeben zu können. Standardmäßig ist keine Berechtigungsstufe erforderlich. Sie können die Anforderung in eine der Berechtigungsstufen, einschließlich Systemberechtigung, ändern.
  - Über die Serveroption REQSYSAUTHOUTFILE können Sie angeben, dass Systemberechtigung für Befehle erforderlich ist, die zur Folge haben, dass der Server Daten in eine externe Datei schreibt. Standardmäßig ist für diese Befehle Systemberechtigung erforderlich.
- Sie können die Datensicherung auf einem Clientknoten ausschließlich auf Rootbenutzer-IDs oder berechtigte Benutzer beschränken. Um beispielsweise Sicherungen auf die Rootbenutzer-ID zu beschränken, geben Sie den Befehl REGISTER NODE oder UPDATE NODE unter Angabe des Parameters BACKUPINITIATION=root aus:

```
update node backupinitiation=root
```

## Zugriff über Porteinschränkungen einschränken

Schränken Sie den Zugriff auf den Server ein, indem Sie Porteinschränkungen anwenden.

### Informationen zu diesem Vorgang

Gegebenenfalls müssen Sie abhängig von Ihren Sicherheitsanforderungen den Zugriff auf bestimmte Server einschränken. Der IBM Spectrum Protect-Server kann so konfiguriert werden, dass er an vier TCP/IP-Ports empfangsbereit ist: zwei Ports, die für reguläre TCP/IP-Protokolle oder SSL-/TLS-Protokolle verwendet werden können, und zwei Ports, die nur für das SSL-/TLS-Protokoll verwendet werden können.

## Vorgehensweise

Sie können die Serveroptionen wie in Tabelle 1 aufgeführt zur Angabe des erforderlichen Ports festlegen.

Tabelle 1. Serveroptionen und Portzugriff

| Serveroption    | Portzugriff  |
|-----------------|--|
| TCPPORT         | Gibt die Nummer des Ports an, dem der TCP/IP-DFV-Treiber des Servers auf Anforderungen von Clientsitzungen warten soll. Dieser Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen empfangsbereit. Der Standardwert ist 1500.  |
| TCPADMINPORT    | Gibt die Nummer des Ports an, an dem der TCP/IP-DFV-Treiber des Servers auf Anforderungen von anderen Sitzungen als Clientsitzungen warten soll. Dieser Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen empfangsbereit. Der Standardwert ist der Wert für TCPPORT.<br><br>Verwenden Sie diese Option, um den Datenverkehr des Verwaltungsclients vom Datenverkehr des regulären Clients, der die Optionen TCPPORT und SSLTCPSPORT verwendet, zu trennen. |
| SSLTCPSPORT     | Gibt die SSL-TCP/-IP-Portadresse für einen Server an. Dieser Port ist nur für SSL-fähige Sitzungen empfangsbereit. Ein Standardwert für den Port ist nicht verfügbar.  |
| SSLTCPADMINPORT | Gibt die Portadresse an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen von SSL-fähigen Sitzungen wartet. Ein Standardwert für den Port ist nicht verfügbar.<br><br>Verwenden Sie diese Option, um den Datenverkehr des Verwaltungsclients vom Datenverkehr des regulären Clients, der die Optionen TCPPORT und SSLTCPSPORT verwendet, zu trennen.  |

Einschränkungen:

Wenn Sie die Server-Ports, die nur für SSL gelten, (SSLTCPSPORT und SSLTCPADMINPORT) angeben, gelten die folgenden Einschränkungen:

- Wenn Sie den Server-Port, der nur für SSL gilt, für den Parameter LLADDRESS im Befehl DEFINE SERVER oder im Befehl UPDATE SERVER angeben, müssen Sie auch den Parameter SSL=YES angeben.

- Wenn Sie den Server-Port, der nur für SSL gilt, für die Clientoption TCPSPORT angeben, müssen Sie auch YES für die SSL-Clientoption angeben.

## Speicherumgebung vor Ransomware-Attacken schützen

---

Speicherumgebungen, die mit dem Internet verbunden sind, können das Ziel von Ransomware-Attacken sein. Sie können Maßnahmen ergreifen, um Ihre Speicherumgebung vor Ransomware zu schützen und Ihre Server und Clients im Fall einer Attacke wiederherstellen zu können.

### Informationen zu diesem Vorgang

---

*Ransomware* ist eine Schadsoftware, die für den Zugriff auf ein Computersystem und zum Verschlüsseln der Daten verwendet wird. Normalerweise verschlüsselt der Initiator einer Ransomware-Attacke Daten und kontaktiert dann den Eigner der Daten, um Lösegeld zu fordern. Der Initiator der Attacke droht für den Fall, dass das Lösegeld nicht bezahlt wird, damit, die Daten verschlüsselt zu lassen. Aus diesem Grund ist es notwendig, Ihre Speicherumgebung vor einer Ransomware-Attacke zu schützen, indem Sie eine Kopie der Daten an einem Standort speichern, der *nicht* über das Internet zugänglich ist.

Eine Möglichkeit besteht darin, Ihre Datenbank auf Band und Clients in Kopierspeicherpools auf Band zu sichern und die Banddatenträger dann an einen sicheren anderen Standort zu transportieren. Wenn Sie diese Strategie verwenden, können Sie die IBM Spectrum Protect-Funktion 'Disaster Recovery Manager' (DRM) aktivieren, um den Transport von ausgelagerten Datenträgern zu verfolgen und diese Informationen in der IBM Spectrum Protect-Datenbank zu registrieren. DRM konsolidiert Pläne, Scripts und andere Informationen in einer Plandatei. Mithilfe der Plandatei können Sie Ihre Server und Clients nach einer Ransomware-Attacke wiederherstellen.

### Vorgehensweise

---

1. Überlegen Sie bei der Planung für Ihre Speicherumgebung, ob Bänder als Speichermedium verwendet werden sollen und ob die Banddatenträger an einem anderen Standort transportiert werden sollen. Anweisungen zum Konfigurieren von Bandspeicher finden Sie in Bandspeicherlösung.
2. Überlegen Sie bei der Planung für Ihre Speicherumgebung, ob die Funktion DRM zur Wiederherstellung nach einer Ransomware-Attacke, einer ungeplanten Betriebsunterbrechung oder einem Katastrophenfall verwendet werden soll. Eine Einführung in DRM finden Sie in Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM.
3. Überprüfen Sie die Maßnahmen, die für Ihre Speicherumgebung festgelegt sind, um sicherzustellen, dass eine ausreichende Anzahl Sicherungen beibehalten wird und die Kopien für eine ausreichende Anzahl Tage beibehalten werden. Wenn Ihre neuesten Daten durch Ransomware verschlüsselt sind, können Sie weiterhin auf vorherige Versionen zugreifen. Um Maßnahmen festzulegen, verwenden Sie das Operations Center oder die Befehle DEFINE COPYGROUP und UPDATE COPYGROUP. Informationen zu bevorzugten Einstellungen finden Sie in Aufbewahrung und Verfall von Sicherungsversionen.
4. Überwachen Sie Ihr System täglich, um Ransomware so bald wie möglich zu erkennen. Weitere Informationen finden Sie in Prüfliste für tägliche Überwachungstasks und Prüfliste für regelmäßige Überwachungstasks.

## Kommunikation schützen

---

Ihre Daten und Kennwörter sind sicherer, wenn Sie mithilfe von Secure Sockets Layer (SSL) oder Transport Layer Security (TLS), einer Form von SSL, geschützt werden.

SSL und TLS sind die Standardtechnologien zum Erstellen verschlüsselter Sitzungen zwischen Servern und Clients. SSL und TLS stellen einen sicheren Kanal für Server und Clients bereit, um über offene Kommunikationspfade zu kommunizieren. Bei SSL und TLS wird die Identität des Servers mithilfe digitaler Zertifikate geprüft. Clients und Server, die IBM Spectrum Protect-Software der Version 8.1.2 oder höher für die Kommunikation verwenden, werden automatisch für die Verwendung von TLS 1.2 konfiguriert. Speicheragenten, die IBM Spectrum Protect-Software der Version 8.1.3 und höher oder Tivoli Storage Manager-Software der Version 7.1.8 oder höher verwenden, werden ebenfalls automatisch konfiguriert.

Anmerkung: In Version 8.1.2 müssen Sie Speicheragenten manuell für die Verwendung von SSL konfigurieren.

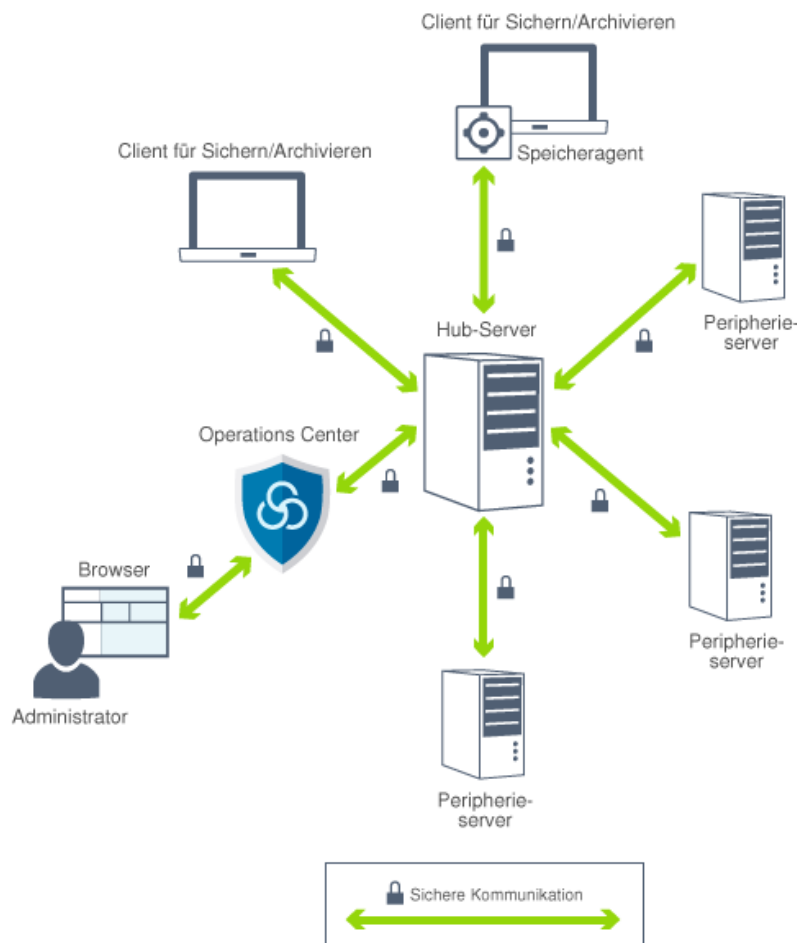
Um die Systemleistung zu verbessern, verwenden Sie TLS für die Authentifizierung ohne die Verschlüsselung von Objektdaten. Informationen zur Angabe, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, finden Sie in der Beschreibung der Clientoption SSL für die Client/Server-Kommunikation und in der Beschreibung des Parameters SSL im Befehl UPDATE SERVER für die Kommunikation zwischen Servern. Wenn TLS für die Verschlüsselung von Objektdaten verwendet werden soll, fügen Sie gegebenenfalls weitere Prozessressourcen auf dem IBM Spectrum Protect-Server hinzu, um den erhöhten Datenaustausch im Netz handhaben zu können.

Wenn Sie Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren, schützt TLS Kennwörter zwischen dem IBM Spectrum Protect-Server und dem LDAP-Server. TLS ist für die gesamte Kommunikation mit LDAP-Kennwort erforderlich.

- Kommunikation über Secure Sockets Layer und Transport Layer Security  
Mithilfe des Protokolls Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) können Sie Transportschichtssicherheit für eine sichere Verbindung zwischen IBM Spectrum Protect-Servern, -Clients, -Speicheragenten und dem Operations Center bereitstellen. Wenn Sie Daten zwischen dem Server, dem Client und dem Speicheragenten austauschen, wird SSL oder TLS zum Verschlüsseln der Daten verwendet.
- Speicheragenten, Server, Clients und das Operations Center für die Verbindung zum Server unter Verwendung von SSL konfigurieren  
Konfigurieren Sie Secure Sockets Layer (SSL) auf dem IBM Spectrum Protect-Server, dem Client für Sichern/Archivieren, dem Speicheragenten und im Operations Center, um sicherzustellen, dass Daten während der Kommunikation verschlüsselt werden.

## Kommunikation über Secure Sockets Layer und Transport Layer Security

Mithilfe des Protokolls Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) können Sie Transportschichtssicherheit für eine sichere Verbindung zwischen IBM Spectrum Protect-Servern, -Clients, -Speicheragenten und dem Operations Center bereitstellen. Wenn Sie Daten zwischen dem Server, dem Client und dem Speicheragenten austauschen, wird SSL oder TLS zum Verschlüsseln der Daten verwendet.



Einschränkung: Sie dürfen das SSL- oder TLS-Protokoll nicht für die Kommunikation mit einer IBM DB2-Datenbankinstanz verwenden, die vom IBM Spectrum Protect-Server verwendet wird.

Jeder Server oder Speicheragent verfügt über einen eindeutigen privaten Schlüssel und ein eindeutiges signiertes Zertifikat, mit dem SSL-Verbindungen ermöglicht werden. Wenn Sie selbst signierte Zertifikate verwenden, müssen Sie das selbst signierte Zertifikat für jeden Server oder Speicheragenten an alle Clients, Speicheragenten und Server verteilen, die TLS für die Kommunikation verwenden. Wenn Sie von einer Zertifizierungsstelle (CA) signierte Zertifikate verwenden, müssen Sie nur die CA-Zertifikate an alle Clients, Speicheragenten und Server verteilen, die TLS für die Kommunikation verwenden.

Wenn Sie ein Stammzertifikat von einer Zertifizierungsstelle verwenden, müssen Sie das Zertifikat in jeder Schlüsseldatenbank für den Client, den Server und den Speicheragenten installieren, der die SSL-Kommunikation einleitet. Ein *Stammzertifikat* ist ein Zertifikat, das die Stammzertifizierungsstelle angibt. Das Zertifikat wird von dem SSL-Client oder -Server geprüft, der die SSL-Kommunikation anfordert oder einleitet.



Der IBM Spectrum Protect-Server erlaubt CA-signierte Zertifikate mit SHA-256 oder niedriger. SHA-256-Zertifikate werden aufgrund verbesserter Sicherheit und der Einhaltung von NIST-Standards empfohlen. Für die Kommunikation mit dem Operations Center wird SHA-256 empfohlen.

Ab IBM Spectrum Protect Version 8.1.2 ist SSL standardmäßig für die Kommunikation zwischen Servern und Clients der Version 8.1.2 aktiviert. Ab IBM Spectrum Protect-Software der Version 8.1.3 oder höher und ab Tivoli Storage Manager-Software der Version 7.1.8 werden Speicheragenten automatisch für die Verwendung von SSL konfiguriert.

Anmerkung: In Version 8.1.2 müssen Sie Speicheragenten manuell für die Verwendung von SSL konfigurieren.

Der IBM Spectrum Protect-Server, -Client oder -Speicheragent kann während der Kommunikation als SSL-Client fungieren. Ein SSL-Client ist die Komponente, die die Kommunikation einleitet und das Zertifikat für einen SSL-Server prüft. Wenn beispielsweise der IBM Spectrum Protect-Client die SSL-Kommunikation mit dem IBM Spectrum Protect-Server einleitet, ist der IBM Spectrum Protect-Client der SSL-Client und der Server der SSL-Server.

In Tabelle 1 sind die Komponenten aufgelistet, die ein SSL-Client oder SSL-Server sein können.

Tabelle 1. SSL-Clients und -Server in der IBM Spectrum Protect-Umgebung

| SSL-Client                                    | SSL-Server                                 | Szenario   |
|---|--|--|
| Client  | Server                                     | Der IBM Spectrum Protect-Client initiiert eine Kommunikationsanforderung mit dem IBM Spectrum Protect-Server. Der Client prüft das Zertifikat. Der Server stellt das Zertifikat bereit.  |
| Server (wie beispielsweise ein Quellenserver) | Server (wie beispielsweise ein Zielserver) | Der IBM Spectrum Protect-Quellenserver initiiert eine Kommunikationsanforderung mit dem IBM Spectrum Protect-Zielserver. Der Quellenserver fungiert als SSL-Client und prüft das vom Zielserver bereitgestellte Zertifikat.<br><br>Dieser Typ von Kommunikation ist während der Replikationsverarbeitung üblich.   |
| Client über einen Speicheragenten             | Server                                     | Der Client überprüft jedes Zertifikat, wenn er die SSL-Kommunikation mit dem IBM Spectrum Protect-Server und dem Speicheragenten separat einleitet.<br><br>Wenn der Speicheragent mit dem Server unter Verwendung des SSL-Kommunikationsprotokolls kommuniziert, fungiert der Speicheragent als SSL-Client und prüft das vom Server bereitgestellte Zertifikat.<br><br>Der Speicheragent kann gleichzeitig SSL-Client und SSL-Provider sein. |
| Server  | LDAP-Server                                | Der IBM Spectrum Protect-Server initiiert eine Kommunikationsanforderung mit dem LDAP-Server. Der IBM Spectrum Protect-Server fungiert als SSL-Client und prüft das vom LDAP-Server bereitgestellte Zertifikat.  |
| Operations Center                             | Server                                     | Das Operations Center initiiert eine Kommunikationsanforderung mit dem IBM Spectrum Protect-Server. Das Operations Center fungiert als SSL-Client und prüft das vom IBM Spectrum Protect-Server bereitgestellte Zertifikat.  |
| Reporting                                     | Server                                     | Der Reporting-Agent initiiert eine Kommunikationsanforderung mit dem IBM Spectrum Protect-Server. Das Reporting-Feature fungiert als SSL-Client und prüft das vom IBM Spectrum Protect-Server bereitgestellte Zertifikat.  |

## Speicheragenten, Server, Clients und das Operations Center für die Verbindung zum Server unter Verwendung von SSL konfigurieren

Konfigurieren Sie Secure Sockets Layer (SSL) auf dem IBM Spectrum Protect-Server, dem Client für Sichern/Archivieren, dem Speicheragenten und im Operations Center, um sicherzustellen, dass Daten während der Kommunikation verschlüsselt werden.

Mithilfe eines selbst signierten SSL-Zertifikats oder eines signierten Zertifikats einer unabhängigen Zertifizierungsstelle (CA) können Sie eine SSL-Kommunikationsanforderung zwischen dem Server, dem Client und dem Speicheragenten überprüfen. Jeder IBM Spectrum Protect-Server, -Client oder -Speicheragent, der SSL ermöglicht, muss ein vertrauenswürdigen selbst signiertes Zertifikat verwenden oder ein eindeutiges Zertifikat anfordern, das von einer Zertifizierungsstelle signiert ist.

Der Vorteil CA-signierter Zertifikate liegt darin, dass ein einziges CA-signiertes Zertifikat für alle Server verwendet werden kann und damit ein einziges Zertifikat an Clients verteilt werden kann. Wenn Sie ein selbst signiertes Zertifikat verwenden, wird das Zertifikat automatisch für jeden Server und jeden Speicheragenten erstellt. Wenn Sie ein Stammzertifikat von einer Zertifizierungsstelle verwenden, muss das Zertifikat in jeder Schlüsseldatenbank für den Client, den Server und den Speicheragenten installiert werden, der die SSL-Kommunikation einleitet. Das Zertifikat wird von dem SSL-Client oder -Server geprüft, der die SSL-Kommunikation anfordert oder einleitet.

Einschränkung: Einige Zertifizierungsstellen (CAs) verwenden Zertifikate in einem Format, das von IBM Spectrum Protect nicht erkannt wird. Unter Umständen müssen Sie sich an Ihre Zertifizierungsstelle wenden, um das Zertifikat in ein Format zu konvertieren, das mit

IBM Spectrum Protect verwendet werden kann.

- Server zum Akzeptieren von SSL-Verbindungen konfigurieren  
Konfigurieren Sie den Server zum Akzeptieren von SSL-Verbindungen, bevor Sie die SSL-Kommunikation vom Server zu einem Client, einem Speicheragenten oder einem anderen Server aktivieren.
- Speicheragenten für die Verwendung von SSL konfigurieren  
Um sicherzustellen, dass Daten für die Kommunikation zwischen dem Speicheragenten und dem Server sowie zwischen dem Speicheragenten und dem Client verschlüsselt werden, konfigurieren Sie die Speicheragenten für die Kommunikation unter Verwendung des SSL-Protokolls.
- Client für die Verbindung zu einem Speicheragenten unter Verwendung von SSL konfigurieren  
Um die Daten, die zwischen einem Client und einem Speicheragenten übertragen werden, zu schützen, konfigurieren Sie den Client so, dass die Verbindung zum Speicheragenten unter Verwendung des SSL-Protokolls hergestellt wird.

## Server zum Akzeptieren von SSL-Verbindungen konfigurieren

---

Konfigurieren Sie den Server zum Akzeptieren von SSL-Verbindungen, bevor Sie die SSL-Kommunikation vom Server zu einem Client, einem Speicheragenten oder einem anderen Server aktivieren.

### Vorgehensweise

---

1. Geben Sie den Port an, an dem der Server auf die SSL-fähige Clientkommunikation wartet, oder akzeptieren Sie die Standardportnummer. Aktualisieren Sie wahlweise die Datei `dmserv.opt` im Serverinstanzverzeichnis, indem Sie die Option `TCPSPORT` und/oder die Option `TCPADMINPORT` angeben. Die Optionen `SSLTCPSPORT` und `SSLTCPADMINPORT` können nur für Verbindungen, die ausschließlich für SSL gelten, verwendet werden.
2. Erstellen Sie die Serverschlüsseldatenbank, indem Sie den Server starten. Die Serverschlüsseldatenbankdatei, `cert.kdb`, wird im Serverinstanzverzeichnis gespeichert und der Standardzertifikatskennsatz wird automatisch als "TSM Server SelfSigned SHA Key" festgelegt. Das Zertifikat wird in die Datei `cert256.arm` exportiert.
3. Wenn Sie das selbst signierte Standardzertifikat verwenden, ist die Datei für das selbst signierte Standardzertifikat (`cert256.arm`) erforderlich, wenn Sie die Verbindung zum Server unter Verwendung von TLS herstellen.
4. Wenn Sie ein CA-signiertes Zertifikat importieren, führen Sie die folgenden Schritte aus:

- a. Importieren Sie ein eindeutiges Zertifikat, das von einer Zertifizierungsstelle signiert wurde, auf jeden Server, der SSL ermöglicht. Sie können sowohl ein CA-signiertes Stammzertifikat als auch ein CA-signiertes Zwischenzertifikat importieren. Für jeden Server wird dasselbe CA-signierte Zertifikat verwendet. Melden Sie sich am IBM Spectrum Protect-Serversystem mit der Instanzbenutzer-ID an und geben Sie im Instanzverzeichnis den folgenden Beispielbefehl aus:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -label "CA-Stammzertifikat" -file ca.crt
```

- b. Um ein CA-signiertes Zwischenzertifikat zu importieren, geben Sie den folgenden Beispielbefehl aus:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed  
-label "CA-Zwischenzertifikat" -file intca.crt
```

- c. Das Stammzertifikat (`ca.crt`) und das Zwischenzertifikat (`intca.crt`) sind erforderlich, wenn Sie die Verbindung zum Server unter Verwendung von TLS herstellen.
- d. Erstellen Sie auf dem Server eine Zertifikatsanforderung für die Unterzeichnung durch die CA, indem Sie einen ähnlichen Befehl wie in dem folgenden Beispiel ausgeben:

```
gsk8capicmd_64 -certreq -create -db cert.kdb -stashed -label "CA-Zertifikat"  
-sigalg sha256 -size 2048 -ku "digitalSignature,keyEncipherment,keyAgreement "  
-eku "clientAuth,serverAuth" -dn "CN=tucson.example.com,OU=Spectrum Protect,O=IBM"  
-san_dnsname tucson.example.com -san_ipaddr 9.11.0.0 -file cert_request.csr
```

- e. Um das signierte Zertifikat zu erhalten und als Standardzertifikat für die Kommunikation mit Clients festzulegen, geben Sie den folgenden Beispielbefehl aus:

```
gsk8capicmd_64 -cert -receive -db cert.kdb -stashed -file signiertes_Zertifikat.crt  
-default_cert yes
```

5. Wenn Änderungen durchgeführt wurden, starten Sie den Server erneut.

### Nächste Schritte

---

Aktivieren Sie SSL-Kommunikation von einem Client, einem Speicheragenten oder einem anderen Server zu diesem Server. Um die folgenden Tasks ausführen zu können, müssen Ihnen das Zertifikat des Servers und die Portnummer, die für den Server definiert ist, zur Verfügung stehen.

1. Informationen zum Aktivieren der SSL-Kommunikation von einem Client zu diesem Server finden Sie in IBM Spectrum Protect-Client/Server-Übertragung mit Secure Sockets Layer konfigurieren.

- Informationen zum Aktivieren der SSL-Kommunikation von einem anderen Server zu diesem Server finden Sie in Server für die Verbindung zu einem anderen Server unter Verwendung von SSL konfigurieren.
  - Informationen zum Aktivieren der SSL-Kommunikation von einem Speicheragenten zu diesem Server finden Sie in Speicheragenten für die Verwendung von SSL konfigurieren.
  - Informationen zum Aktivieren der SSL-Kommunikation vom Operations Center zu diesem Server finden Sie in Operations Center für die Verbindung zum Hub-Server unter Verwendung von SSL konfigurieren.
- Clients für die Kommunikation mit dem Server unter Verwendung von SSL konfigurieren  
Um sicherzustellen, dass Daten während der Client/Server-Kommunikation verschlüsselt werden, konfigurieren Sie Clients für die Kommunikation mit dem Server unter Verwendung des SSL-Protokolls.
  - Server für die Verbindung zu einem anderen Server unter Verwendung von SSL konfigurieren  
Um sicherzustellen, dass Daten während der Kommunikation zwischen Servern verschlüsselt werden, konfigurieren Sie Server für die Kommunikation mit Servern unter Verwendung des SSL-Protokolls.
  - Operations Center für die Verbindung zum Hub-Server unter Verwendung von SSL konfigurieren  
Um sicherzustellen, dass Daten für die Kommunikation zwischen dem Operations Center und dem Hub-Server verschlüsselt werden, konfigurieren Sie das Operations Center für die Kommunikation mit dem Hub-Server unter Verwendung des SSL-Protokolls.

**Zugehörige Verweise:**

TCPPOPT

TCPADMINPORT

QUERY SESSION (Clientsitzungen abfragen)

## Clients für die Kommunikation mit dem Server unter Verwendung von SSL konfigurieren

---

Um sicherzustellen, dass Daten während der Client/Server-Kommunikation verschlüsselt werden, konfigurieren Sie Clients für die Kommunikation mit dem Server unter Verwendung des SSL-Protokolls.

### Vorbereitende Schritte

---

Das Zertifikat des Servers und die Nummer des Ports, den der Server verwendet, müssen Ihnen zur Verfügung stehen. Weitere Informationen finden Sie in Server zum Akzeptieren von SSL-Verbindungen konfigurieren.

### Vorgehensweise

---

Informationen zum Aktivieren der SSL-Kommunikation zwischen dem Server und Clients finden Sie in IBM Spectrum Protect-Client/Server-Übertragung mit Secure Sockets Layer konfigurieren.

## Server für die Verbindung zu einem anderen Server unter Verwendung von SSL konfigurieren

---

Um sicherzustellen, dass Daten während der Kommunikation zwischen Servern verschlüsselt werden, konfigurieren Sie Server für die Kommunikation mit Servern unter Verwendung des SSL-Protokolls.

### Vorbereitende Schritte

---

Das Zertifikat und die Portnummer des Servers, zu dem die Verbindung hergestellt wird, müssen Ihnen zur Verfügung stehen. Weitere Informationen finden Sie in Server zum Akzeptieren von SSL-Verbindungen konfigurieren.

### Informationen zu diesem Vorgang

---

Tipps:

- Wenn beide Server IBM Spectrum Protect-Software der Version 8.1.2 oder höher verwenden, wird SSL automatisch konfiguriert. Die manuelle Konfiguration wird empfohlen, ist aber nicht erforderlich. Wenn einer der Server IBM Spectrum Protect-Software vor Version 8.1.2 oder Tivoli Storage Manager-Software vor Version 7.1.8 verwendet, müssen Sie SSL manuell konfigurieren.
- In Version 8.1.2 müssen Sie Speicheragenten manuell für die Verwendung von SSL konfigurieren. In Version 8.1.3 werden Speicheragenten automatisch für die Verwendung von SSL konfiguriert.

In der Prozedur werden die folgenden Serveradressen als Beispiele verwendet:

- Die Adresse von ServerA (der Server, zu dem die Verbindung hergestellt wird) lautet `bfa.tucson.example.com`.

- Die Adresse von ServerB lautet `bfb.tucson.example.com`.

## Vorgehensweise

---

1. Erstellen Sie die Serverschlüsseldatenbank, indem Sie den Server starten. Die Serverschlüsseldatenbankdatei, `cert.kdb`, wird im Serverinstanzverzeichnis gespeichert.
2. Importieren Sie für jeden Server die Datei `cert256.arm` oder die CA-Zertifikatsdateien des anderen Servers:

```
gsk8capicmd_64 -cert -add -label Server-IP-Adresse -db cert.kdb -stashed  
-file cert256.arm
```

Tipp: Verwenden Sie die IP-Adresse des Servers als den Kennsatznamen.

3. Auf jedem Server können Sie die Zertifikate in der Schlüsseldatenbank anzeigen, indem Sie den folgenden Befehl ausgeben:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

4. Starten Sie die Server erneut.
5. Geben Sie den Befehl `DEFINE SERVER` aus.
  - a. Geben Sie für ServerA den folgenden Befehl aus:

```
DEFINE SERVER BFB hla=bfb.tucson.example.com lla=1542  
serverpa=Kennwort_für_BFB SSL=YES
```

- b. Geben Sie für ServerB den folgenden Befehl aus:

```
DEFINE SERVER BFA hla=bfa.tucson.example.com lla=1542  
serverpa=Kennwort_für_BFA SSL=YES
```

### Zugehörige Verweise:

QUERY SESSION (Clientsitzungen abfragen)

TCPPORT

TCPADMINPORT

DEFINE SERVER (Server für Übertragung zwischen Servern definieren)

## Operations Center für die Verbindung zum Hub-Server unter Verwendung von SSL konfigurieren

---

Um sicherzustellen, dass Daten für die Kommunikation zwischen dem Operations Center und dem Hub-Server verschlüsselt werden, konfigurieren Sie das Operations Center für die Kommunikation mit dem Hub-Server unter Verwendung des SSL-Protokolls.

### Vorbereitende Schritte

---

Das Zertifikat des Hub-Servers und die Nummer des Ports, den der Server verwendet, müssen Ihnen zur Verfügung stehen. Weitere Informationen finden Sie in *Server zum Akzeptieren von SSL-Verbindungen konfigurieren*.

### Vorgehensweise

---

Informationen zur Konfiguration der SSL-Kommunikation für das Operations Center finden Sie in *Kommunikation zwischen dem Operations Center und dem Hub-Server schützen*.

## Speicheragenten für die Verwendung von SSL konfigurieren

---

Um sicherzustellen, dass Daten für die Kommunikation zwischen dem Speicheragenten und dem Server sowie zwischen dem Speicheragenten und dem Client verschlüsselt werden, konfigurieren Sie die Speicheragenten für die Kommunikation unter Verwendung des SSL-Protokolls.

### Vorbereitende Schritte

---

Das Zertifikat des Servers und die Nummer des Ports, den der Server verwendet, müssen Ihnen zur Verfügung stehen. Weitere Informationen finden Sie in *Server zum Akzeptieren von SSL-Verbindungen konfigurieren*.

### Vorgehensweise

---

1. Initialisieren Sie den Speicheragenten und fügen Sie der Einheitenkonfigurationsdatei und der Optionsdatei des Speicheragenten (`dsmsta.opt`) Kommunikationsinformationen hinzu, indem Sie den Befehl `DSMSTA SETSTORAGESEVER` ausgeben. Sie müssen

den Parameter SSL=YES angeben, um die Schlüsseldatenbankdatei in dsmsta.opt zu erstellen. Alle Kennwörter in dsmsta.opt werden verschlüsselt.

```
dsmsta setstorageserver myname=Name_des_Speicheragenten mypa=Kennwort_des_Speicheragenten  
myhla=IP-Adresse servername=Servername serverpa=Serverkennwort hla=IP-Adresse lla=SSL-Port ssl=yes
```

2. Erstellen Sie das Schlüsseldatenbankzertifikat und die Standardzertifikate, indem Sie den Speicheragenten starten.
3. Importieren Sie für den Speicheragenten und den Server die Datei cert256.arm oder die CA-Zertifikatsdateien des jeweils anderen:

```
gsk8capicmd_64 -cert -add -label IP-Adresse -db cert.kdb -stashed  
-file cert256.arm
```

Tipp: Verwenden Sie die IP-Adresse als den Kennsatznamen.

4. Sie können die Zertifikate in der Schlüsseldatenbank anzeigen, indem Sie den folgenden Befehl ausgeben:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

5. Starten Sie den Speicheragenten und den Server erneut.
6. Bauen Sie die Kommunikation zwischen dem Server und dem Speicheragenten auf, indem Sie den folgenden Befehl ausgeben:

```
define server sta hla=IP-Adresse lla=Port serverpa=Kennwort ssl=yes
```

#### Zugehörige Verweise:

QUERY SESSION (Clientsitzungen abfragen)

TCPPORT

TCPADMINPORT

DEFINE SERVER (Server für Übertragung zwischen Servern definieren)

## Client für die Verbindung zu einem Speicheragenten unter Verwendung von SSL konfigurieren

---

Um die Daten, die zwischen einem Client und einem Speicheragenten übertragen werden, zu schützen, konfigurieren Sie den Client so, dass die Verbindung zum Speicheragenten unter Verwendung des SSL-Protokolls hergestellt wird.

### Vorbereitende Schritte

---

Das Zertifikat und die Portnummer für den Speicheragenten müssen Ihnen zur Verfügung stehen.

### Informationen zu diesem Vorgang

---

Nachdem Sie einen Speicheragenten zum Akzeptieren von SSL-Verbindungen konfiguriert haben, konfigurieren Sie Clients für die Herstellung der Verbindung zu dem Speicheragenten unter Verwendung von SSL.

### Vorgehensweise

---

Informationen zum Aktivieren der SSL-Kommunikation zwischen den Clients und dem Speicheragenten finden Sie in IBM Spectrum Protect-Client/Server-Übertragung mit Secure Sockets Layer konfigurieren.

#### Zugehörige Verweise:

TCPPORT

TCPADMINPORT

## IBM Spectrum Protect-Benutzer mithilfe eines LDAP-Servers authentifizieren

---

In einem IBM Spectrum Protect-System müssen sich Benutzer beim Server durch die Angabe einer Benutzer-ID und eines Kennworts authentifizieren. Wenn Ihr Unternehmen einen Lightweight Directory Access Protocol-Server (LDAP-Server) zur Verwaltung von Benutzer-IDs verwendet, können Sie den LDAP-Server für die Authentifizierung von IBM Spectrum Protect-Benutzer-IDs verwenden.

Sie können eine der folgenden Methoden verwenden, um Benutzer mit einem LDAP-Server zu authentifizieren:

Methode, die für IBM Spectrum Protect-Server der Version 7.1.7 und höher bevorzugt wird

Um diese Methode, die manchmal auch als *integrierter Modus* bezeichnet wird, verwenden zu können, müssen Benutzer-IDs in einer Active Directory-Datenbank auf einem LDAP-Server registriert werden. Anschließend registrieren Sie dieselben Benutzer

beim IBM Spectrum Protect-Server. Wenn eine registrierte Benutzer-ID auf den IBM Spectrum Protect-Server zugreift, werden die Berechtigungsnachweise mithilfe der Active Directory-Datenbank authentifiziert.

Führen Sie zur Verwendung dieser Methode die Anweisungen in Benutzer mithilfe einer Active Directory-Datenbank authentifizieren aus.

Methode, die für Server vor Version 7.1.7 und von Benutzern von IBM® Security Directory Server verwendet wird

Um diese Methode verwenden zu können, müssen Benutzer-IDs in einer Active Directory-Datenbank auf einem LDAP-Server registriert werden. Benutzer-IDs können auch stattdessen in einer Datenbank von IBM Security Directory Server (zuvor IBM Tivoli Directory Server) auf einem LDAP-Server registriert werden. Bei dieser Methode können Sie nicht die Standardbenutzerkonten verwenden, die beim LDAP-Server registriert sind. Sie müssen separate Benutzerkonten erstellen, die einer bestimmten Organisationseinheit zugeordnet sind. Führen Sie zur Verwendung dieser Methode die Anweisungen in Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1) aus. .

- Benutzer mithilfe einer Active Directory-Datenbank authentifizieren  
Sie können IBM Spectrum Protect-Benutzer mithilfe einer Active Directory-Datenbank auf einem Lightweight Directory Access Protocol-Server (LDAP-Server) authentifizieren. Bei dieser Methode verwenden Sie die Standardbenutzerkonten, die beim LDAP-Server registriert sind. Dieselbe Benutzer-ID kann zur Authentifizierung beim IBM Spectrum Protect-Server und LDAP-Server verwendet werden.

## Clientdaten auf einen anderen Server replizieren

---

Mithilfe der Replikation von Clientdaten von einem Quellenserver auf einen anderen Server kann sichergestellt werden, dass gesicherte Clientdaten für die Wiederherstellung verfügbar sind, wenn der Quellenserver beschädigt ist. Bei der Replikation werden Daten inkrementell vom Quellenserver auf den Zielserver kopiert, um Übernahme- und Rückübertragungsfunktionalität bereitzustellen.

### Informationen zu diesem Vorgang

---

Wenn ein Katastrophenfall eintritt und der Quellenserver vorübergehend nicht verfügbar ist, können Clientknoten ihre Daten vom Zielserver wiederherstellen. Wenn eine Wiederherstellung des Quellenservers nicht möglich ist, können Sie Clientknotenkonfigurationen ändern, um Daten auf dem Zielserver zu speichern. Bei einem Ausfall kann für den Quellenserver automatisch eine Übernahme durch einen Zielserver zum Zweck der Datenwiederherstellung erfolgen.

Einschränkung: Ein Server kann Daten nur auf einen einzigen Zielserver replizieren.

Die Replikation kann für Daten, die in einem beliebigen Typ von Speicherpool gespeichert sind, ausgeführt werden. Der Speicherpooltyp auf dem Quellenreplikationsserver und der Speicherpooltyp dem Zielreplikationsserver können unterschiedlich sein. Die Replikation kann anhand des Typs der Clientknotendaten gesteuert werden:

- Gleichzeitig aktive und inaktive Sicherungsdaten oder nur aktive Sicherungsdaten
- Archivierungsdaten
- Daten, die von IBM Spectrum Protect for Space Management-Clients auf einen Quellenserver umgelagert wurden

Wenn Sie Daten in Verzeichniscontainerspeicherpools replizieren, verwenden Sie Speicherpoolschutz, um die Effizienz des Replikationsprozesses zu verbessern und die Reparatur von Daten zu ermöglichen. Wenn Sie Ihre Speicherpools mithilfe des Operations Center konfigurieren, werden Zeitpläne für den Schutz automatisch in Koordination mit dem Replikationszeitplan definiert.

### Vorgehensweise

---

1. Stellen Sie sicher, dass Server kompatibel sind und über die Systemressourcen für die erfolgreiche Verwendung der Replikation verfügen.

Es sind mehr Speicherkapazität und mehr Prozessorkerne erforderlich. Die Größe der Datenbank und der zugehörigen Protokolle müssen geändert werden, um sicherzustellen, dass Transaktionen ausgeführt werden können. Es ist ein dediziertes Netz mit ausreichender Bandbreite zur Verarbeitung des zu replizierenden Datenvolumens erforderlich.

- a. Stellen Sie sicher, dass die Quellen- und Zielserver für die Replikation kompatibel sind. Siehe Replikationskompatibilität.
- b. Stellen Sie sicher, dass der Server über die entsprechenden Ressourcen verfügt, um eine gute Leistung erzielen zu können.  
Ausführliche Informationen finden Sie in Prüfliste für Knotenreplikation.

2. Aktivieren Sie die Replikation. Siehe Knotenreplikation aktivieren.
3. Planen Sie die Replikation für den Quellenserver. Informationen zur Integration dieses Zeitplans in die Zeitpläne für die regelmäßige Serververwaltung finden Sie in Zeitpläne für Serververwaltungsaktivitäten definieren.
4. Planen Sie den Speicherpoolschutz für alle Verzeichniscontainerspeicherpools auf dem Quellenserver. Siehe Daten in Verzeichniscontainerspeicherpools schützen.
5. Überwachen Sie die Replikation mithilfe des Operations Center. Weitere Informationen finden Sie in Prüfliste für tägliche Überwachungstasks.

- Replikationskompatibilität  
Vor dem Konfigurieren von Replikationsoperationen mit IBM Spectrum Protect müssen Sie sicherstellen, dass die Quellen- und

- Zielreplikationsserver für die Replikation kompatibel sind.
- Knotenreplikation aktivieren  
Sie können die Knotenreplikation zum Schützen Ihrer Daten aktivieren.
- Daten in Verzeichniscontainerspeicherpools schützen  
Schützen Sie Daten in Verzeichniscontainerspeicherpools, um die Knotenreplikationszeit zu reduzieren und die Reparatur von Daten in Verzeichniscontainerspeicherpools zu ermöglichen.
- Replikationseinstellungen ändern  
Ändern Sie Replikationseinstellungen im Operations Center. Ändern Sie Einstellungen wie die Anzahl Replikationssitzungen, Replikationsregeln, die Daten, die repliziert werden sollen, den Replikationszeitplan und die Replikationsworkload.
- Unterschiedliche Aufbewahrungsmaßnahmen für den Quellenserver und den Zielservers festlegen  
Auf dem Zielreplikationsserver können Sie Maßnahmen festlegen, mit denen die replizierten Clientknotendaten anders als auf dem Quellenserver verwaltet werden. Beispielsweise können Sie auf dem Quellen- und dem Zielservers eine unterschiedliche Anzahl Versionen von Dateien aufbewahren.

## Replikationskompatibilität

Vor dem Konfigurieren von Replikationsoperationen mit IBM Spectrum Protect müssen Sie sicherstellen, dass die Quellen- und Zielreplikationsserver für die Replikation kompatibel sind.

Tabelle 1. Replikationskompatibilität von Serverversionen

| Version des Quellenreplikationsservers | Kompatible Versionen für den Zielreplikationsserver |
|--|---|
| Version 7.1                            | Version 7.1 oder höher                              |
| Version 7.1.1                          | Version 7.1 oder höher                              |
| Version 7.1.3                          | Version 7.1.3 oder höher                            |
| Version 7.1.4                          | Version 7.1.3 oder höher                            |
| Version 7.1.5                          | Version 7.1.3 oder höher                            |
| Version 7.1.6                          | Version 7.1.3 oder höher                            |
| Version 7.1.7                          | Version 7.1.3 oder höher                            |
| Version 7.1.8                          | Version 7.1.3 oder höher                            |
| Version 8.1                            | Version 7.1.3 oder höher                            |
| Version 8.1.1                          | Version 7.1.3 oder höher                            |
| Version 8.1.2                          | Version 7.1.3 oder höher                            |
| Version 8.1.3                          | Version 7.1.3 oder höher                            |

## Knotenreplikation aktivieren

Sie können die Knotenreplikation zum Schützen Ihrer Daten aktivieren.

### Vorbereitende Schritte

Stellen Sie sicher, dass die Quellen- und Zielservers für die Replikation kompatibel sind.

### Informationen zu diesem Vorgang

Replizieren Sie den Clientknoten, um alle Clientdaten, einschließlich Metadaten, zu replizieren. Standardmäßig ist die Knotenreplikation inaktiviert, wenn Sie den Server zum ersten Mal starten.

Tipps:

- Um die Replikationsverarbeitungszeit zu reduzieren, schützen Sie den Speicherpool vor dem Replizieren von Clientknoten. Wenn die Knotenreplikation gestartet wird, werden die Datenbereiche, die bereits durch den Speicherpoolschutz repliziert werden, übersprungen.
- Die Replikation erfordert mehr Speicherkapazität und genügend Bandbreite für die Ausführung der Verarbeitung. Ändern Sie die Größe der Datenbank und der zugehörigen Protokolle, um sicherzustellen, dass Transaktionen ausgeführt werden können.

### Vorgehensweise


Um die Knotenreplikation zu aktivieren, führen Sie im Operations Center die folgenden Schritte aus:

- a. Klicken Sie auf der Seite Server auf Details.
- b. Klicken Sie auf der Seite Details auf Merkmale.
- c. Wählen Sie im Abschnitt Replikation im Feld Abgehende Replikation die Option Aktiviert aus.
- d. Klicken Sie auf Sichern.

## Nächste Schritte

---

Führen Sie die folgenden Aktionen aus:

1. Informationen zur Überprüfung, ob die Replikation erfolgreich war, finden Sie in Prüfliste für tägliche Überwachungstasks.
2.  Wenn der IBM Spectrum Protect-Server Knoten auf einen fernen Server repliziert, prüfen Sie, ob der Datendurchsatz an den fernen Server mithilfe der Technologie von Aspera Fast Adaptive Secure Protocol (FASP) verbessert werden kann. Führen Sie die Anweisungen in Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann aus.

## Daten in Verzeichniscontainerspeicherpools schützen

---

Schützen Sie Daten in Verzeichniscontainerspeicherpools, um die Knotenreplikationszeit zu reduzieren und die Reparatur von Daten in Verzeichniscontainerspeicherpools zu ermöglichen.

### Vorbereitende Schritte

---

Stellen Sie sicher, dass mindestens ein Verzeichniscontainerspeicherpool auf dem Zielreplikationsserver vorhanden ist. Wenn Sie die Replikation im Operations Center aktivieren, können Sie den Speicherpoolschutz planen. Um die Replikation zu konfigurieren und den Speicherpoolschutz zu aktivieren, führen Sie die folgenden Schritte aus:

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Speicher und klicken Sie auf Replikation.
2. Klicken Sie auf der Seite 'Replikation' auf Serverpaar.
3. Führen Sie die Schritte im Assistenten 'Serverpaar hinzufügen' aus.

### Informationen zu diesem Vorgang

---

Durch das Schützen eines Verzeichniscontainerspeicherpools werden Datenbereiche in einem anderen Speicherpool gesichert und die Leistung bei der Knotenreplikation wird gegebenenfalls verbessert. Wenn die Knotenreplikation gestartet wird, werden die Datenbereiche, die bereits durch Speicherpoolschutz gesichert werden, übersprungen und die Replikationsverarbeitungszeit wird somit reduziert. Sie können den Schutz von Speicherpools mehrmals am Tag planen, um den Änderungen an Daten Rechnung zu tragen.

Indem ein Speicherpool geschützt wird, werden keine Ressourcen verwendet, die vorhandene Daten und Metadaten replizieren, wodurch die Serverleistung verbessert wird. Sie müssen Verzeichniscontainerspeicherpools verwenden, wenn nur der Speicherpool geschützt und gesichert werden soll.

Alternative Schutzstrategie: Als Alternative zur Verwendung der Replikation können Sie Daten in Verzeichniscontainerspeicherpools schützen, indem Sie die Daten in Containerkopierspeicherpools kopieren. Daten in Containerkopierspeicherpools werden auf Banddatenträgern gespeichert. Bandkopien, die an einem anderen Standort aufbewahrt werden, stellen zusätzlichen Schutz für die Wiederherstellung nach einem Katastrophenfall in einer replizierten Umgebung bereit.

### Vorgehensweise

---

1. Um den Speicherpoolschutz zu aktivieren, können Sie auch stattdessen den Befehl PROTECT STGPOOL auf dem Quellenserver verwenden, um Datenbereiche in einem Verzeichniscontainerspeicherpool zu sichern. Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen POOL1 zu schützen, geben Sie den folgenden Befehl aus:

```
protect stgpool pool1
```

Im Rahmen der Ausführung des Befehls PROTECT STGPOOL werden beschädigte Speicherbereiche im Zielspeicherpool repariert. Eine Reparatur ist nur möglich, wenn die Speicherbereiche auf dem Zielserver bereits als beschädigt markiert sind. Beispielsweise kann vor der Ausgabe des Befehls PROTECT STGPOOL mit einem Befehl AUDIT CONTAINER eine Beschädigung im Zielspeicherpool identifiziert werden.

2. Optional: Wenn beschädigte Speicherbereiche im Zielspeicherpool repariert wurden und Sie mehrere Quellenspeicherpools in einem einzigen Zielspeicherpool schützen, führen Sie die folgenden Schritte aus, um eine vollständige Reparatur zu gewährleisten:
  - a. Geben Sie den Befehl PROTECT STGPOOL für alle Quellenspeicherpools aus, um die Beschädigung möglichst vollständig zu reparieren.
  - b. Geben Sie den Befehl PROTECT STGPOOL erneut für alle Quellenspeicherpools aus. Verwenden Sie bei dieser zweiten Operation den Parameter FORCERECONCILE=YES. Mit diesem Schritt wird sichergestellt, dass alle Reparaturen anderer



Quellenpools korrekt für alle Quellenspeicherpools erkannt werden.


## Ergebnisse

Wenn ein Verzeichniscontainerspeicherpool geschützt wird, können Sie den Speicherpool für den Fall, dass eine Beschädigung auftritt, mit dem Befehl REPAIR STGPOOL reparieren.

Einschränkung: Wenn Sie Clientknoten replizieren, den Verzeichniscontainerspeicherpool aber nicht schützen, können Sie den Speicherpool nicht reparieren.

## Nächste Schritte


Führen Sie die folgenden Aktionen aus:

1. Um den Replikationsworkloadstatus anzuzeigen, führen Sie die Anweisungen in Prüfliste für tägliche Überwachungstasks aus.
2.  Wenn der IBM Spectrum Protect-Server Knoten auf einen fernen Server repliziert, prüfen Sie, ob der Datendurchsatz an den fernen Server mithilfe der Technologie von Aspera Fast Adaptive Secure Protocol (FASP) verbessert werden kann. Führen Sie die Anweisungen in Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann aus.

### Zugehörige Tasks:

 Verzeichniscontainerspeicherpools auf Band kopieren

### Zugehörige Verweise:

 AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)

 PROTECT STGPOOL (Speicherpooldaten schützen)

## Replikationseinstellungen ändern

Ändern Sie Replikationseinstellungen im Operations Center. Ändern Sie Einstellungen wie die Anzahl Replikationssitzungen, Replikationsregeln, die Daten, die repliziert werden sollen, den Replikationszeitplan und die Replikationsworkload.

## Informationen zu diesem Vorgang

In den folgenden Szenarios müssen Sie möglicherweise Ihre Replikationseinstellungen ändern:

- Änderungen an Datenprioritäten
- Änderungen an Replikationsregeln
- Erfordernis eines anderen Servers als Zielsever
- Geplante Prozesse, die sich negativ auf die Serverleistung auswirken

## Vorgehensweise

Ändern Sie Replikationseinstellungen mithilfe des Operations Center.

| Task  | Prozedur  |
|---|---|
| Ändern einer Replikationsregel                        | <ol style="list-style-type: none"><li>a. Klicken Sie auf der Seite Server auf Details.</li><li>b. Klicken Sie auf der Seite Details auf Merkmale.</li><li>c. Wählen Sie im Abschnitt Replikation die Replikationsregel aus, die angewendet werden soll: Standardregel für Archivierungsdaten, Standardregel für Sicherungsdaten oder Standardregel für speicher verwaltete Daten.</li><li>d. Klicken Sie auf Sichern.</li></ol>   |
| Aufbewahrungsdauer für Replikationsdatensätze angeben | <ol style="list-style-type: none"><li>a. Klicken Sie auf der Seite Server auf Details.</li><li>b. Klicken Sie auf der Seite Details auf Merkmale.</li><li>c. Geben Sie im Abschnitt Replikation im Feld Replikationsprotokoll aufbewahren die Anzahl Tage ein, die Replikationsdatensätze beibehalten werden müssen. Sie können auch das Kontrollkästchen Nicht aufbewahren auswählen, wenn Replikationsdatensätze nicht erforderlich sind.</li><li>d. Klicken Sie auf Sichern.</li></ol> |

| Task                           | Prozedur   |
|--------------------------------|--|
| Zielreplikationsserver angeben | a. Klicken Sie auf der Seite Server auf Details.<br>b. Klicken Sie auf der Seite Details auf Merkmale.<br>c. Geben Sie im Abschnitt Replikation den Zielsever an.<br>d. Klicken Sie auf Sichern. |
| Replikationsprozess abbrechen  | a. Klicken Sie auf der Seite Server auf Aktive Tasks.<br>b. Wählen Sie den Prozess oder die Sitzung aus, der bzw. die abgebrochen werden soll.<br>c. Klicken Sie auf Abbrechen.                  |

## Unterschiedliche Aufbewahrungsmaßnahmen für den Quellenserver und den Zielsever festlegen

Auf dem Zielreplikationsserver können Sie Maßnahmen festlegen, mit denen die replizierten Clientknotendaten anders als auf dem Quellenserver verwaltet werden. Beispielsweise können Sie auf dem Quellen- und dem Zielsever eine unterschiedliche Anzahl Versionen von Dateien aufbewahren.

### Vorgehensweise

- Überprüfen Sie auf dem Quellenreplikationsserver die Replikationskonfiguration und stellen Sie sicher, dass der Quellenreplikationsserver mit dem Zielreplikationsserver kommunizieren kann, indem Sie den Befehl `VALIDATE REPLICATION` ausgeben. Überprüfen Sie beispielsweise die Konfiguration unter Angabe des Namens eines Clientknotens, der repliziert wird:

```
validate replication node1 verifyconnection=yes
```

- Geben Sie auf dem Quellenreplikationsserver den Befehl `VALIDATE REPLPOLICY` aus, um die Unterschiede zwischen den Maßnahmen auf dem Quellenreplikationsserver und den Maßnahmen auf dem Zielreplikationsserver zu überprüfen. Um beispielsweise die Unterschiede zwischen den Maßnahmen auf dem Quellenserver und den Maßnahmen auf dem Zielsever `CVT_SRV2` anzuzeigen, geben Sie auf dem Quellenserver den folgenden Befehl aus:

```
validate replpolicy cvt_srv2
```








- Aktualisieren Sie die Maßnahmen auf dem Zielsever, falls erforderlich.  
Tipp: Mithilfe des Operations Center können Sie die Maßnahmen auf dem Zielsever ändern. Führen Sie die Anweisungen in Maßnahmen editieren aus.  
Um beispielsweise inaktive Dateiversionen auf dem Zielsever für einen kürzeren Zeitraum als auf dem Quellenserver aufzubewahren, reduzieren Sie die Einstellung Sicherungen in den Verwaltungsklassen, die für replizierte Clientdaten gelten.
- Ermöglichen Sie dem Zielreplikationsserver die Verwendung seiner Maßnahmen zur Verwaltung der replizierten Clientknotendaten, indem Sie auf dem Quellenserver den Befehl `SET DISSIMILARPOLICIES` ausgeben. Um beispielsweise die Maßnahmen auf dem Zielreplikationsserver `CVT_SRV2` zu aktivieren, geben Sie auf dem Quellenserver den folgenden Befehl aus:

```
set dissimilarpolicies cvt_srv2 on
```

Bei der nächsten Ausführung des Replikationsprozesses werden die Maßnahmen auf dem Zielreplikationsserver zur Verwaltung der replizierten Clientknotendaten verwendet.

Tipp: Wenn Sie die Replikation mithilfe des Operations Center konfigurieren und die Maßnahmen auf dem Quellen- und dem Zielreplikationsserver nicht übereinstimmen, wird die für den Quellenreplikationsserver angegebene Maßnahme verwendet. Wenn die Maßnahmen auf dem Zielreplikationsserver mithilfe des Befehls `SET DISSIMILARPOLICIES` aktiviert wurden, wird die für den Zielreplikationsserver angegebene Maßnahme verwendet. Wenn der Zielreplikationsserver nicht über die von dem Knoten auf dem Quellenreplikationsserver verwendete Maßnahme verfügt, wird die Maßnahme `STANDARD` verwendet.

#### Zugehörige Verweise:

-  [EXPORT POLICY](#) (Maßnahmeninformationen exportieren)
-  [SET DISSIMILARPOLICIES](#) (Maßnahmen auf dem Zielreplikationsserver zum Verwalten replizierter Daten aktivieren)
-  [VALIDATE REPLICATION](#) (Replikation für einen Clientknoten überprüfen)
-  [VALIDATE REPLPOLICY](#) (Maßnahmen auf dem Zielreplikationsserver überprüfen)
-  [AIX-Betriebssysteme](#)  [Linux-Betriebssysteme](#)  [Windows-Betriebssysteme](#)

## Clusterumgebungen konfigurieren




Sie können den IBM Spectrum Protect-Server für das Clustering auf AIX-, Linux- oder Windows-Systemen konfigurieren.

Eine Clusterumgebung kann für die folgenden Betriebssysteme verwendet werden:

- IBM® PowerHA SystemMirror for AIX
- IBM Tivoli System Automation for Multiplatforms for AIX and Linux
- Microsoft Failovercluster für Windows


Sie können andere Clusterprodukte zusammen mit IBM Spectrum Protect verwenden, es ist jedoch keine Dokumentation nur nur eingeschränkte Unterstützung verfügbar. Die neuesten Informationen zur Unterstützung für Clusterumgebungen finden Sie unter <http://www.ibm.com/support/docview.wss?uid=swg21609772>.

Bevor Sie ein anderes Clusterprodukt verwenden, müssen Sie sicherstellen, dass DB2 die erforderlichen Dateisysteme unterstützt. Weitere Informationen zu der von Ihnen verwendeten Version von DB2 finden Sie in der Produktinformation zu DB2, indem Sie nach empfohlenen Dateisystemen suchen.

- Übersicht über die Clusterumgebung  
*Cluster* bestehen aus vielen Komponenten, wie beispielsweise aus IBM Spectrum Protect-Servern, Hardware und Software. Mithilfe des Clustering können Sie zwei oder mehr Server oder Knoten über ein System mit gemeinsamer Plattennutzung verknüpfen.
-  AIX-Betriebssysteme AIX-Umgebung für Clustering konfigurieren  
Sie können den IBM Spectrum Protect-Server für AIX-Clusterumgebungen mithilfe von IBM PowerHA SystemMirror for AIX oder IBM Tivoli System Automation for Multiplatforms konfigurieren.
-  Linux-Betriebssysteme Linux-Umgebung für Clustering konfigurieren  
Sie können den IBM Spectrum Protect-Server unter Linux in einer Clusterumgebung mithilfe von IBM Tivoli System Automation for Multiplatforms Version 3.2.2 konfigurieren.
-  Windows-Betriebssysteme Windows-Clusterumgebung konfigurieren  
Sie können einen IBM Spectrum Protect-Server für Windows in einer Microsoft-Failoverclusterumgebung konfigurieren. Windows-Clusterumgebungen bestehen aus Komponenten, wie beispielsweise IBM Spectrum Protect-Servern, Hardware und Software. Wenn diese Komponenten mit demselben Plattensystem verbunden sind, wird die Ausfallzeit auf ein Mindestmaß reduziert.

#### Zugehörige Informationen:

Upgrade für den Server in einer Clusterumgebung durchführen

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Übersicht über die Clusterumgebung

---

*Cluster* bestehen aus vielen Komponenten, wie beispielsweise aus IBM Spectrum Protect-Servern, Hardware und Software. Mithilfe des Clustering können Sie zwei oder mehr Server oder Knoten über ein System mit gemeinsamer Plattennutzung verknüpfen.

Diese Konfiguration ermöglicht es den Knoten, Daten gemeinsam zu nutzen, was eine höhere Serververfügbarkeit bewirkt und Ausfallzeiten minimiert. Beispiel:

- Sie können Anwendungen und Hardwarekomponenten, die in einem Cluster implementiert sind, konfigurieren, überwachen und steuern.
- Sie können eine Clusterverwaltungsschnittstelle und IBM Spectrum Protect verwenden, um Clusteranordnungen anzugeben und Übernahmemuster zu definieren. Der Server ist Teil des Clusters, das eine zusätzliche Sicherheitsstufe bereitstellt, indem sichergestellt wird, dass keine Transaktionen verloren gehen, da ein Server fehlgeschlagen ist. Durch das von Ihnen definierte Übernahmemuster werden zukünftige Fehler verhindert.
- Sie können Clustering auf den Knotenreplikationsprozess anwenden. Die Serververfügbarkeit ist damit höher als sie es wäre, wenn die Knotenreplikation als eigenständiger Prozess verwendet würde. Die Serververfügbarkeit ist höher, da die Wahrscheinlichkeit der Übernahme eines Clients durch einen anderen Server in einer Clusterumgebung geringer ist. Wenn Sie Daten von mehreren Quellenreplikationsservern auf einen einzigen Zielreplikationsserver replizieren, besteht ein hohes Maß an Abhängigkeit vom Zielreplikationsserver. Durch eine Clusterumgebung wird die Abhängigkeit vom Zielreplikationsserver verringert.

Komponenten in einem Server-Cluster werden als *Clusterobjekte* bezeichnet. Clusterobjekte sind einer Merkmalgruppe mit Datenwerten zugeordnet, die die Identität und das Verhalten eines Objekts im Cluster beschreiben. Clusterobjekte können die folgenden Komponenten umfassen:

- Knoten
- Speicher
- Dienste und Anwendungen
- Netze

Sie verwalten Clusterobjekte, indem Sie deren Merkmale bearbeiten; dies erfolgt normalerweise über eine Clusterverwaltungsanwendung.

- Clusterknoten  
Alle Knoten in einem Cluster haben ähnliche Merkmale; dadurch können sie gemeinsam verwendet werden.

## AIX-Umgebung für Clustering konfigurieren











---

Sie können den IBM Spectrum Protect-Server für AIX-Clusterumgebungen mithilfe von IBM® PowerHA SystemMirror for AIX oder IBM Tivoli System Automation for Multiplatforms konfigurieren.

PowerHA SystemMirror SystemMirror for AIX und Tivoli System Automation erkennen Systemausfälle und steuern die Übernahme durch einen Wiederherstellungsprozessor mit einem minimalen Verlust an Benutzerzeit. Sie können den IBM Spectrum Protect-Server auf einem System in einem PowerHA- oder einem Tivoli System Automation-Cluster konfigurieren. Der IBM Spectrum Protect-Server kann dann bei einem Systemausfall auf einem anderen System im Cluster gestartet werden.

Sowohl bei der Übernahme als auch bei der Rückübertragung sieht es so aus, als würde der IBM Spectrum Protect-Server angehalten und dann erneut gestartet. Alle Transaktionen, die zum Zeitpunkt der Übernahme oder der Rückübertragung aktiv waren, werden rückgängig gemacht; alle abgeschlossenen Transaktionen bleiben abgeschlossen. IBM Spectrum Protect-Clients betrachten die Übernahme oder Rückübertragung als Kommunikationsfehler und versuchen, ihre Verbindungen wiederherzustellen.

Die folgenden Informationen enthalten Details zu diesen Clustering-Optionen.

- Konfigurieren Sie IBM Spectrum Protect for AIX für die Verwendung von IBM PowerHA SystemMirror for AIX in einer Clusterumgebung; lesen Sie dazu die folgenden Abschnitte.
- Konfigurieren Sie IBM Spectrum Protect for AIX für die Verwendung von Tivoli System Automation in einer Clusterumgebung; lesen Sie dazu die Informationen unter <http://www.ibm.com/support/docview.wss?uid=swg27039780>.
- Siehe die Produktinformation zu PowerHA SystemMirror.
-  AIX-Betriebssysteme Anforderungen für einen PowerHA-Cluster  
IBM PowerHA SystemMirror for AIX erkennt Systemausfälle und steuert die Übernahme durch einen Wiederherstellungsprozessor mit einem minimalen Verlust an Benutzerzeit.
-  AIX-Betriebssysteme PowerHA-Übernahme und -Rückübertragung  
Wenn ein Knoten ausfällt, überträgt der Server-Cluster die vom Knoten gehosteten Gruppen auf andere Knoten im Cluster. Dieser Übertragungsprozess wird als *Übernahme* (Failover) bezeichnet. Der gegenteilige Prozess, *Rückübertragung* (Failback), findet statt, wenn der ausgefallene Knoten wieder aktiv wird und die Gruppen, die auf die anderen Knoten übertragen wurden, wieder auf den ursprünglichen Knoten zurückübertragen werden.
-  AIX-Betriebssysteme PowerHA SystemMirror for AIX installieren und konfigurieren  
Sie können den IBM Spectrum Protect-Server für AIX-Clusterumgebungen mithilfe von IBM PowerHA SystemMirror for AIX konfigurieren.
-  AIX-Betriebssysteme IBM Spectrum Protect-Server auf einem Produktionsknoten für PowerHA installieren  
Installieren Sie den IBM Spectrum Protect-Server auf einem Produktionsknoten für PowerHA, um den Server für das Clustering konfigurieren zu können.
-  AIX-Betriebssysteme IBM Spectrum Protect-Client auf einem Produktionsknoten für PowerHA installieren  
Sie müssen nur die Dateigruppe des Clients für Sichern/Archivieren installieren, die die Dateien des Clients für Sichern/Archivieren und den Verwaltungsbefehlszeilenclient enthält.
-  AIX-Betriebssysteme Konfiguration des IBM Spectrum Protect-Servers für PowerHA überprüfen  
Wenn Sie den IBM Spectrum Protect-Server für die Verwendung von PowerHA konfigurieren, müssen Sie die Konfiguration überprüfen.
-  AIX-Betriebssysteme Standby-Knoten für PowerHA konfigurieren  
Stellen Sie für PowerHA vor dem Konfigurieren des Standby-Knotens sicher, dass der IBM Spectrum Protect-Server nicht auf dem Produktionsknoten ausgeführt wird.
-  AIX-Betriebssysteme Speichereinheiten für austauschbare Datenträger für AIX für PowerHA definieren  
Für ein Betriebssystem AIX müssen Sie die Speichereinheiten für austauschbare Datenträger definieren, die von IBM Spectrum Protect auf den Produktions- und Standby-Knoten verwendet werden. Der Speicherarchivmanager überprüft, ob sich die Kassette, die die Speichereinheit für austauschbare Datenträger enthält, im korrekten Laufwerk befindet.
-  AIX-Betriebssysteme Cluster-Manager- und IBM Spectrum Protect-Konfigurationen ausführen  
Aktualisieren Sie die Konfiguration des Cluster-Managers, um den IBM Spectrum Protect-Server als eine Anwendung und eine Übernahmeressource des Standby-Knotens zu definieren. Der Produktionsknoten ist Eigner dieser Anwendung.
-  AIX-Betriebssysteme Fehlerbehebung in der PowerHA-Clusterumgebung  
Die folgende Liste enthält Informationen zur Behebung häufig auftretender Fehler. Die Informationen, die für IBM PowerHA SystemMirror for AIX bereitgestellt werden, repräsentieren nicht alle möglichen Szenarios.

## Anforderungen für einen PowerHA-Cluster


---

IBM PowerHA SystemMirror for AIX erkennt Systemausfälle und steuert die Übernahme durch einen Wiederherstellungsprozessor mit einem minimalen Verlust an Benutzerzeit.

Für die Konfiguration des IBM Spectrum Protect-Servers gelten die folgenden Hardwarevoraussetzungen:

- Eine Hardwarekonfiguration, die für PowerHA geeignet ist. Die Speichereinheiten für austauschbare Datenträger des IBM Spectrum Protect-Servers müssen physisch mit mindestens zwei Knoten des PowerHA-Clusters an einem gemeinsam genutzten Bus (einschließlich eines Speicherbereichsnetzes) verbunden sein.
- Ausreichend gemeinsam genutzter Plattenspeicherplatz zum Speichern der IBM Spectrum Protect-Datenbank, der Wiederherstellungsprotokolle, des Instanzverzeichnisses und der Plattenspeicherpools, die verwendet werden sollen. Informationen zur Bestimmung, wie viel Speicherplatz für die Datenbank und das Wiederherstellungsprotokoll erforderlich ist, um die Verfügbarkeit der Datenbank und des Wiederherstellungsprotokolls sicherzustellen, finden Sie in Bestandskapazität verwalten.
- Ein TCP/IP-Netz

Tipp: Wenn ein IBM Spectrum Protect-Server Speichereinheiten für austauschbare Datenträger verwaltet, können Sie zwei IBM Spectrum Protect-Server konfigurieren, die auf verschiedenen Systemen in einem PowerHA-Cluster ausgeführt werden. Jedes System kann beide Server ausführen, wenn das andere System ausfällt. Um zwei IBM Spectrum Protect-Server für die Ausführung auf unterschiedlichen Systemen in einem PowerHA-Cluster zu konfigurieren, müssen Sie ein anderes Dateisystem verwenden, auf das beide Server zugreifen können.

 AIX-Betriebssysteme

## PowerHA-Übernahme und -Rückübertragung

---

Wenn ein Knoten ausfällt, überträgt der Server-Cluster die vom Knoten gehosteten Gruppen auf andere Knoten im Cluster. Dieser Übertragungsprozess wird als *Übernahme* (Failover) bezeichnet. Der gegenteilige Prozess, *Rückübertragung* (Failback), findet statt, wenn der ausgefallene Knoten wieder aktiv wird und die Gruppen, die auf die anderen Knoten übertragen wurden, wieder auf den ursprünglichen Knoten zurückübertragen werden.

Die Begriffe *Produktionsknoten* und *Standby-Knoten* beziehen sich auf die beiden PowerHA-Knoten, auf denen der IBM Spectrum Protect-Server ausgeführt wird.


PowerHA handhabt die Übernahme der TCP/IP-Adresse und das Laden des gemeinsam genutzten Dateisystems auf den Standby-Knoten bzw. auf den Produktionsknoten.

Wenn eine *Übernahme* oder eine *Rückübertragung* erfolgt, werden alle Transaktionen, die zu diesem Zeitpunkt gerade verarbeitet werden, rückgängig gemacht. Für IBM Spectrum Protect-Clients stellt die *Übernahme* oder *Rückübertragung* einen Kommunikationsfehler dar. Daher müssen Sie wieder eine Verbindung herstellen, die auf den Einstellungen für die Optionen COMMRESTARTDURATION und COMMRESTARTINTERVAL basiert.

In der Regel können Sie den Client für Sichern/Archivieren von der letzten festgeschriebenen Transaktion aus erneut starten. Wenn ein Clientzeitplan ausgeführt wird, wenn eine *Übernahme* erfolgt, schlägt die Clientoperation wahrscheinlich fehl. Wenn Sie Clientoperationen erneut starten können, muss dies ab dem Anfang der Verarbeitung erfolgen. Die Client- und Agentenoperationen werden so ausgeführt, wie dies normalerweise der Fall wäre, wenn der Server angehalten und erneut gestartet worden wäre, während der Client und die Agenten verbunden waren. Der einzige Unterschied besteht darin, dass der Server physisch auf anderer Hardware erneut gestartet wird.

Wenn keine automatische *Rückübertragung* erfolgen soll, können Sie die Ressource als kaskadierende Ressourcengruppe ohne *Rückübertragung* konfigurieren.




### Zugehörige Informationen:


 Produktinformation zu PowerHA SystemMirror

## PowerHA SystemMirror for AIX installieren und konfigurieren

---

Sie können den IBM Spectrum Protect-Server für AIX-Clusterumgebungen mithilfe von IBM® PowerHA SystemMirror for AIX konfigurieren.

-  AIX-Betriebssysteme PowerHA-Cluster installieren und konfigurieren  
Möglicherweise treten Verarbeitungsfehler auf, wenn die Installation und Konfiguration von IBM PowerHA SystemMirror for AIX nicht ordnungsgemäß ausgeführt wird.
-  AIX-Betriebssysteme IBM Spectrum Protect-Server auf dem Primärknoten für PowerHA konfigurieren  
Sie können eine IBM Spectrum Protect-Serverinstanz auf dem Primärknoten konfigurieren.
-  AIX-Betriebssysteme IBM Spectrum Protect-Server auf einem Sekundärknoten für PowerHA mit einer gemeinsam genutzten DB2-Instanz konfigurieren  
Wenn das DB2-Instanzverzeichnis von den Knoten im PowerHA-Cluster gemeinsam genutzt wird, müssen Sie keine DB2-Instanz auf dem Sekundärknoten erstellen. Der Assistent dsmicfgx wird nicht ausgeführt.

-  AIX-Betriebssysteme IBM Spectrum Protect-Server auf einem Sekundärknoten für PowerHA mit einer separaten DB2-Instanz konfigurieren  
Sie müssen eine DB2-Instanz auf jedem Sekundärknoten erstellen, wenn das DB2-Instanzverzeichnis (/home/tsminst1/sqllib) von den Knoten im PowerHA-Cluster nicht gemeinsam genutzt wird.

 AIX-Betriebssysteme

## PowerHA-Cluster installieren und konfigurieren

---

Möglicherweise treten Verarbeitungsfehler auf, wenn die Installation und Konfiguration von IBM PowerHA SystemMirror for AIX nicht ordnungsgemäß ausgeführt wird.

### Vorgehensweise

---

Führen Sie die folgenden Schritte aus, um den PowerHA-Cluster zu installieren und zu konfigurieren:

1. Definieren Sie die gemeinsam genutzten Dateisysteme und logischen Datenträger, wenn sie benötigt werden. Möglicherweise sollen Dateien aufgrund von Integritäts- oder Leistungsaspekten in separate Dateisysteme oder auf separate physische Platten gestellt werden. Stellen Sie das Ausgangsverzeichnis der Benutzerinstanz nicht auf eine gemeinsam genutzte Platte. Spiegeln Sie die logischen Datenträger (einschließlich der zu Grunde liegenden Dateisysteme), um maximale Verfügbarkeit bereitzustellen. Die Dateisysteme, die definiert werden müssen, umfassen das Instanzverzeichnis des IBM Spectrum Protect-Servers, die Datenbank- und Protokollverzeichnisse, alle Verzeichnisse für Plattenspeicherpools und Verzeichnisse für Speicherpools des Einheitentyps FILE.
2. Konfigurieren Sie PowerHA derart, dass der Produktionsknoten Eigner der gemeinsam genutzten Datenträgergruppen ist und der Standby-Knoten die gemeinsam genutzten Datenträgergruppen übernimmt, wenn der Produktionsknoten ausfällt.
3. Konfigurieren Sie PowerHA derart, dass auch für die Dateisysteme eine Übernahme erfolgt.
4. Definieren Sie eine Service-IP-Adresse für den IBM Spectrum Protect-Server. Die Service-IP-Adresse darf nicht mit einer der Host-IP-Adressen übereinstimmen. Die Service-IP-Adresse und nicht die tatsächliche Host-IP-Adresse wird von Host zu Host versetzt.
5. Führen Sie eine Übernahme für die gemeinsam genutzte Datenbank und die Protokoll- und Instanzverzeichnisse auf den Standby-Knoten des PowerHA-Clusters durch.

### Ergebnisse

---

Sie müssen die Speichereinheiten für austauschbare Datenträger für die Übernahme konfigurieren und den IBM Spectrum Protect-Server als Anwendung für PowerHA definieren.

 AIX-Betriebssysteme

## IBM Spectrum Protect-Server auf dem Primärknoten für PowerHA konfigurieren

---

Sie können eine IBM Spectrum Protect-Serverinstanz auf dem Primärknoten konfigurieren.


### Vorgehensweise

---

1. Lesen Sie die Abschnitte in den Informationen zum Konfigurieren des IBM Spectrum Protect-Servers.
2. Nach dem Konfigurieren der IBM Spectrum Protect-Serverinstanz auf dem Primärknoten können Sie den IBM Spectrum Protect-Server auf einem Sekundärknoten konfigurieren.

#### Zugehörige Tasks:

IBM Spectrum Protect-Serverinstanz konfigurieren

 AIX-Betriebssysteme

## IBM Spectrum Protect-Server auf einem Sekundärknoten für PowerHA mit einer gemeinsam genutzten DB2-Instanz konfigurieren

---

Wenn das DB2-Instanzverzeichnis von den Knoten im PowerHA-Cluster gemeinsam genutzt wird, müssen Sie keine DB2-Instanz auf dem Sekundärknoten erstellen. Der Assistent dsmicfgx wird nicht ausgeführt.

### Vorgehensweise

---

Um eine Serverinstanz auf dem Sekundärknoten mit einer gemeinsam genutzten DB2-Instanz zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Fügen Sie auf jedem Knoten im Cluster dem Script `/opt/tivoli/tsm/server/bin/rc.dsmserv` den folgenden Text hinzu:

```
DB2NODES_TEMP='/tmp/db2nodes.tmp'
DB2NODES=${homeDir}/sqlllib/db2nodes.cfg
# Aktueller Hostname
HOSTNAME=$(/bin/Hostname)
# Hostname in db2nodes.cfg gespeichert
DB2_HOST=$(cat $DB2NODES | cut -d ' ' -f 2)
# Bei unterschiedlichen Namen die Datei aktualisieren
if [[ "$HOSTNAME" != "$DB2_HOST" ]]
then
    echo "Hostname in db2nodes.cfg wird aktualisiert"
    sed -e s ${DB2_HOST} ${HOSTNAME}_g $DB2NODES > $DB2NODES_TEMP
    cp $DB2NODES_TEMP $DB2NODES
fi
```

Tipp: Wenn der Text nicht in das Script eingeschlossen wird, können Sie ihn vor der Ausgabe des Scripts `/opt/tivoli/tsm/server/bin/rc.dsmserv` einfügen.

2. Versetzen Sie alle gemeinsam genutzten Ressourcen auf den Sekundärknoten.
3. Aktualisieren Sie im Script `/opt/tivoli/tsm/server/bin/startserver` die folgenden Variablen unter Angabe dieser Werte:

Tabelle 1. Variablen im Script `/opt/tivoli/tsm/server/bin/startserver`

| Beschreibung  | Variablen   | Beispiel   |
|---|-------------|--|
| Setzen Sie INST_USER auf die Instanzbenutzer-ID.  | INST_USER   | INST_USER='tsmuser1'   |
| Setzen Sie INST_DIR auf die Position des IBM Spectrum Protect-Instanzverzeichnisses. Dieses Verzeichnis enthält dsmserv.dbid und dsmserv.opt.   | INST_DIR    | INST_DIR='/home/tsmuser1/tsminst1'   |
| Wählen Sie eine der folgenden Startoptionen aus:<br><br>Option 1 - Instanz verwenden:<br><br>\$INST_USER, führen Sie den Server jedoch als Root (-U) aus.<br><br>Option 2 - Instanz verwenden:<br><br>\$INST_USER und führen Sie den Server als \$INST_USER (-u) aus. | INST_OPTION | Option 1:<br><br>INST_OPTION='-U \$INST_USER'<br><br>Option 2:<br><br>INST_OPTION='-u \$INST_USER' |

4. Starten Sie den Server, indem Sie das folgende Script ausgeben:

```
/opt/tivoli/tsm/server/bin/startserver
```

5. Geben Sie nach dem Starten des Servers den Befehl `BACKUP DB` aus, um sicherzustellen, dass die Daten erfolgreich gesichert werden.



## IBM Spectrum Protect-Server auf einem Sekundärknoten für PowerHA mit einer separaten DB2-Instanz konfigurieren

Sie müssen eine DB2-Instanz auf jedem Sekundärknoten erstellen, wenn das DB2-Instanzverzeichnis (`/home/tsminst1/sqllib`) von den Knoten im PowerHA-Cluster nicht gemeinsam genutzt wird.

### Informationen zu diesem Vorgang

Sie können den IBM Spectrum Protect-Server auf einem Sekundärknoten mithilfe des Assistenten `dsmicfgx` oder manuell konfigurieren.

### Vorgehensweise

- Um eine DB2-Instanz auf einem Sekundärknoten mithilfe des Assistenten `dsmicfgx` zu erstellen, führen Sie die folgenden Schritte aus:
  1. Führen Sie den Assistenten `dsmicfgx` aus.
  2. Wählen Sie in der Anzeige Instanzverzeichnis das Kontrollkästchen Aktivieren, wenn Sie die Serverinstanz auf einem Sekundärknoten eines Clusters mit hoher Verfügbarkeit konfigurieren aus.

- Um eine DB2-Instanz manuell auf einem Sekundärknoten zu erstellen, führen Sie die folgenden Schritte aus:
  - Versetzen Sie alle gemeinsam genutzten Ressourcen auf den Sekundärknoten.
  - Erstellen Sie eine DB2-Instanz, indem Sie den folgenden Befehl db2icrt ausgeben:

```
/opt/tivoli/tsm/db2/instance/db2icrt -s ese -u Instanzbenutzer Instanzbenutzer
```

Dabei ist *Instanzbenutzer* derselbe Benutzer, der auch Eigner der DB2-Instanz auf dem Primärknoten ist.

- Melden Sie sich nach dem Erstellen der DB2-Instanz als Instanzbenutzer an oder geben Sie den Befehl su aus:

```
su - <Instanzbenutzer>
```

- Geben Sie als Instanzbenutzer die folgenden Befehle aus:

```
db2start
db2 update dbm cfg using DFTDBPATH gemeinsam_genutzter_Datenbankpfad
db2 catalog db TSMDB1
db2stop
```

Dabei ist *gemeinsam\_genutzter\_Datenbankpfad* das gemeinsam genutzte Datenbankverzeichnis. Das gemeinsam genutzte Datenbankverzeichnis ist normalerweise das Serverinstanzverzeichnis.

Tipp: Um den Wert für *gemeinsam\_genutzter\_Datenbankpfad* zu bestimmen, geben Sie auf dem Primärknoten den folgenden Befehl aus:

```
db2 get dbm cfg | grep DFTDBPATH
```

- Aktualisieren Sie im Script `/opt/tivoli/tsm/server/bin/startserver` die folgenden Variablen unter Angabe dieser Werte:

Tabelle 1. Variablen im Script `/opt/tivoli/tsm/server/bin/startserver`

| Beschreibung  | Variab<br>le    | Beispiel   |
|---|-----------------|--|
| Setzen Sie INST_USER auf die Instanzbenutzer-ID.  | INST_U<br>SER   | INST_USER='tsmuser1'<br>'  |
| Setzen Sie INST_DIR auf die Position des IBM Spectrum Protect-Instanzverzeichnisses. Dieses Verzeichnis enthält dmserv.dbid und dmserv.opt.   | INST_D<br>IR    | INST_DIR='/home/tsm<br>user1/tsminst1'   |
| Wählen Sie eine der folgenden Startoptionen aus:<br><br>Option 1 - Instanz verwenden:<br><br>\$INST_USER, führen Sie den Server jedoch als Root (-U) aus.<br><br>Option 2 - Instanz verwenden:<br><br>\$INST_USER und führen Sie den Server als \$INST_USER (-u) aus. | INST_O<br>PTION | Option 1:<br><br>INST_OPTION='-U<br>\$INST_USER'<br><br>Option 2:<br><br>INST_OPTION='-u<br>\$INST_USER' |

- Starten Sie den Server, indem Sie das folgende Script ausgeben:

```
/opt/tivoli/tsm/server/bin/startserver
```

- Geben Sie nach dem Starten des Servers den Befehl BACKUP DB aus, um sicherzustellen, dass die Daten erfolgreich gesichert werden.



## IBM Spectrum Protect-Server auf einem Produktionsknoten für PowerHA installieren

Installieren Sie den IBM Spectrum Protect-Server auf einem Produktionsknoten für PowerHA, um den Server für das Clustering konfigurieren zu können.

### Vorgehensweise

Führen Sie die folgenden Schritte aus, um den IBM Spectrum Protect-Server auf dem Produktionsknoten zu installieren:

- Installieren Sie IBM Spectrum Protect. Wählen Sie eine der folgenden Komponenten aus:
  - Den IBM Spectrum Protect-Server
  - Den IBM Spectrum Protect-Einheitentreiber, falls erforderlich
  - Die IBM Spectrum Protect-Lizenz



Die ausführbaren Dateien werden normalerweise auf den internen Platten des Produktionsknotens installiert, nicht in dem gemeinsam genutzten IBM Spectrum Protect-Plattenspeicher. Die ausführbaren Dateien des IBM Spectrum Protect-Servers werden im Verzeichnis /opt/tivoli/tsm/server/bin installiert.

2. Konfigurieren Sie IBM Spectrum Protect für die Verwendung der TCP/IP-Übertragungsmethode. Anweisungen finden Sie in den Informationen zur Konfiguration einer Serverinstanz in AIX: Erste Schritte nach der Installation von IBM Spectrum Protect.
3. Definieren Sie eine neue Benutzer-ID als Eigner der IBM Spectrum Protect-Serverinstanz oder verwenden Sie eine vorhandene Benutzer-ID, die noch nicht Eigner einer IBM Spectrum Protect-Instanz ist. Während Sie mit der Instanzbenutzer-ID angemeldet sind, führen Sie die folgenden Schritte aus:
  - a. Erstellen Sie mit dem Befehl mkdir ein Instanzverzeichnis in einem gemeinsam genutzten Dateisystem, für das die Übernahme durch das Standby-System möglich ist. Diese Platte muss für PowerHA definiert sein.
  - b. Erstellen Sie mit dem Befehl mkdir die Datenbank- und Protokollverzeichnisse in gemeinsam genutzten Dateisystemen, für die eine Übernahme durch das Standby-System möglich ist. Diese Platten müssen auch für PowerHA für die Übernahme definiert sein.
  - c. Schließen Sie die Konfiguration mithilfe des Assistenten dsmdir ab.

#### Zugehörige Tasks:

AIX: Server installieren

Upgrade für den Server durchführen

 AIX-Betriebssysteme

## IBM Spectrum Protect-Client auf einem Produktionsknoten für PowerHA installieren

---

Sie müssen nur die Dateigruppe des Clients für Sichern/Archivieren installieren, die die Dateien des Clients für Sichern/Archivieren und den Verwaltungsbefehlszeilenclient enthält.

### Vorgehensweise

---

Detaillierte Anweisungen zum Installieren des IBM Spectrum Protect-Clients finden Sie in IBM Spectrum Protect-Clients für Sichern/Archivieren installieren.

Führen Sie die folgenden Schritte aus, um den IBM Spectrum Protect-Client auf dem Produktionsknoten zu installieren.

1. Installieren Sie die ausführbaren Dateien des IBM Spectrum Protect-Clients im Verzeichnis /usr/tivoli/tsm/client/ba/bin. Diese Dateien werden normalerweise auf den internen Platten des Produktionsknotens installiert.
2. Damit der Client den Server finden kann, müssen Sie sicherstellen, dass die Clientoptionsdatei, dsm.sys, auf den IBM Spectrum Protect-Server verweist. Der Servername in dsm.sys wird nur im Parameter -servername des Befehls dsmdir verwendet, um den Server anzugeben, auf den zugegriffen werden soll.

 AIX-Betriebssysteme

## Konfiguration des IBM Spectrum Protect-Servers für PowerHA überprüfen

---

Wenn Sie den IBM Spectrum Protect-Server für die Verwendung von PowerHA konfigurieren, müssen Sie die Konfiguration überprüfen.

### Informationen zu diesem Vorgang

---

Wenn Sie PowerHA verwenden, müssen sich alle Datenbank-, Protokoll-, Speicher- und Instanzverzeichnisse auf gemeinsam genutzten Platten befinden, die für die Übernahme durch PowerHA konfiguriert sind.

### Vorgehensweise

---

Um die Verzeichnisse zu identifizieren, die sich auf gemeinsam genutzten Platten befinden, führen Sie die folgenden Schritte aus:

1. Melden Sie sich als der Instanzbenutzer an.
2. Führen Sie das Script /opt/tivoli/tsm/server/bin/dsmclustfs aus.
3. Prüfen Sie die Dateisysteme, die von dem Script zurückgemeldet werden, und stellen Sie sicher, dass sie sich auf gemeinsam genutzten Platten befinden. Das folgende Beispielscript zeigt, welchen Typ von Informationen Sie überprüfen müssen:

```
> su - tsminstl
$ /opt/tivoli/tsm/server/bin/dsmclustfs
SQL1026N Der Datenbankmanager ist bereits aktiv.
```

Die folgenden Datenbankverbindungsinformationen werden angezeigt, wenn der IBM Spectrum Protect-Server die Verbindung zur DB2-Datenbank herstellt:

```
DB20000I Der Befehl START DATABASE MANAGER wurde erfolgreich ausgeführt.
```

Datenbankverbindungsinformationen

```
Datenbankserver           = DB2/AIX64 11.1.0
SQL-Berechtigungs-ID     = TSMINST1
Aliasname der lokalen Datenbank = TSMDB1
```

```
Dateisysteme, die für die DB2-Datenbank erforderlich sind: /TSMdbspace2 /TSMdbspace1
Dateisystem, das für die aktive Protokolldatei erforderlich ist: /TSMalog
Dateisystem, das für das Archivprotokoll erforderlich ist: /TSMarchlog
Spiegel der aktiven Protokolldatei für diese Datenbank nicht definiert
```

Das Script enthält die folgenden obligatorischen DB2-Dateisysteme:

```
/TSMdb-1 /TSMalog-1 /TSMarchlog-1
```

```
Plattenbasierte TSM-Datenträger werden überprüft...
TSM-Daten sind in den folgenden Dateisystemen gespeichert: /TSMdisk-1 /TSMfile-1
```

 AIX-Betriebssysteme

## Standby-Knoten für PowerHA konfigurieren

---

Stellen Sie für PowerHA vor dem Konfigurieren des Standby-Knotens sicher, dass der IBM Spectrum Protect-Server nicht auf dem Produktionsknoten ausgeführt wird.

### Vorgehensweise

---


Führen Sie die folgenden Schritte aus, um den Standby-Knoten zu konfigurieren:

1. Öffnen Sie auf dem Standby-Knoten die gemeinsam genutzte Datenträgergruppe und alle IBM Spectrum Protect-Dateisysteme.
2. Installieren Sie den IBM Spectrum Protect-Produktcode auf dem Standby-Knoten. Weitere Informationen finden Sie in IBM Spectrum Protect-Server auf einem Produktionsknoten für PowerHA installieren. Wenn die ausführbaren Dateien im gemeinsam genutzten Plattenspeicher installiert werden, müssen Sie die Dateien möglicherweise auf dem Standby-Knoten installieren. IBM Spectrum Protect-Einheitentreiber, SMIT-Anzeigen und andere Dateien müssen in AIX-Systemverzeichnissen installiert werden.
3. Öffnen Sie den Assistenten dsmicfgx. Befolgen Sie die Anweisungen, um die Konfiguration abzuschließen. Wählen Sie das Kontrollkästchen aus, um anzugeben, dass es sich hierbei um einen Sekundärknoten im Cluster handelt.
4. Starten Sie den Server auf dem Standby-Knoten. Fragen Sie die Datenbank, das Wiederherstellungsprotokoll und die Speicherpooldatenträger ab, um zu prüfen, ob sie mit denen beim Starten des Servers auf dem Produktionsknoten übereinstimmen.
5. Installieren Sie den Client auf dem Standby-Knoten. Wenn die ausführbaren Dateien im gemeinsam genutzten Plattenspeicher installiert werden, müssen Sie die Dateien möglicherweise auf dem Standby-Knoten installieren. IBM Spectrum Protect, SMIT-Anzeigen und andere Dateien müssen in AIX-Systemverzeichnissen installiert werden. Verwenden Sie den AIX-Befehl RCP mit der Option -p, um die Datei dsm.sys vom Produktionsknoten auf den Standby-Knoten zu kopieren. Wird die Datei dsm.sys auf einem Knoten geändert, muss sie auf den anderen Knoten kopiert werden.

### Ergebnisse

---

Tipp: Wird die Datei dsm.sys auf einem Knoten geändert, müssen Sie die Datei auf den anderen Knoten kopieren.

 AIX-Betriebssysteme

## Speichereinheiten für austauschbare Datenträger für AIX for PowerHA definieren

---

Für ein Betriebssystem AIX müssen Sie die Speichereinheiten für austauschbare Datenträger definieren, die von IBM Spectrum Protect auf den Produktions- und Standby-Knoten verwendet werden. Der Speicherarchivmanager überprüft, ob sich die Kassette, die die Speichereinheit für austauschbare Datenträger enthält, im korrekten Laufwerk befindet.

### Informationen zu diesem Vorgang


---

Voraussetzung:

- Wenn Sie einen Speicherarchivmanagerserver definieren, der nicht gemeinsam mit dem IBM Spectrum Protect-Server genutzt wird, müssen Sie sicherstellen, dass der Parameter RESETDRIVES für den Befehl DEFINE LIBRARY oder den Befehl UPDATE LIBRARY YES lautet. Wenn Sie einen Speicherarchivmanagerserver definieren, der gemeinsam mit dem IBM Spectrum Protect-Server genutzt wird, muss die Option SANDISCOVERY in der IBM Spectrum Protect-Serveroptionsdatei dsmserv.opt auf ON gesetzt werden. Standardmäßig ist diese Option auf OFF gesetzt.
- Sie können den Befehl PERFORM LIBACTION für die Speicherarchivtypen SCSI und VTL ausgeben. Verwenden Sie diesen Befehl, um die Laufwerke und Pfade für ein Speicherarchiv in einem einzigen Schritt zu definieren.

Wenn die SAN-Einheitenzuordnung korrekt ist, fahren Sie mit Cluster-Manager- und IBM Spectrum Protect-Konfigurationen ausführen fort. Wenn die Einheitenamen auf dem primären und dem sekundären System nicht übereinstimmen, müssen Sie die SAN-Erkennung verwenden, damit der IBM Spectrum Protect-Server auf die Einheiten zugreifen kann.

#### Zugehörige Tasks:

 Gemeinsame Speicherarchivnutzung konfigurieren (Version 7.1.1)

#### Zugehörige Verweise:

DEFINE LIBRARY (Speicherarchiv definieren)


UPDATE LIBRARY (Speicherarchiv aktualisieren)

PERFORM LIBACTION (Alle Laufwerke und Pfade für ein Speicherarchiv definieren oder löschen)

SANDISCOVERY

#### Zugehörige Informationen:

 Von IBM Spectrum Protect unterstützte Einheiten

 AIX-Betriebssysteme

## Cluster-Manager- und IBM Spectrum Protect-Konfigurationen ausführen

Aktualisieren Sie die Konfiguration des Cluster-Managers, um den IBM Spectrum Protect-Server als eine Anwendung und eine Übernahmeressource des Standby-Knotens zu definieren. Der Produktionsknoten ist Eigner dieser Anwendung.

### Informationen zu diesem Vorgang

Sie können Befehle von IBM® PowerHA SystemMirror for AIX oder Tivoli System Automation ausgeben, um den Cluster zu konfigurieren. Fahren Sie mit der Konfiguration des IBM Spectrum Protect-Servers fort.

#### Zugehörige Informationen:

 Produktinformation zu PowerHA SystemMirror

 Produktinformation zu IBM Tivoli System Automation for Multiplatforms Version 3.2.2

 AIX-Betriebssysteme

## Fehlerbehebung in der PowerHA-Clusterumgebung

Die folgende Liste enthält Informationen zur Behebung häufig auftretender Fehler. Die Informationen, die für IBM® PowerHA SystemMirror for AIX bereitgestellt werden, repräsentieren nicht alle möglichen Szenarios.

Warnungen, die nach der Ausführung des Dienstprogramms clverify ausgegeben werden

Sie können das PowerHA-Clusterprüfdienstprogramm clverify auf einem einzelnen Knoten ausführen, um die Clusterkonfiguration und die Zuordnung in den PowerHA-Ressourcen zu überprüfen. Wenn Sie das Dienstprogramm clverify nach der Definition des IBM Spectrum Protect-Servers als PowerHA-Anwendung ausführen, werden Warnungen ausgegeben.

Warnungen werden angezeigt, da sich die Shell-Skripts, mit denen die IBM Spectrum Protect-Server gestartet und gestoppt werden, in einem gemeinsam genutzten Dateisystem befinden. Die Shell-Skripts können jeweils nur auf einem einzigen Knoten ausgeführt werden. Daher können die Shell-Skripts jeweils nur auf einem Knoten verfügbar sein. Sie können die Warnungen des Dienstprogramms clverify ignorieren. Kann ein gemeinsam genutztes Dateisystem nicht angehängt werden, kann der IBM Spectrum Protect-Server nicht gestartet werden.

IBM Spectrum Protect-Server wird nach dem Ausgeben des Scripts startserver nicht gestartet

Wenn Sie das Shell-Skript startserver verwenden und PowerHA den IBM Spectrum Protect-Server nicht starten kann, starten Sie ihn manuell an einem Terminal ohne Angabe der Option 'quiet'. Wenn der Server mit der Option 'quiet' ausgeführt werden soll, geben Sie den Befehl dsmserv -q aus.

Nachrichten, die dem Befehl tctl zugeordnet sind

Wenn Sie den Befehl tctl -f/dev/rmt2 rewind ausgeben, kann die folgende Nachricht angezeigt werden:

```
/dev/rmt2: A device is already mounted or cannot be unmounted
```

Diese Nachricht gibt an, dass die E/A-Einheit mit einem Befehl SCSI RESERVE durch ein anderes System als das System gesperrt wird, auf dem der Befehl tctl ausgeführt wurde. Wenn Sie die persistente Reservierung verwenden, stellt der IBM Spectrum

Protect-Server die Laufwerkreservierung standardmäßig zurück. Wenn der Einheitentreiber keine persistente Reservierung verwendet, führt der Server eine Zurücksetzung des Ziels aus.

Nachricht ANS4329S Server hat keinen Datenspeicherbereich mehr








Wenn die Nachricht ANS4329S Server hat keinen Datenspeicherbereich mehr auf einem IBM Spectrum Protect-Client angezeigt wird, ist die Lizenz für den IBM Spectrum Protect-Server möglicherweise nicht konform. Geben Sie den Befehl QUERY LICENSE aus, um die Konformitätsinformationen für die Lizenz anzuzeigen. Wenn der Konformitätsstatus gültig ist, geben Sie den Befehl QUERY ACTLOG auf dem Server aus und überprüfen Sie die angezeigten Nachrichten, um das Problem zu bestimmen.

 Linux-Betriebssysteme

## Linux-Umgebung für Clustering konfigurieren

---

Sie können den IBM Spectrum Protect-Server unter Linux in einer Clusterumgebung mithilfe von IBM® Tivoli System Automation for Multiplatforms Version 3.2.2 konfigurieren.

-  **Übersicht über einen IBM Spectrum Protect-Cluster mit zwei Knoten, der Tivoli System Automation verwendet**  
Verwenden Sie den Tivoli System Automation-Cluster, um eine höherer Server- und Datenbankverfügbarkeit während eines Fehlers zu gewährleisten. Mithilfe der Übernahmefunktion von Tivoli System Automation können Serverkomponenten wie beispielsweise die Datenbank nach einem Fehler automatisch wiederhergestellt werden.
-  **IBM Spectrum Protect-Cluster mit Tivoli System Automation konfigurieren**  
Sie müssen den IBM Spectrum Protect-Cluster konfigurieren, um Tivoli System Automation verwenden zu können.
-  **Voraussetzungen zum Konfigurieren einer Linux-Clusterumgebung mit Tivoli System Automation**  
Bevor Sie IBM Spectrum Protect in einer Clusterumgebung mit Tivoli System Automation installieren und konfigurieren, müssen Sie die Voraussetzungen überprüfen.
-  **IBM Spectrum Protect-Komponenten auf den Primär- und Sekundärknoten installieren und konfigurieren**  
Sie müssen die IBM Spectrum Protect-Server- und -Datenbankkomponenten auf den Primär- und Sekundärknoten im Cluster installieren. Konfigurieren Sie anschließend zunächst den Primärknoten und dann den Sekundärknoten.
-  **Tivoli System Automation auf den Primär- und Sekundärknoten installieren**  
Nachdem Sie IBM Spectrum Protect auf den Primär- und Sekundärknoten im Cluster installiert und konfiguriert haben, müssen Sie Tivoli System Automation auf diesen Knoten installieren und konfigurieren. Anschließend müssen Sie diese Knoten für die Domäne aktivieren, die Ressourcen konfigurieren und die Basismaßnahme aktivieren. Abschließend müssen Sie den IBM Spectrum Protect-Verzeichnissen die Mountpunkte hinzufügen.
-  **Speicherressourcen konfigurieren**  
Verwenden Sie die Tivoli System Automation-Benutzerschnittstelle, oder -Befehlszeile, um Speicherressourcen hinzuzufügen oder zu löschen und um Mountpunkte, die nicht mehr benötigt werden, zu löschen. Wenn Sie dem Cluster einen Speicherpool hinzufügen, müssen Sie den Speicherpool der Ressourcengruppe hinzufügen. Wenn Sie einen Speicherpool aus dem Cluster entfernen, müssen Sie den Speicherpool auch aus der Ressourcengruppe löschen.
-  **Upgrade für einen Server durchführen, der mit Tivoli System Automation konfiguriert ist**  
Sie können ein Upgrade für einen Server der Version 6.3 oder Version 7.1 durchführen, der mit Tivoli System Automation konfiguriert ist.

 Linux-Betriebssysteme

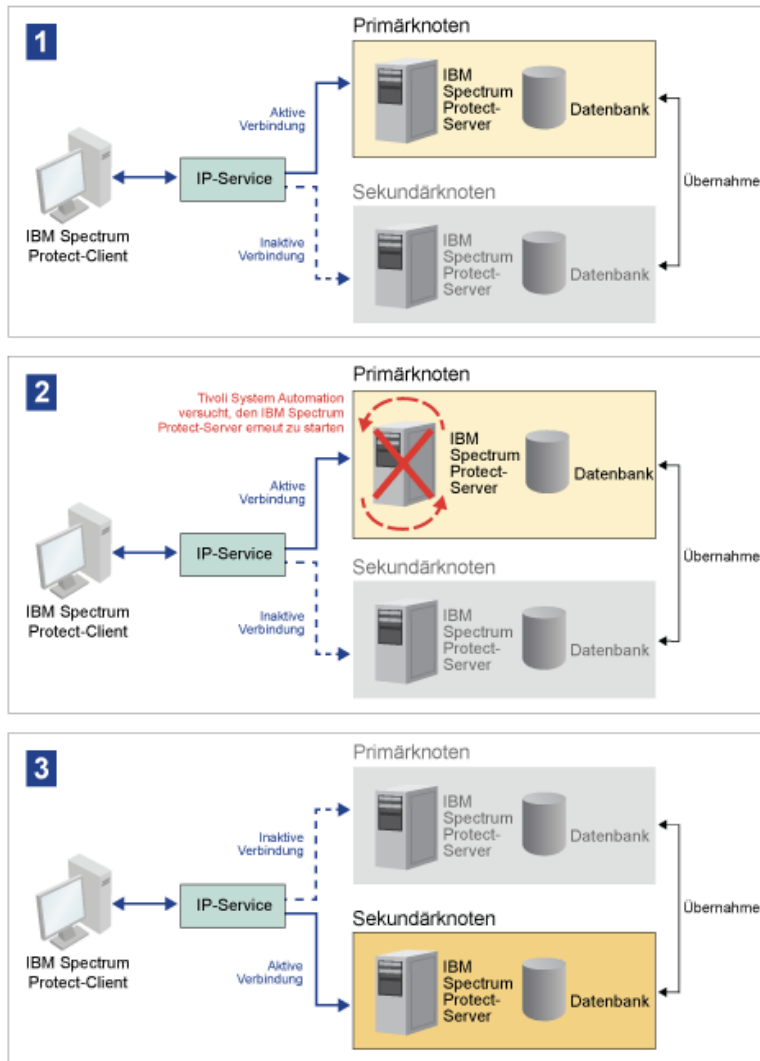
## Übersicht über einen IBM Spectrum Protect-Cluster mit zwei Knoten, der Tivoli System Automation verwendet

---

Verwenden Sie den Tivoli System Automation-Cluster, um eine höherer Server- und Datenbankverfügbarkeit während eines Fehlers zu gewährleisten. Mithilfe der Übernahmefunktion von Tivoli System Automation können Serverkomponenten wie beispielsweise die Datenbank nach einem Fehler automatisch wiederhergestellt werden.

Der IBM Spectrum Protect-Server und die DB2-Datenbank sind die zu Grunde liegenden Serverkomponenten für diesen Cluster mit zwei Knoten. Der Server ist die Kernkomponente. Er ist für die Client- und Serveraktivität verantwortlich. Die DB2-Datenbank ist eine interne Komponente, die als Teil des Servers installiert wird. Der Server steuert die gesamte Datenbankaktivität, wie beispielsweise Start und Beendigung. Wenn der Server einen Fehler der Server- oder Datenbankkomponente erkennt, versucht er, die Datenbank erneut zu starten. Wenn der Neustart fehlschlägt, werden der Server und die Datenbank automatisch auf dem Primärknoten beendet und Tivoli System Automation startet diese Komponenten automatisch auf dem Sekundärknoten. Da die IBM Spectrum Protect-Funktionen sofort wiederhergestellt werden, ist die Server- und Datenbankverfügbarkeit höher.

Abbildung 1. Die Übernahmefunktion. Die Server- und Datenbankkomponenten schlagen auf dem Primärknoten fehl. Tivoli System Automation startet diese Komponenten auf dem Sekundärknoten.

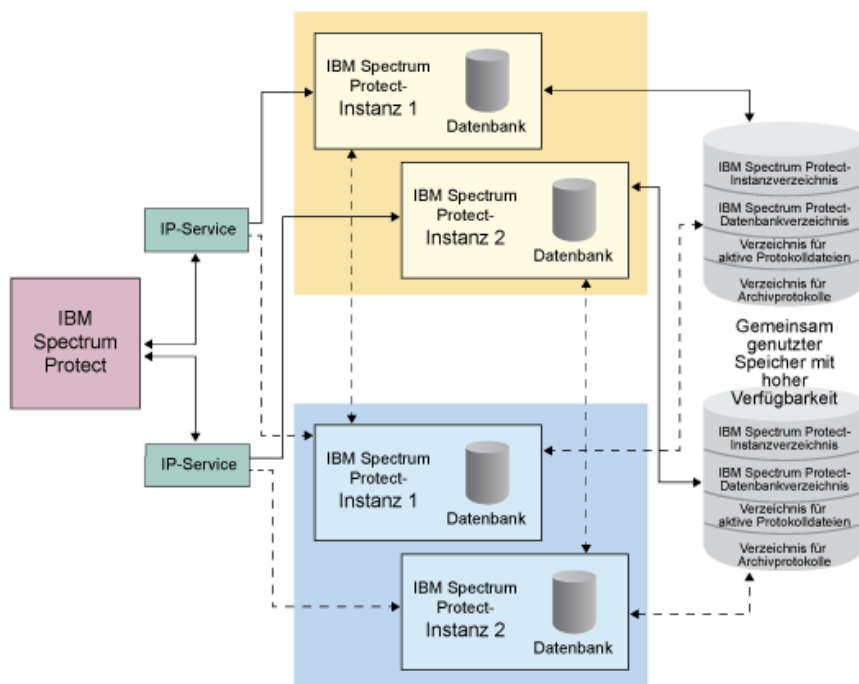




Der Server und die Datenbank umfassen die folgenden Protokollverzeichnisse, die für die Speicherung verwendet werden:

- IBM Spectrum Protect-Instanzverzeichnis
- Verzeichnis für aktive Protokolldateien
- Verzeichnis für Archivprotokolle
- Datenbankverzeichnis

Die beiden Knoten in diesem Tivoli System Automation-Cluster sind für den Zugriff auf gemeinsam genutzten Speicher mit hoher Verfügbarkeit, der die Daten schützt, konfiguriert. Beispielsweise umfasst eine Zwei-Knoten-Topologie einen Primärknoten und einen Sekundärknoten. Diese Knoten befinden sich auf unterschiedlichen physischen Systemen, können aber unter Verwendung des gemeinsam genutzten Speicherbereichs auf dieselben Daten zugreifen.

Abbildung 2. Mehrere IBM Spectrum Protect-Serverinstanzen auf unterschiedlichen Knoten. Diese Serverinstanzen befinden sich auf unterschiedlichen physischen Systemen. Diese Instanzen können auf gemeinsam genutzten Speicher mit hoher Verfügbarkeit zugreifen.



- 
**Linux-Betriebssysteme** Zwei-Knoten-Topologie mit gemeinsam genutzter Platte  
 Dieser Cluster verwendet eine Zwei-Knoten-Topologie mit gemeinsam genutzter Platte. Er umfasst einen Primärknoten und einen Sekundärknoten. Der Primärknoten hostet den IBM Spectrum Protect-Server, die Datenbank, die IBM Spectrum Protect-Instanz und die Daten. Der Sekundärknoten ist der Knoten, auf den die IBM Spectrum Protect-Ressourcen versetzt werden, wenn ein Fehler auftritt.
- 
**Linux-Betriebssysteme** Tivoli System Automation-Ressourcengruppen  
 Tivoli System Automation-Ressourcengruppen mit definierten Automatisierungsmaßnahmen ermöglichen Ihnen die Verwaltung der IBM Spectrum Protect-Komponenten für diesen Cluster. Die einzige Ausnahme ist die Datenbankserverinstanzressource, die vom IBM Spectrum Protect-Server verwaltet wird.

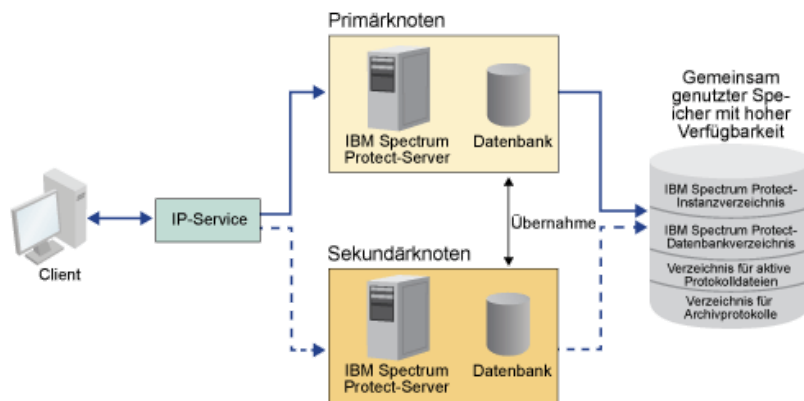
 Linux-Betriebssysteme

## Zwei-Knoten-Topologie mit gemeinsam genutzter Platte

Dieser Cluster verwendet eine Zwei-Knoten-Topologie mit gemeinsam genutzter Platte. Er umfasst einen Primärknoten und einen Sekundärknoten. Der Primärknoten hostet den IBM Spectrum Protect-Server, die Datenbank, die IBM Spectrum Protect-Instanz und die Daten. Der Sekundärknoten ist der Knoten, auf den die IBM Spectrum Protect-Ressourcen versetzt werden, wenn ein Fehler auftritt.

Die zwei Knoten in diesem Cluster sind über ein einzelnes öffentliches Netz miteinander verbunden und mit einem System mit *gemeinsam genutztem Plattenspeicher*, das immer verfügbar ist, über ein Festnetz verbunden. *Gemeinsam genutzter Plattenspeicher*

bedeutet, dass ein oder mehrere Platten sowohl für den Primärknoten als auch für den Sekundärknoten verfügbar sind. Diese Platten werden jeweils nur einem einzigen Knoten, dem Primärknoten, bereitgestellt. Daten können von einem einzelnen Knoten als Eingabe an die gemeinsam genutzten Speicherplatten gesendet oder als Ausgabe von ihnen abgerufen werden. Die folgende Abbildung zeigt eine Zwei-Knoten-Topologie mit gemeinsam genutzter Platte, bei der die automatische Übernahme durch den Sekundärknoten erfolgt, wenn ein Fehler auftritt.



Linux-Betriebssysteme

## Tivoli System Automation-Ressourcengruppen

Tivoli System Automation-Ressourcengruppen mit definierten Automatisierungsmaßnahmen ermöglichen Ihnen die Verwaltung der IBM Spectrum Protect-Komponenten für diesen Cluster. Die einzige Ausnahme ist die Datenbankserverinstanzressource, die vom IBM Spectrum Protect-Server verwaltet wird.

Die gemeinsam genutzten Dateisysteme und IBM Spectrum Protect-Komponenten sind als Ressourcen definiert. Mehrere Ressourcen bilden eine Ressourcengruppe. Jede Ressource in einer Ressourcengruppe hat einen Ressourcentyp. Jede IBM Spectrum Protect-Instanz in einem Cluster umfasst eine einzelne Ressourcengruppe. Während geplanter Betriebsunterbrechungen können Ressourcengruppen manuell vom Primärknoten auf den Sekundärknoten versetzt werden.

Die IBM Spectrum Protect-Ressourcengruppe umfasst die folgenden Ressourcen. Die IBM Spectrum Protect-Ressourcengruppe hat den Namen SA-tsm-inst1-rg; dabei gibt 'inst1' den Instanznamen an. Die folgenden Ressourcen werden für unterschiedliche, aber obligatorische Funktionen in diesem Cluster verwendet.

### Service-IP

Die Service-IP-Ressource wird für die Kommunikation verwendet. Sie hat den Namen tsm-inst1-ip-rs; dabei gibt 'inst1' den Instanznamen an. Das Service-IP wird von Tivoli System Automation verwaltet. Dieses IP ist auf dem Knoten verfügbar, auf dem der IBM Spectrum Protect-Server ausgeführt wird. Sie müssen die logische Schnittstelle für das Service-IP auf derselben physischen Schnittstelle wie die Schnittstelle für das öffentliche Netz erstellen.

### Ressource *Gemeinsam genutzter Plattenspeicher*

Eine Ressource *Gemeinsam genutzter Plattenspeicher* ist eine physische Speichereinheit auf dem IBM Spectrum Protect-Server, auf der IBM Spectrum Protect- und DB2-Anwendungsdaten gespeichert werden. Sie müssen die folgenden Plattenspeicherressourcen erstellen:

- Instanzverzeichnis - tsm-inst1-instdir-ag
- DB2-Verzeichnis - tsm-inst1-db2dir-ag
- Verzeichnis für aktive Protokolldateien - tsm-inst1-actlog-ag
- Verzeichnis für Archivprotokolle - tsm-inst1-archlog-ag

### Ressource *Gemeinsam genutzter Plattenspeicher* für Speicherpools

Die Speicherpoolressource umfasst physische Speichereinheiten auf dem IBM Spectrum Protect-Server, auf denen Clientdaten gespeichert werden.

### Datenträgergruppenressourcen


Wenn Sie Ihren Speicher mithilfe von Datenträgergruppen konfigurieren, ist für die vorhergehenden Ressourcen *Gemeinsam genutzter Plattenspeicher* eine Datenträgergruppenressource verfügbar. Datenträgergruppenressourcen werden automatisch von Tivoli System Automation erstellt.

Anwendungsressourcen für die IBM Spectrum Protect-Serverinstanz

Bei der IBM Spectrum Protect-Serverinstanzressource handelt es sich um die Serverressource, die die IBM Spectrum Protect-Anwendung verwaltet. Diese Ressource wird mithilfe von Tivoli System Automation-Steuerscripts verwaltet.

Tabelle 1. Tasks, die von den Tivoli System Automation-Steuerscripts ausgeführt werden

| Tasks      | Beschreibung   | Beispielbefehle   |
|------------|--|---|
| Starten    | Startet die IBM Spectrum Protect-Serverinstanz.  | Mit dem Befehl <code>/opt/tivoli/tsm/server/bin/rc.dsmserv -u db2inst1 -i /tsminst1</code> wird die Serverinstanz vom Benutzer <code>db2inst1</code> im Verzeichnis <code>/tsminst1</code> gestartet. |
| Stoppen    | Stoppt die IBM Spectrum Protect-Serverinstanz.   | <code>kill -s SIGURG 345</code> ; dabei ist <code>345</code> die <i>PID</i> . Die <i>PID</i> ist in der Datei <code>/tsminst1/dsmserv.v6lock</code> angegeben.  |
| Überwachen | Prüft, ob die Datei <code>/tsminst1/dsmserv.v6lock</code> vorhanden ist. Mithilfe der <i>PID</i> wird geprüft, ob der Prozess aktiv ist. | <code>ps -ef   grep 345</code> ; dabei ist <code>345</code> die <i>PID</i> .  |

-  Linux-Betriebssysteme Ressourcenabhängigkeiten Ressourcenabhängigkeiten werden automatisch erstellt, um zu steuern, in welcher Reihenfolge Ressourcen gestartet werden. Diese Abhängigkeiten steuern auch, welche Ressourcen erneut gestartet oder beendet werden müssen, wenn die spezifische Ressource, von der diese Ressourcen abhängig sind, fehlschlägt.

 Linux-Betriebssysteme

## IBM Spectrum Protect-Cluster mit Tivoli System Automation konfigurieren

Sie müssen den IBM Spectrum Protect-Cluster konfigurieren, um Tivoli System Automation verwenden zu können.

### Vorgehensweise

1. Installieren und konfigurieren Sie die IBM Spectrum Protect-Komponenten auf den Primär- und Sekundärknoten.
2. Installieren Sie Tivoli System Automation auf den Primär- und Sekundärknoten.
3. Konfigurieren Sie die Speicherressourcen.
4. Abhängig von der IBM Spectrum Protect-Version, die auf dem Server installiert ist, müssen Sie gegebenenfalls ein Upgrade des IBM Spectrum Protect-Servers für den Tivoli System Automation-Cluster durchführen.
5. Optional: Sie können die Variable `FILE_EXIT` im Cluster-Script `tsmservctrl` definieren, um die Tivoli System Automation-Ereignisdaten in die IBM Spectrum Protect-Serverdatei `FILEEXIT` umzuleiten. Editieren Sie beispielsweise das Cluster-Script `tsmservctrl` im Verzeichnis `<Serverinstallationsverzeichnis>/tsam/controls` und fügen Sie die folgende Zeile hinzu:

```
FILE_EXIT="fileexittmp"
```

 Linux-Betriebssysteme

## Voraussetzungen zum Konfigurieren einer Linux-Clusterumgebung mit Tivoli System Automation

Bevor Sie IBM Spectrum Protect in einer Clusterumgebung mit Tivoli System Automation installieren und konfigurieren, müssen Sie die Voraussetzungen überprüfen.

Überprüfen Sie, ob die folgenden Voraussetzungen erfüllt sind.

- Planen Sie die Installation des IBM Spectrum Protect-Servers.
- Überprüfen Sie nach der Installation von IBM Spectrum Protect Folgendes:
  - Stellen Sie sicher, dass die DB2-Datenbank auf demselben Knoten wie der Server installiert ist.
  - Stellen Sie sicher, dass der Server die Datenbankwiederherstellung steuern kann.
  - Stellen Sie sicher, dass gemeinsam genutzte Speichereinheiten verfügbar sind. IBM Spectrum Protect erfordert gemeinsam genutzte Speichereinheiten mit hoher Verfügbarkeit, um die Datenintegrität gewährleisten zu können.
  - Stellen Sie sicher, dass jeder Knoten im Cluster mehrere Instanzen des Servers enthalten kann.
- Bereiten Sie die Installation von Tivoli System Automation vor. Anweisungen finden Sie in der Tivoli System Automation-Produktdokumentation. Suchen Sie in der Veröffentlichung *Installation and Configuration Guide* nach *Preparing for installation*.
- Stellen Sie nach der Installation von Tivoli System Automation sicher, dass Tivoli System Automation die Übernahme, wie beispielsweise IP-Übernahme und Datenübernahme, für die Datenbank, die Instanzdaten, die aktive Protokolldatei und das



Archivprotokoll sowie für Speicherpools verarbeiten kann.

#### Zugehörige Tasks:




Installation des IBM Spectrum Protect-Servers planen

 Linux-Betriebssysteme

## IBM Spectrum Protect-Komponenten auf den Primär- und Sekundärknoten installieren und konfigurieren

---

Sie müssen die IBM Spectrum Protect-Server- und -Datenbankkomponenten auf den Primär- und Sekundärknoten im Cluster installieren. Konfigurieren Sie anschließend zunächst den Primärknoten und dann den Sekundärknoten.

-  Linux-Betriebssysteme IBM Spectrum Protect-Serverkomponenten installieren  
Nachdem Sie die Voraussetzungen überprüft haben, müssen Sie die erforderlichen Komponenten auf den Primär- und Sekundärknoten auf dem System installieren.
-  Linux-Betriebssysteme Primärknoten konfigurieren  
Um die Zwei-Knoten-Topologie zu definieren, konfigurieren Sie die IBM Spectrum Protect-Komponenten auf beiden Knoten. Zunächst müssen Sie die IBM Spectrum Protect-Instanz auf dem Primärknoten konfigurieren.
-  Linux-Betriebssysteme Sekundärknoten konfigurieren  
Nachdem Sie den Primärknoten konfiguriert haben, müssen Sie den Sekundärknoten konfigurieren, damit Tivoli System Automation die IBM Spectrum Protect-Serverkomponenten auf den Sekundärknoten versetzen kann, wenn der Server auf dem Primärknoten fehlschlägt.

 Linux-Betriebssysteme

## IBM Spectrum Protect-Serverkomponenten installieren

---

Nachdem Sie die Voraussetzungen überprüft haben, müssen Sie die erforderlichen Komponenten auf den Primär- und Sekundärknoten auf dem System installieren.


### Vorgehensweise

---

Lesen Sie die Abschnitte in den Informationen zum Installieren der IBM Spectrum Protect-Serverkomponenten.

#### Zugehörige Tasks:

IBM Spectrum Protect-Serverkomponenten installieren

 Linux-Betriebssysteme

## Primärknoten konfigurieren

---

Um die Zwei-Knoten-Topologie zu definieren, konfigurieren Sie die IBM Spectrum Protect-Komponenten auf beiden Knoten. Zunächst müssen Sie die IBM Spectrum Protect-Instanz auf dem Primärknoten konfigurieren.

### Vorbereitende Schritte

---

- Installieren Sie die IBM Spectrum Protect-Serverkomponenten.
- Stellen Sie sicher, dass der IBM Spectrum Protect-Instanzeigner für alle Knoten in der Clusterdomäne dieselbe Benutzer-ID und dieselbe Gruppen-ID hat.
- Stellen Sie sicher, dass der IBM Spectrum Protect-Instanzeigner für alle Clusterknoten dasselbe Kennwort hat.

### Vorgehensweise

---

1. Detaillierte Anweisungen zum Erstellen der Verzeichnisse und der Benutzer-ID für die Serverinstanz finden Sie in Linux: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen.
2. Stellen Sie sicher, dass der IBM Spectrum Protect-Server, die DB2-Instanz und die Verzeichnisse für die aktive Protokolldatei und das Archivprotokoll gemeinsam genutzt werden.
3. Definieren Sie die Mountpunkte, indem Sie der Datei /etc/fstab Einträge hinzufügen.

Wenn Sie auf den Clusterknoten Mountpunkte hinzufügen, verwenden Sie die Option noauto, um zu verhindern, dass die Mountpunkte automatisch auf mehr als einem Knoten im Cluster bereitgestellt werden.

4. Definieren Sie für jeden der Mountpunkte die folgenden Berechtigungen:
  - 755. Beispielsweise wird mit dem folgenden Befehl die Berechtigung 755 für den Mountpunkt /tsminst1 definiert.

```
chmod -R 755 /tsminst1
```

- IBM Spectrum Protect-Serverinstanzeigner. Beispielsweise werden mit dem folgenden Befehl die Berechtigungen für den Instanzeigner definiert.

```
chown -R tsminst1 /tsminst1
```

- IBM Spectrum Protect-Servergruppe, zu der der Instanzeigner gehört. Beispielsweise werden mit dem folgenden Befehl die Berechtigungen für die Gruppe des Instanzeigners definiert.

```
chgrp tsmsrv_1_group /tsminst1
```

5. Detaillierte Anweisungen zur Konfiguration des IBM Spectrum Protect-Servers mithilfe des Konfigurationsassistenten finden Sie in Linux: IBM Spectrum Protect mithilfe des Konfigurationsassistenten konfigurieren. Stellen Sie sicher, dass alle gemeinsam genutzten Verzeichnisse auf dem Primärknoten bereitgestellt werden.
6. Starten Sie die IBM Spectrum Protect-Serverinstanz auf dem Primärknoten mithilfe des Dienstprogramms DSMSEV. Beispielsweise wird mit dem folgenden Befehl der Server für den normalen Betrieb gestartet.

```
/opt/tivoli/tsm/server/bin/dsmsevr
```

7. Stellen Sie sicher, dass die IBM Spectrum Protect-Komponenten ohne Fehler gestartet werden.
8. Fahren Sie den IBM Spectrum Protect-Server herunter.
9. Heben Sie als Rootbenutzer die Bereitstellung der gemeinsam genutzten Laufwerke auf.



## Sekundärknoten konfigurieren

---

Nachdem Sie den Primärknoten konfiguriert haben, müssen Sie den Sekundärknoten konfigurieren, damit Tivoli System Automation die IBM Spectrum Protect-Serverkomponenten auf den Sekundärknoten versetzen kann, wenn der Server auf dem Primärknoten fehlschlägt.

### Vorgehensweise

---

1. Um die Verzeichnisse und die Benutzer-ID für die Serverinstanz manuell zu erstellen, führen Sie die Anweisungen in Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen aus.
2. Stellen Sie sicher, dass der IBM Spectrum Protect-Server, die DB2-Instanz und die Verzeichnisse für die aktive Protokolldatei und das Archivprotokoll gemeinsam genutzt werden.
3. Definieren Sie die Mountpunkte, indem Sie in der Datei /etc/fstab Einträge hinzufügen.

Wenn Sie auf den Clusterknoten Mountpunkte hinzufügen, verwenden Sie die Option noauto. Mit dieser Option wird verhindert, dass die Mountpunkte automatisch auf mehr als einem Knoten im Cluster bereitgestellt werden.

Stellen Sie sicher, dass alle gemeinsam genutzten Verzeichnisse auf dem Sekundärknoten bereitgestellt werden.

4. Definieren Sie für jeden der Mountpunkte die folgenden Berechtigungen:
  - 755. Beispielsweise wird mit dem folgenden Befehl die Berechtigung 755 für den Mountpunkt /tsminst1 definiert.

```
chmod -R 755 /tsminst1
```

- IBM Spectrum Protect-Serverinstanzeigner. Beispielsweise werden mit dem folgenden Befehl die Berechtigungen für den Instanzeigner definiert.

```
chown -R tsminst1 /tsminst1
```

- IBM Spectrum Protect-Servergruppe, zu der der Instanzeigner gehört. Beispielsweise werden mit dem folgenden Befehl die Berechtigungen für die Gruppe des Instanzeigners definiert.

```
chgrp tsmsrv_1_group /tsminst1
```

5. Erstellen Sie die IBM Spectrum Protect-Serverinstanz, indem Sie den Befehl db2icrt ausgeben. Anweisungen finden Sie in Serverinstanz erstellen.  
Hinweis: Sie müssen keine neue Serveroptionsdatei erstellen, da der Sekundärknoten die Datei dsmsevr.opt des Primärknotens verwendet.  
Stellen Sie sicher, dass alle gemeinsam genutzten Verzeichnisse auf dem Sekundärknoten bereitgestellt werden.
6. Katalogisieren Sie die Datenbank, indem Sie den Befehl catalog db ausgeben. Beispielsweise wird mit dem folgenden Befehl die Datenbank tsmdb1 katalogisiert.

```
db2 catalog db tsmdb1
```

7. Bereiten Sie die Datenbank für die Sicherung vor. Anweisungen finden Sie in Datenbankmanager für die Datenbanksicherung vorbereiten.
8. Starten Sie den IBM Spectrum Protect-Server mithilfe des Dienstprogramms DSMSEV. Beispielsweise wird mit dem folgenden Befehl der Server für den normalen Betrieb gestartet.

```
/opt/tivoli/tsm/server/bin/dsmsevr
```

9. Stellen Sie sicher, dass die IBM Spectrum Protect-Komponenten ohne Fehler gestartet werden.
10. Fahren Sie auf dem Sekundärknoten den IBM Spectrum Protect-Server herunter und heben Sie die Bereitstellung der gemeinsam genutzten Verzeichnisse auf.



## Tivoli System Automation auf den Primär- und Sekundärknoten installieren

Nachdem Sie IBM Spectrum Protect auf den Primär- und Sekundärknoten im Cluster installiert und konfiguriert haben, müssen Sie Tivoli System Automation auf diesen Knoten installieren und konfigurieren. Anschließend müssen Sie diese Knoten für die Domäne aktivieren, die Ressourcen konfigurieren und die Basismaßnahme aktivieren. Abschließend müssen Sie den IBM Spectrum Protect-Verzeichnissen die Mountpunkte hinzufügen.

- **Kennsatz für die Mountpunkte erstellen**  
Erstellen Sie für jeden Mountpunkt auf den Primär- und Sekundärknoten im Cluster einen Kennsatz.
- **Tivoli System Automation installieren und konfigurieren**  
Sie müssen IBM Tivoli System Automation for Multiplatforms auf den Primär- und Sekundärknoten im System installieren.
- **Aktivierung der Clusterknoten für die Domäne vorbereiten**  
Nachdem Sie Tivoli System Automation auf den Primär- und Sekundärknoten im Cluster installiert haben, müssen Sie diese Knoten vorbereiten, um den Cluster aktivieren und die Clusterdomäne starten zu können.
- **Datenträgergruppenressourcen konfigurieren**  
Wenn Sie Datenträgergruppen für Ihren Cluster erstellt haben, müssen Sie diese Ressourcen konfigurieren. Tivoli System Automation findet und definiert automatisch die Ressourcen für gemeinsam genutzte Plattendatenträger.
- **Ressourcen konfigurieren, die sich nicht in einer Datenträgergruppe befinden**  
Wenn Sie Ihre Ressourcen *gemeinsam genutzter Plattenspeicher* unter Verwendung des Ressourcentyps ext2, ext3 oder reiserfs in einem der Knoten im Cluster erstellt haben, müssen Sie diese Ressourcen konfigurieren.
- **Basismaßnahme aktivieren**  
Nach dem Konfigurieren der Ressourcen müssen Sie die Maßnahme auf dem Primär- und Sekundärknoten aktivieren, um alle übrigen Ressourcen und die Ressourcengruppe zu erstellen.
- **Mountpunkte den IBM Spectrum Protect-Verzeichnissen hinzufügen**  
Bevor Sie den Cluster starten können, müssen Sie die Mountpunkte hinzufügen, die für die IBM Spectrum Protect-Komponenten erstellt wurden.



## Kennsatz für die Mountpunkte erstellen

Erstellen Sie für jeden Mountpunkt auf den Primär- und Sekundärknoten im Cluster einen Kennsatz.

### Vorgehensweise

1. Erstellen Sie für jeden der Datenträger, die Sie zuvor für die Mountpunkte für gemeinsam genutztes Verzeichnis erstellt haben, einen Kennsatz, indem Sie den Befehl `e2label` ausgeben. Beispielsweise wird mit dem folgenden Befehl der Kennsatz `/tsminst1` erstellt, der über eine Partition `/dev/tsmvg1/tsminst1LV` verfügt.

```
e2label /dev/tsmvg1/tsminst1LV /tsminst1
```

2. Ersetzen Sie für jeden Knoten im Cluster die Einträge für die Mountpunkte, die Sie zuvor in der Datei `/etc/fstab` erstellt haben. Geben Sie beispielsweise für den vorherigen Beispielkennsatz den folgenden Befehl aus:

```
LABEL=/tsminst1 /tsminst1 ext3 defaults 0 0
```



## Tivoli System Automation installieren und konfigurieren



Sie müssen IBM® Tivoli System Automation for Multiplatforms auf den Primär- und Sekundärknoten im System installieren.

## Vorgehensweise

---

1. Ausführliche Informationen zum Installieren und Konfigurieren von Tivoli System Automation finden Sie in der Veröffentlichung Tivoli System Automation Installation and Configuration Guide.
2. Laden Sie die Datei TSM-25072011-1015.zip über Integrated Service Management Library herunter. Extrahieren Sie die komprimierte Datei auf jedem Clusterknoten.
3. Überprüfen Sie nach dem Extrahieren der komprimierten Datei, ob das neue Tivoli System Automation-Verzeichnis, das während der Installation erstellt wurde, das Verzeichnis /TSM/HA und die zugehörigen Unterverzeichnisse umfasst.

### Zugehörige Informationen:

-  Produktinformation zu IBM Tivoli System Automation for Multiplatforms Version 3.2.2
-  Linux-Betriebssysteme

## Aktivierung der Clusterknoten für die Domäne vorbereiten

---

Nachdem Sie Tivoli System Automation auf den Primär- und Sekundärknoten im Cluster installiert haben, müssen Sie diese Knoten vorbereiten, um den Cluster aktivieren und die Clusterdomäne starten zu können.

### Vorgehensweise

---

1. Bereiten Sie jeden Knoten für die Domäne vor, indem Sie den Befehl `preprnode` ausgeben. Geben Sie diesen Befehl für alle Clusterknoten in der Domäne aus. Beispielsweise werden mit dem folgenden Befehl die Knoten `HOST1.ibm.com` und `HOST2.ibm.com` vorbereitet.
2. Erstellen Sie für jeden Knoten eine Domäne, indem Sie den Befehl `mkrpdomain` ausgeben. Beispielsweise wird mit dem folgenden Befehl die Domäne `tsm_domain` für die Knoten `HOST1.ibm.com` und `HOST2.ibm.com` erstellt.
3. Starten Sie die Domäne für jeden Knoten, indem Sie den Befehl `startrpdomain` ausgeben. Beispielsweise wird mit dem folgenden Befehl die Domäne `tsm_domain` gestartet.

```
preprnode HOST1.ibm.com HOST2.ibm.com
```

```
mkrpdomain tsm_domain HOST1.ibm.com HOST2.ibm.com
```

```
startrpdomain tsm_domain
```

 Linux-Betriebssysteme

## Datenträgergruppenressourcen konfigurieren

---

Wenn Sie Datenträgergruppen für Ihren Cluster erstellt haben, müssen Sie diese Ressourcen konfigurieren. Tivoli System Automation findet und definiert automatisch die Ressourcen für gemeinsam genutzte Plattendatenträger.

### Vorgehensweise

---

Um die Datenträgergruppenressourcen für die gemeinsam genutzten IBM Spectrum Protect-Verzeichnisse und -Mountpunkte, die Sie zuvor erstellt haben, zu konfigurieren, führen Sie die folgenden Schritte auf dem Primärknoten aus:

1. Importieren Sie die Datenträgergruppen. Verwenden Sie beispielsweise den Befehl `vgimport X`, um die `x`-Datenträgergruppen zu importieren.
2. Aktivieren Sie die Datenträgergruppen. Verwenden Sie beispielsweise den Befehl `vgchange -ay X`, um die `x`-Datenträgergruppen zu aktivieren.
3. Hängen Sie das Dateisystem an, indem Sie den Befehl `mount` ausgeben. In dem folgenden Beispiel wird das Dateisystem `x` angehängt.

```
mount X
```

4. Starten Sie die Domäne erneut, indem Sie die Befehle `stoprpdomain` und `startrpdomain` ausgeben. Beispielsweise wird mit den folgenden Befehlen die Domäne `tsm_domain` erneut gestartet.

```
stoprpdomain tsm_domain  
startrpdomain tsm_domain
```

5. Hängen Sie das Dateisystem ab, indem Sie den Befehl `umount` ausgeben. Verwenden Sie beispielsweise den Befehl `umount X`, um das Dateisystem `x` abzuhängen.
6. Inaktivieren Sie die Datenträgergruppen. Verwenden Sie beispielsweise den Befehl `vgchange -an X`, um die `x`-Datenträgergruppen zu inaktivieren.

- Überprüfen Sie, ob alle der IBM®.AgfileSystem-Speicherressourcen von Tivoli System Automation übernommen wurden, indem Sie den folgenden Befehl ausgeben:

```
lsrsrc -s "Name=='Ressourcenname' && ResourceType=1" IBM.AgFileSystem
```



## Ressourcen konfigurieren, die sich nicht in einer Datenträgergruppe befinden

Wenn Sie Ihre Ressourcen *gemeinsam genutzter Plattenspeicher* unter Verwendung des Ressourcentyps ext2, ext3 oder reiserfs in einem der Knoten im Cluster erstellt haben, müssen Sie diese Ressourcen konfigurieren.

### Vorgehensweise

Führen Sie auf dem Primärknoten die folgenden Schritte aus:

- Hängen Sie das Dateisystem an, indem Sie den Befehl mount ausgeben. Beispielsweise wird mit dem folgenden Befehl das Dateisystem X angehängt.

```
mount X
```

- Starten Sie die Domäne erneut, indem Sie die Befehle stoprpdomain und startrpdomain ausgeben. Beispielsweise wird mit den folgenden Befehlen die Domäne tsm\_domain erneut gestartet.

```
stoprpdomain tsm_domain  
startrpdomain tsm_domain
```

- Hängen Sie das Dateisystem ab, indem Sie den Befehl umount ausgeben. Beispielsweise wird mit dem folgenden Befehl das Dateisystem X abgehängt.

```
umount X
```

- Überprüfen Sie, ob alle der IBM®.AgfileSystem-Speicherressourcen von Tivoli System Automation übernommen wurden, indem Sie den folgenden Befehl ausgeben:

```
lsrsrc -s "Name=='Ressourcenname' && ResourceType=1" IBM.AgFileSystem
```

Um beispielsweise die Ressource *tsmalog* zu prüfen, geben Sie den folgenden Befehl aus:

```
lsrsrc -s "Name=='tsmalog' && ResourceType=1" IBM.AgFileSystem  
Resource Persistent Attributes for IBM.AgFileSystem resource 1:  
ResourceHandle= "0x2038 0xffff 0x6ad47197 0x256fc23d 0x9338a9950x263fa510"  
Name = "tsmalog"  
ResourceType = 1 <-----  
MountPoint = ""  
DeviceName = ""  
Vfs = "ext3"  
AggregateResource = "0x3fff 0xffff 0x00000000 0x00000000 0x00000000 0x00000000"  
ContainerResource = "0x2036 0xffff 0x6ad47197 0x256fc23d 0x9338a995 0x25ffaa28"  
GhostDevice = 0  
ResourceId = "360050768019c021d30000000000005da"  
ProtectionMode = 1  
UserControl = 0  
SysMountPoint = "/tsmalog"  
Label = "/tsmalog"  
FSID = "5792f887-8547-4c33-a519-9d0c50ab6882"  
PreOnlineMethod = 0  
ContainerResourceId = "360050768019c021d30000000000005da"  
AutoMonitor = 1  
Options = "defaults,noauto"  
PreOfflineMethod = 0  
ActivePeerDomain = "TSM-Domäne"  
NodeNameList =  
{ "tsmlnode01.storage.tucson.ibm.com", "tsmlnode02.storage.tucson.ibm.com" }
```



## Basismaßnahme aktivieren

Nach dem Konfigurieren der Ressourcen müssen Sie die Maßnahme auf dem Primär- und Sekundärknoten aktivieren, um alle übrigen Ressourcen und die Ressourcengruppe zu erstellen.

## Informationen zu diesem Vorgang

---

Um die Basismaßnahme zu aktivieren, müssen Sie die Service-IP-Ressource und IBM Spectrum Protect-Anwendungsressourcen für die IBM Spectrum Protect-Serverinstanz erstellen. Anschließend müssen Sie die Ressourcengruppe und die Maßnahmen zum Verwalten des Clusters erstellen.

## Vorgehensweise

---

Führen Sie die folgenden Schritte zunächst auf dem Primärknoten und dann auf dem Sekundärknoten aus.

1. Wechseln Sie in das Verzeichnis, in das der Inhalt der Datei TSM-25072011-1015.zip extrahiert wurde.
2. Definieren Sie die Dateiberechtigungen für die Scripts im Verzeichnis bin, indem Sie den Befehl `chmod` ausgeben. Beispielsweise werden mit dem folgenden Befehl die Dateiberechtigungen für alle Scripts im Verzeichnis bin definiert. XXX ist der Name des extrahierten Ordners.

```
chmod 755 /XXX/TSM/HA/bin/*
```

3. Wechseln Sie in das Verzeichnis bin, indem Sie den Befehl `cd` ausgeben.
4. Aktualisieren Sie die folgenden Variablen im Script `base_cluster_variables.sh`:
  - `NODE1` gibt den Hostnamen für Knoten 1 (Primärknoten) im Cluster an.
  - `NODE2` gibt den Hostnamen für Knoten 2 (Sekundärknoten) im Cluster an.
  - `IP_GATEWAY` gibt das Gateway des Service-IP an.
  - `SUBNET_MASK` gibt die Teilnetzmaske des Service-IP an.
  - `NET_INT` gibt den Namen der Netzchnittstelle eines bestimmten Knotens im Cluster an. Dieser Name muss für alle Knoten im Cluster identisch sein.

5. Führen Sie das Konfigurationsscript `configureHA.sh` aus, indem Sie den Befehl `./configureHA.sh` auf allen Knoten im Cluster ausgeben.

Wenn das Script `configureHA.sh` mit dem Fehler `-bash: ./configureHA.sh: /bin/bash^M: bad interpreter: No such file or directory` fehlschlägt, geben Sie den Befehl `dos2unix` für alle Scripts im Verzeichnis bin aus. Führen Sie beispielsweise für jedes Script den folgenden Befehl aus:

```
dos2unix -o <Dateiname>
```

6. Überprüfen Sie, ob die Konfiguration erfolgreich ausgeführt wird, indem Sie überprüfen, ob das Konfigurationsscript erfolgreich ausgeführt wird.
7. **Achtung:** Führen Sie diesen Schritt nur auf dem Primärknoten aus!  
Führen Sie das Setup-Script aus, indem Sie den Befehl `./setup.sh` ausgeben. Beispielsweise wird mit dem folgenden Befehl das Setup-Script für die IBM Spectrum Protect-Serverinstanz `inst1` für den Instanzbenutzer `dbinst1` im IBM Spectrum Protect-Serverinstanzverzeichnis `/tsminst1` mit `9.11.142.129` als Service-IP ausgeführt.

```
./setup.sh inst1 dbinst1 /tsminst1 9.11.142.129
```

8. Überprüfen Sie, ob das korrekte IP (Internet Protocol) verwendet wird, indem Sie den folgenden Befehl ausführen:

```
lssam -V
```

9. Wiederholen Sie Schritt 5 für alle IBM Spectrum Protect-Instanzen in Ihrer IBM Spectrum Protect-Serverumgebung.
10. Führen Sie alle vorhergehenden Schritte auf dem Sekundärknoten aus.

 Linux-Betriebssysteme

## Mountpunkte den IBM Spectrum Protect-Verzeichnissen hinzufügen

---

Bevor Sie den Cluster starten können, müssen Sie die Mountpunkte hinzufügen, die für die IBM Spectrum Protect-Komponenten erstellt wurden.

## Vorgehensweise

---

Um der Clusterressourcengruppe die Mountpunkte für gemeinsam genutzte Platten hinzuzufügen und den Cluster online zu schalten, führen Sie die folgenden Schritte aus:

1. Geben Sie Mountpunkte für die folgenden Verzeichnisse an:
  - Instanz
  - Datenbank

- o Aktive Protokolldatei
  - o Archivprotokoll
  - o Speicherpool
2. Fügen Sie jedem Mountpunkt Ressourcen hinzu:
    - a. Überprüfen Sie, ob die Ressourcengruppe `tsm-$INST_NAME-rg` online ist, indem Sie den Befehl `lssam` ausgeben.
    - b. Wenn die Ressourcengruppe `tsm-$INST_NAME-rg` online ist, schalten Sie sie offline, indem Sie den folgenden Befehl ausgeben:
 

```
chrg -o offline tsm-$INST_NAME-rg
```
    - c. Wechseln Sie in das Verzeichnis, in das der Inhalt der Datei `TSM-25072011-1015.zip` extrahiert wurde.
    - d. Wechseln Sie in das Verzeichnis `'bin'`, indem Sie den Befehl `cd` ausgeben.
    - e. Um jedem Mountpunkt gemeinsam genutzte Plattenressourcen hinzuzufügen, führen Sie das Script `./update_setup.sh` aus. Beispielsweise wird mit dem folgenden Befehl der Mountpunkt `/tsminst1` der IBM Spectrum Protect-Serverinstanz `inst1` hinzugefügt.
 

```
./update_setup.sh inst1 /tsminst1
```
  3. Schalten Sie die Ressourcengruppe `tsm-$INST_NAME-rg` online, indem Sie den folgenden Befehl ausgeben:
 

```
chrg -o online tsm-$INST_NAME-rg
```
  4. Stellen Sie unter Verwendung des Service-Gateway-IP die Verbindung zum Server her, um zu überprüfen, ob die Konfiguration korrekt ist.



## Speicherressourcen konfigurieren

Verwenden Sie die Tivoli System Automation-Benutzerschnittstelle, oder -Befehlszeile, um Speicherressourcen hinzuzufügen oder zu löschen und um Mountpunkte, die nicht mehr benötigt werden, zu löschen. Wenn Sie dem Cluster einen Speicherpool hinzufügen, müssen Sie den Speicherpool der Ressourcengruppe hinzufügen. Wenn Sie einen Speicherpool aus dem Cluster entfernen, müssen Sie den Speicherpool auch aus der Ressourcengruppe löschen.

- Speicherpool einer Ressourcengruppe hinzufügen  
Wenn bei Ihrer IBM Spectrum Protect-Konfiguration Daten auf Platten gespeichert werden, müssen Sie der Ressourcengruppe den Mountpunkt für gemeinsam genutzte Platten für den Speicherpool hinzufügen.
- Speicherpool aus einer Ressourcengruppe löschen  
Sie können einen Speicherpool, der nicht mehr erforderlich ist, löschen. Wenn ein Speicherpool aus der IBM Spectrum Protect-Serverinstanz entfernt wird, muss er aus der Ressourcengruppe gelöscht werden.
- Mountpunkt aus einer Ressourcengruppe löschen  
Sie können einen Mountpunkt, der nicht mehr erforderlich ist, bei Bedarf löschen.



## Speicherpool einer Ressourcengruppe hinzufügen

Wenn bei Ihrer IBM Spectrum Protect-Konfiguration Daten auf Platten gespeichert werden, müssen Sie der Ressourcengruppe den Mountpunkt für gemeinsam genutzte Platten für den Speicherpool hinzufügen.

### Vorgehensweise

Um der Ressourcengruppe den Mountpunkt für gemeinsam genutzte Platten für den Speicherpool hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Sperren Sie die Ressourcengruppe, indem Sie den Befehl `rgreq -o lock` ausgeben. Beispielsweise wird mit dem folgenden Befehl die Ressourcengruppe `Beispielressourcengruppe_X` gesperrt.
 

```
rgreq -o lock Beispielressourcengruppe_X
```
2. Wechseln Sie in das Verzeichnis `'bin'`, indem Sie den Befehl `cd` ausgeben:
3. Um einer Ressourcengruppe eine Speicherpoolressource hinzuzufügen, führen Sie das Script `update_setup.sh` aus, indem Sie den Befehl `./update_setup.sh` ausgeben. Beispielsweise wird mit dem folgenden Befehl der Speicherpoolmountpunkt `/inst1stg1` der IBM Spectrum Protect-Serverinstanz `inst1` hinzugefügt.

```
./update_setup.sh inst1 /inst1stg1
```

4. Entsperren Sie die Ressourcengruppe, indem Sie den Befehl `rgreq -o unlock` ausgeben. Beispielsweise wird mit dem folgenden Befehl die Ressourcengruppe `Beispielressourcengruppe_X` entsperrt.

```
rgreq -o unlock Beispielressourcengruppe_X
```



## Speicherpool aus einer Ressourcengruppe löschen

---

Sie können einen Speicherpool, der nicht mehr erforderlich ist, löschen. Wenn ein Speicherpool aus der IBM Spectrum Protect-Serverinstanz entfernt wird, muss er aus der Ressourcengruppe gelöscht werden.

### Vorgehensweise

---

Um einen Speicherpool zu löschen, führen Sie die folgenden Schritte aus:

1. Sperren Sie die Ressourcengruppe, indem Sie den Befehl `rgreq -o lock` ausgeben. Beispielsweise wird mit dem folgenden Befehl die Ressourcengruppe `Beispielressourcengruppe_X` gesperrt.

```
rgreq -o lock Beispielressourcengruppe_X
```

2. Wechseln Sie in das Verzeichnis `bin`, indem Sie den Befehl `cd` ausgeben.
3. Um eine Speicherpoolressource aus einer Ressourcengruppe zu löschen, führen Sie das Script `delete_mount.sh` aus, indem Sie den Befehl `./delete_mount.sh` ausgeben. Beispielsweise wird mit dem folgenden Befehl der Mountpunkt `/inst1stg1` aus der IBM Spectrum Protect-Serverinstanz `inst1` gelöscht.

```
./delete_mount.sh /inst1stg1 inst1
```

4. Entsperren Sie die Ressourcengruppe, indem Sie den Befehl `rgreq -o unlock` ausgeben. Beispielsweise wird mit dem folgenden Befehl die Ressourcengruppe `Beispielressourcengruppe_X` entsperrt.

```
rgreq -o unlock Beispielressourcengruppe_X
```



## Mountpunkt aus einer Ressourcengruppe löschen

---

Sie können einen Mountpunkt, der nicht mehr erforderlich ist, bei Bedarf löschen.

### Vorgehensweise

---

Um einen Mountpunkt zu löschen, führen Sie die folgenden Schritte aus:

1. Überprüfen Sie, ob die Ressourcengruppe `tsm- $\$INST\_NAME$ -rg` online ist, indem Sie den Befehl `lssam` ausgeben.
2. Wenn die Ressourcengruppe `tsm- $\$INST\_NAME$ -rg` online ist, schalten Sie die offline, indem Sie den folgenden Befehl ausgeben:

```
chrg -o offline tsm- $\$INST\_NAME$ -rg
```

3. Wechseln Sie in das Verzeichnis `bin`, indem Sie den Befehl `cd` ausgeben.
4. Um einen Mountpunkt zu löschen, führen Sie das Script `delete_mount.sh` aus. Beispielsweise wird mit dem folgenden Befehl der Mountpunkt `/tsminst1` aus der Ressourcengruppe der IBM Spectrum Protect-Serverinstanz `inst1` gelöscht.

```
./delete_mount.sh /tsminst1 inst1
```

5. Schalten Sie die Ressourcengruppe `tsm- $\$INST\_NAME$ -rg` online, indem Sie den folgenden Befehl ausgeben:

```
chrg -o online tsm- $\$INST\_NAME$ -rg
```



## Upgrade für einen Server durchführen, der mit Tivoli System Automation konfiguriert ist

---

Sie können ein Upgrade für einen Server der Version 6.3 oder Version 7.1 durchführen, der mit Tivoli System Automation konfiguriert ist.

### Vorgehensweise

---



Um für den Server ein Upgrade auf jedem Knoten in dem Cluster durchzuführen, melden Sie sich bei dem Server an und führen Sie die folgenden Schritte aus. Mit diesen Schritten wird das Upgrade auf dem Primärknoten gestartet; später in dieser Prozedur wird dann das Upgrade für den Sekundärknoten durchgeführt.

1. Stoppen Sie die Serverressourcen, indem Sie den Befehl `chrg -o Offline tsm-tsminst1-rg` ausgeben. Beispielsweise werden mit dem folgenden Befehl die Ressourcen in der Ressourcengruppe `tsm-tsminst1-rg` gestoppt:

```
chrg -o Offline tsm-tsminst1-rg
```

2. Stoppen Sie die Tivoli System Automation-Domäne, indem Sie den Befehl `stoprpdomain` ausgeben. Beispielsweise wird mit dem folgenden Befehl die Domäne `tsm_domain` gestoppt:

```
stoprpdomain tsm_domain
```

3. Stellen Sie die Server-Mountpunkte auf dem Primärknoten bereit.
4. Informationen zur Durchführung eines Upgrades für den Server auf dem Primärknoten finden Sie in Upgrade für IBM Spectrum Protect durchführen.
5. Nachdem die Durchführung des Upgrades abgeschlossen ist, führen Sie die Schritte nach dem Upgrade aus, um sicherzustellen, dass das Upgrade auf dem Primärknoten erfolgreich durchgeführt wurde.
6. Stoppen Sie den Server und heben Sie die Bereitstellung der Server-Mountpunkte auf dem Primärknoten auf.
7. Stellen Sie die Server-Mountpunkte auf dem Sekundärknoten bereit.
8. Wenn Sie für einen Server ein Upgrade von Version 6 auf Version 7 durchführen, führen Sie die folgenden Schritte aus:
  - a. Deinstallieren Sie den Server.

Anweisungen finden Sie in Server der Version 6.2 deinstallieren.

- b. Installieren Sie den Server auf dem Sekundärknoten. Führen Sie die Anweisungen in Linux: Serverkomponenten installieren aus.

9. Informationen zur Durchführung eines Upgrades für den Server auf dem Sekundärknoten finden Sie in Upgrade für den Server durchführen.
10. Nachdem die Durchführung des Upgrades abgeschlossen ist, führen Sie die Schritte nach dem Upgrade aus, um sicherzustellen, dass das Upgrade auf dem Sekundärknoten erfolgreich durchgeführt wurde.
11. Heben Sie die Bereitstellung der Server-Mountpunkte auf dem Sekundärknoten auf.
12. Starten Sie die Tivoli System Automation-Domäne, indem Sie den Befehl `startrpdomain` ausgeben. Beispielsweise wird mit dem folgenden Befehl die Domäne `tsa_domain` gestartet:

```
startrpdomain tsa_domain
```

13. Starten Sie die Serverressourcen, indem Sie den Befehl `chrg -o Online tsm-tsminst1-rg` ausgeben. Beispielsweise werden mit dem folgenden Befehl die Ressourcen in der Ressourcengruppe `tsm-tsminst1-rg` gestartet:

```
chrg -o Online tsm-tsminst1-rg
```

 Windows-Betriebssysteme




## Windows-Clusterumgebung konfigurieren



---

Sie können einen IBM Spectrum Protect-Server für Windows in einer Microsoft-Failoverclusterumgebung konfigurieren. Windows-Clusterumgebungen bestehen aus Komponenten, wie beispielsweise IBM Spectrum Protect-Servern, Hardware und Software. Wenn diese Komponenten mit demselben Plattensystem verbunden sind, wird die Ausfallzeit auf ein Mindestmaß reduziert.

Microsoft-Software hilft beim Konfigurieren, Überwachen und Steuern von Anwendungen und Hardwarekomponenten, die in einem Windows-Cluster implementiert sind. Der Administrator verwendet die Microsoft-Cluster-Administratorschnittstelle und IBM Spectrum Protect, um Cluster-Aufteilungen zu kennzeichnen und um das Übernahmemuster zu definieren.

IBM Spectrum Protect unterstützt die Bandübernahme für eine Clusterumgebung unter Verwendung einer Fibre Channel- oder SCSI-Verbindung. Obwohl Microsoft-Failovercluster nicht die Übernahme von Bandeinheiten unterstützen, kann die Übernahmekonfiguration durch die Microsoft Cluster Administrator-Schnittstelle überwacht werden, nachdem sie über IBM Spectrum Protect konfiguriert wurde.

-  **Übersicht über die Microsoft-Failoverclusterumgebung**  
Mit einem Microsoft Failovercluster-Manager können Sie IBM Spectrum Protect-Server-Cluster-Ressourcen in eine Clustergruppe stellen. Die IBM Spectrum Protect-Clustergruppe verfügt über einen Netznamen, eine IP-Adresse, eine oder mehrere physische Platten, einen DB2-Server und einen IBM Spectrum Protect-Server-Service.
-  **Bandübernahme für Knoten in einem Cluster**  
Gruppen in einem Cluster können auf andere Knoten übertragen werden, wenn der Knoten, auf dem sich die Gruppen befinden, fehlschlägt.
-  **Planung für eine Clusterumgebung**  
Die Konfiguration in einer Clusterumgebung bedarf einer sorgfältigen Planung, um die optimale Leistung Ihres Systems

- gewährleisten zu können. Ob Sie Ihr System für Cluster konfigurieren, hängt von Ihren Geschäftsanforderungen ab.
-  Windows-Betriebssysteme IBM Spectrum Protect in einem Microsoft Failovercluster konfigurieren  
Sie müssen sicherstellen, dass Ihr Cluster korrekt installiert und konfiguriert ist, bevor Sie IBM Spectrum Protect installieren.
-  Windows-Betriebssysteme Clusterumgebung verwalten  
Nach der Konfiguration Ihres ersten Clusters oder Ihrer ersten Cluster ist der Verwaltungsaufwand minimal.

 Windows-Betriebssysteme

## Übersicht über die Microsoft-Failoverclusterumgebung

Mit einem Microsoft Failovercluster-Manager können Sie IBM Spectrum Protect-Server-Cluster-Ressourcen in eine Clustergruppe stellen. Die IBM Spectrum Protect-Clustergruppe verfügt über einen Netznamen, eine IP-Adresse, eine oder mehrere physische Platten, einen DB2-Server und einen IBM Spectrum Protect-Server-Service.

Der Netzname der IBM Spectrum Protect-Instanz ist unabhängig vom Namen des physischen Knotens, auf dem die IBM Spectrum Protect-Clustergruppe ausgeführt wird. Clients stellen die Verbindung zu einem IBM Spectrum Protect-Server nicht unter Verwendung des Windows-Knotennamens, sondern unter Verwendung des Netznamens der Instanz her. Der Netzname der Instanz ist einem Primär- oder Ausweichknoten zugeordnet. Die Zuordnung ist davon abhängig, welcher Knoten Eigner der Clustergruppe ist. Jeder Client, der Windows Internet Name Service (WINS) oder Verzeichnisservices zum Lokalisieren von Servern verwendet, kann den IBM Spectrum Protect-Cluster-Server automatisch verfolgen, wenn er zwischen den Knoten versetzt wird. Sie können den Cluster-Server automatisch verfolgen, ohne den Client ändern oder rekonfigurieren zu müssen.

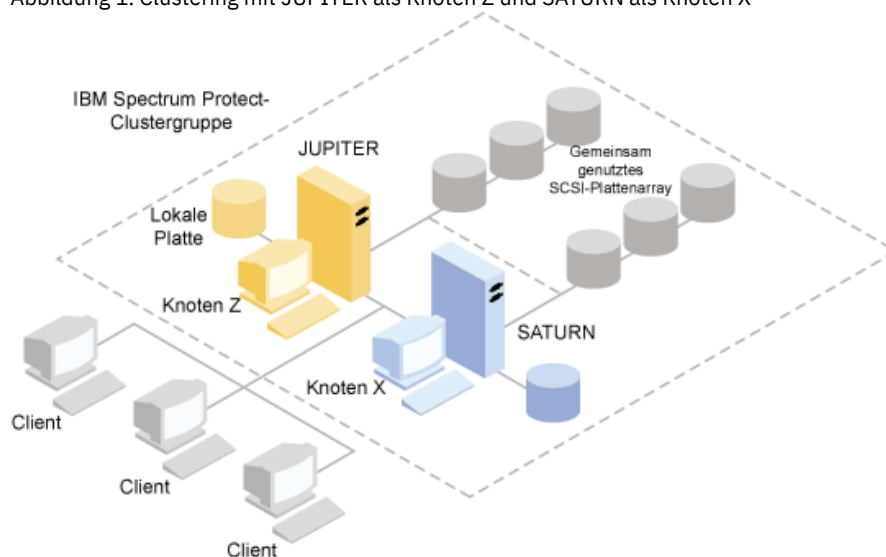
Jede IBM Spectrum Protect-Clustergruppe verfügt über ihre eigene Platte als Teil einer Clusterressourcengruppe. IBM Spectrum Protect-Clustergruppen können keine Daten zwischen Clustergruppen gemeinsam nutzen. Die Datenbank, die aktiven Protokolldateien und die Wiederherstellungsprotokolle sowie die Gruppe von Speicherpooldatenträgern sind für jeden IBM Spectrum Protect-Server, der in einer Clustergruppe konfiguriert ist, auf einer separaten Platte gespeichert. Die Clustergruppe, in der der Server konfiguriert ist, ist Eigner dieser Platte.

Hinweis: Microsoft Failovercluster-Manager unterstützt als Ressource nur eine IP-Adresse. Demzufolge muss jeder IBM Spectrum Protect-Server, der in einem Cluster ausgeführt wird, sein unterstütztes Kommunikationsverfahren ausschließlich auf TCP/IP beschränken. Jeder Client, der nicht TCP/IP als Kommunikationsverfahren verwendet, kann die IBM Spectrum Protect-Clustergruppe nicht erreichen, wenn eine Übernahme (Failover) durch den anderen Clusterknoten erfolgt.

Das folgende Beispiel zeigt, wie ein Microsoft Failovercluster-Manager für einen IBM Spectrum Protect-Cluster-Server funktioniert.

Angenommen, ein IBM Spectrum Protect-Cluster-Server mit dem Namen JUPITER wird auf dem Knoten Z ausgeführt und ein IBM Spectrum Protect-Cluster-Server mit dem Namen SATURN wird auf dem Knoten X ausgeführt. Clients stellen eine Verbindung zum IBM Spectrum Protect-Server JUPITER und zum IBM Spectrum Protect-Server SATURN her, ohne zu wissen, auf welchem Knoten sich ihr Server befindet.

Abbildung 1. Clustering mit JUPITER als Knoten Z und SATURN als Knoten X




Wenn in einer der Software- oder Hardwareressourcen ein Fehler auftritt, erfolgt eine Übernahme. Ressourcen, wie beispielsweise Anwendungen, Platten und eine IP-Adresse, werden von dem fehlerhaften Knoten in den verbleibenden Knoten versetzt. Der verbleibende Knoten führt Folgendes aus:

- Er übernimmt die IBM Spectrum Protect-Clustergruppe.
- Er schaltet die Plattenressourcen, die Netzressourcen und die DB2-Ressourcen online.

- Er startet den IBM Spectrum Protect-Service erneut.
- Er stellt Zugriff auf Administratoren und Clients bereit.

Wenn Knoten X ausfällt, übernimmt Knoten Z die Ausführung von SATURN. Für einen Client erscheint dies exakt so, als würde Knoten X ausgeschaltet und sofort wieder eingeschaltet. Clients verlieren alle Verbindungen zu SATURN, und alle aktiven Transaktionen werden rückgängig gemacht. Clients müssen die Verbindung zu SATURN wiederherstellen, nachdem die Verbindung verloren gegangen ist. Der Standort von SATURN ist für den Client nicht ersichtlich.


 Windows-Betriebssysteme

## Bandübernahme für Knoten in einem Cluster

---

Gruppen in einem Cluster können auf andere Knoten übertragen werden, wenn der Knoten, auf dem sich die Gruppen befinden, fehlschlägt.

Ein Knoten kann als Host für physische oder logische Einheiten, die als Ressourcen bezeichnet werden, dienen. Administratoren fassen diese Clusterressourcen in Funktionseinheiten zusammen, die als Gruppen bezeichnet werden, und ordnen diese Gruppen einzelnen Knoten zu. Wenn ein Knoten ausfällt, überträgt der Server-Cluster die vom Knoten gehosteten Gruppen auf andere Knoten im Cluster. Dieser Übertragungsprozess wird als *Übernahme* (Failover) bezeichnet. Der gegenteilige Prozess, *Rückübertragung* (Failback), findet statt, wenn der ausgefallene Knoten wieder aktiv wird und die Gruppen, die auf die anderen Knoten übertragen wurden, wieder auf den ursprünglichen Knoten zurückübertragen werden.

-  Windows-Betriebssysteme Fibre Channel-Bandübernahme  
IBM Spectrum Protect kann die Übernahme von direkt angeschlossenen Fibre Channel-Bandeinheiten und - Speicherarchivseinheiten auf einem Microsoft Windows-System in einer Clusterumgebung ohne zusätzliche Hardware handhaben.

 Windows-Betriebssysteme

## Planung für eine Clusterumgebung

---

Die Konfiguration in einer Clusterumgebung bedarf einer sorgfältigen Planung, um die optimale Leistung Ihres Systems gewährleisten zu können. Ob Sie Ihr System für Cluster konfigurieren, hängt von Ihren Geschäftsanforderungen ab.




Die Planung für eine Clusterkonfiguration muss gemäß Ihrer Umgebung erfolgen. Sie müssen sicherstellen, dass der korrekte Hardwaretyp und die geeignete Software verwendet werden. Darüber hinaus müssen Sie ein Übernahmemuster konfigurieren.

Wenn ein Knoten ausfällt oder offline geschaltet werden muss, welcher Knoten bzw. welche Knoten im Cluster übernimmt/übernehmen dann die Transaktionsverarbeitung? Bei einem Cluster mit zwei Knoten ist nur wenig Planung erforderlich. Bei einer komplexeren Anordnung sollten Sie darauf achten, wie Ihre Transaktionsverarbeitung am besten ausgeführt wird. Es muss eine Form des Lastausgleichs zwischen den Knoten vorliegen, damit die Spitzenleistung aufrecht erhalten wird. Es muss auch sichergestellt werden, dass Ihre Kunden keine Verzögerung und nur wenig Abfall der Produktivität wahrnehmen.


Für Microsoft Cluster Server und Microsoft Failovercluster benötigt jede IBM Spectrum Protect-Serverinstanz eine private Plattenressourcengruppe. Knoten können Plattenressourcen zwar gemeinsam nutzen, aber nur jeweils ein Knoten kann eine Platte aktiv steuern.

Achtung: Stellen Sie sicher, dass auf allen Computern im Cluster dieselbe Version von Windows (Windows 2012, Windows 2012 R2 und Windows 2016) installiert ist.

Ist eine Konfiguration besser als die andere? Um die optimale Installation zu ermitteln, müssen Sie einen Leistungs- und Kostenvergleich durchführen. Angenommen, es ist ein Cluster vorhanden, dem dem IBM Spectrum Protect-Server zugeordnet ist und über Knoten mit vergleichbarer Leistung verfügt. Während der Übernahme kann die Leistung einer Konfiguration abnehmen, weil ein einziger Knoten beide IBM Spectrum Protect-Clusterinstanzen handhaben muss. Wenn jeder Knoten im Normalbetrieb 100 Clients bearbeitet, muss ein Knoten während eines Fehlers 200 Clients handhaben.

-  Windows-Betriebssysteme Arbeitsblatt für die Clusterkonfiguration  
Notieren Sie Ihre Antworten auf die folgenden Planungsfragen, bevor Sie die Clusterkonfiguration definieren.
-  Windows-Betriebssysteme Cluster-Hardware- und -Softwarekonfiguration planen  
Die Cluster-Hardware- und -Softwarekonfiguration wird während des Planungsstadiums und vor der eigentlichen Installation bestimmt.
-  Windows-Betriebssysteme IBM Spectrum Protect im Microsoft Failovercluster konfigurieren  
Die IBM Spectrum Protect-Clusterkonfigurationsprozedur muss für die Gruppe von Knoten ausgeführt werden, die eine IBM Spectrum Protect-Clustergruppe hostet.

### Zugehörige Informationen:

 IBM Spectrum Protect Supported Operating Systems

## Arbeitsblatt für die Clusterkonfiguration

Notieren Sie Ihre Antworten auf die folgenden Planungsfragen, bevor Sie die Clusterkonfiguration definieren.

1. Welche Clusterlösung ist für Ihre Geschäftsanforderungen am besten geeignet?
2. Welchen Typ von Übernahmemuster benötigen Sie?

Auch die Verwendung der Bandübernahmeunterstützung wirkt sich auf das Muster aus.

3. Wird Bandübernahmeunterstützung benötigt?

Berücksichtigen Sie, wie Bandeinheiten von den IBM Spectrum Protect-Clusterinstanzen verwendet werden. Durch die Art und Weise, auf die Bandeinheiten von Clusterinstanzen verwendet werden, kann die Anzahl der Knoten im Übernahmemuster auf zwei begrenzt werden.

4. Welche Ressourcen sollen für IBM Spectrum Protect dediziert werden?

| Ressourcentyp  | Ressourcenname |
|--|----------------|
| Clusterressourcengruppe                                |                |
| Ressourcen der physischen Platte                       |                |
| IP-Adresse   |                |
| Teilnetzmaske  |                |
| Netz   |                |
| Netzname (Servername)                                  |                |
| Knoten   |                |
| Bandübernahme (optional): Einheitenname - beide Knoten |                |

## Cluster-Hardware- und -Softwarekonfiguration planen

Die Cluster-Hardware- und -Softwarekonfiguration wird während des Planungsstadiums und vor der eigentlichen Installation bestimmt.

### Vorgehensweise

Anhand der folgenden Richtlinien kann bestimmt werden, welche Ressourcen für einen erfolgreichen IBM Spectrum Protect-Cluster benötigt werden:

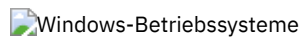
1. Legen Sie die erforderliche Clusterkonfiguration für Server fest, die Platteneinheiten verwenden. Jede IBM Spectrum Protect-Clusterinstanz benötigt eine separate Gruppe von Plattenressourcen auf dem gemeinsamen Plattensubsystem. Unter Umständen können Probleme auftreten, wenn Sie das E/A-Subsystem als einen einzigen großen Bereich konfigurieren. Dies ist beispielsweise der Fall, wenn Sie einen Cluster mit zwei Servern konfigurieren und sich später für eine Erweiterung auf einen Cluster mit vier Servern entscheiden.
2. Identifizieren Sie die Datenträgerressourcen, die IBM Spectrum Protect zugeteilt werden sollen. Teilen Sie nicht eine gemeinsam genutzte Platte in mehrere Partitionen auf, wobei jede Partition einer anderen Anwendung und somit einer anderen Clustergruppe zugeordnet wird.

Beispielsweise könnte Anwendung A, eine stabile Anwendung, aufgrund eines Softwareproblems mit Anwendung B zur Übernahme gezwungen werden. Diese Übernahme könnte erfolgen, wenn beide Anwendungen Partitionen verwenden, die Teil derselben physischen Platte sind. Dieses Problem hat zur Folge, dass die Cluster-Services Anwendung B und ihre zusätzlich erforderliche Plattenressource durch Übernahme übertragen. Da sich die Partitionen auf demselben physischen Laufwerk befinden, wird auch Anwendung A zur Übernahme gezwungen. Aus diesem Grund sollten Sie beim Installieren und Konfigurieren einer IBM Spectrum Protect-Anwendung eine gemeinsam genutzte Platte als Ressource zuordnen, für die, falls erforderlich, eine Übernahme erfolgen kann.

3. Stellen Sie sicher, dass für jede IBM Spectrum Protect-Serverinstanz, die Sie konfigurieren, eine IP-Adresse und ein Netzname angegeben werden. Für einen Cluster mit zwei IBM Spectrum Protect-Clusterinstanzen sind zwei Netznamen erforderlich.
4. Erstellen Sie eine Clusterressourcengruppe und versetzen Sie Plattenressourcen auf sie. Jede IBM Spectrum Protect-Serverinstanz erfordert eine Clusterressourcengruppe. Anfänglich darf die Gruppe nur Plattenressourcen enthalten. Sie können gegebenenfalls auch eine vorhandene Ressourcengruppe umbenennen, die lediglich Plattenressourcen enthält.

- IBM Spectrum Protect wird auf jedem Knoten im Cluster auf einer lokalen Platte installiert. Legen Sie fest, welche Platte auf jedem Knoten verwendet werden soll. Verwenden Sie auf jedem System denselben Laufwerksbuchstaben. Wenn der IBM Spectrum Protect-Server in einer Clusterumgebung installiert wird, muss die Option SANDISCOVERY auf ON gesetzt werden. Standardmäßig ist diese Option auf OFF gesetzt.
- Wenn Sie sich dafür entscheiden, die IBM Spectrum Protect-Bandübernahmeunterstützung nicht zu verwenden, können Sie Bandeinheiten mithilfe einer der folgenden Konfigurationen anschließen:

| Konfiguration   | Vorteile und Nachteile  | Erforderlicher Plattenspeicherplatz   | Vorgehensweise zur Aktivierung der Umlagerung  | Maßnahmen bei Auftreten einer Übernahme  |
|---|---|---|--|--|
| Anschluss an den Knoten, auf dem die IBM Spectrum Protect-Serverinstanz aktiv ist.  | Diese Konfiguration ermöglicht leistungsfähige Sicherungs- und Zurückschreibungsoperationen. Sie ist jedoch nicht vollständig automatisiert, da ein Bedieneingriff erforderlich ist, um eine Übernahme zu handhaben, wenn Verzögerungen durch eine Reparatur auftreten. | Definieren Sie genügend Datenträgerspeicherplatz, für den Daten plattenbasiert sind, um Daten von durchschnittlich mehr als zwei Tagen aufbewahren zu können. | Definieren Sie eine Speicherpoolhierarchie, damit Daten effizient auf die Bandeinheit versetzt werden.                       | Trennen Sie die Bandeinheit manuell und schließen Sie sie wieder an den Knoten an, auf dem der Server aktiviert wurde. |
| Anschluss an ein drittes System ohne Clustering, auf dem eine weitere Instanz des IBM Spectrum Protect-Servers aktiv ist. | Diese Konfiguration ist unter Umständen in Installationen mit Übertragungen mit geringer Bandbreite zwischen den Servern im Cluster und dem Server mit dem Bandeinheitencontroller nicht durchführbar.  | Definieren Sie genügend Datenträgerspeicherplatz, für den Daten plattenbasiert sind, um Daten von durchschnittlich mehr als zwei Tagen aufbewahren zu können. | Verwenden Sie die virtuellen Datenträger, um die Daten von den lokalen Plattendatenträgern auf die Bandeinheit zu versetzen. | Es ist keine Aktion erforderlich; der aktivierte Server verwendet weiterhin die virtuellen Datenträger.                |

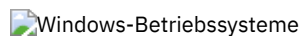


## IBM Spectrum Protect im Microsoft Failovercluster konfigurieren

Die IBM Spectrum Protect-Clusterkonfigurationsprozedur muss für die Gruppe von Knoten ausgeführt werden, die eine IBM Spectrum Protect-Clustergruppe hostet.

Die Schritte für die Prozedur sind von dem Knoten abhängig, den Sie gerade konfigurieren. Wenn Sie den Primärknoten in der Gruppe konfigurieren, wird die IBM Spectrum Protect-Serverinstanz erstellt und konfiguriert. Wenn Sie die übrigen Knoten in der Gruppe konfigurieren, wird jeder Knoten mithilfe einer spezifischen Methode aktualisiert. Die Art und Weise, auf die der Knoten aktualisiert wird, ermöglicht es dem Knoten, die auf dem Primärknoten erstellte IBM Spectrum Protect-Serverinstanz zu hosten. Ein IBM Spectrum Protect-Server muss auf dem ersten Knoten in der Gruppe installiert und konfiguriert werden, bevor die übrigen Knoten in der Gruppe konfiguriert werden. Wird diese Bedingung nicht erfüllt, schlägt die Konfiguration fehl.

Wenn Sie mehrere IBM Spectrum Protect-Clustergruppen konfigurieren, müssen Sie sicherstellen, dass eine IBM Spectrum Protect-Clustergruppe vollständig konfiguriert wird, bevor Sie mit der nächsten Gruppe fortfahren. Da Sie separate IP-Adressen und Netznamen für jede IBM Spectrum Protect-Clustergruppe verwenden, verringern Sie die Fehlerwahrscheinlichkeit, indem Sie jede Clustergruppe separat konfigurieren.



## IBM Spectrum Protect in einem Microsoft Failovercluster konfigurieren

Sie müssen sicherstellen, dass Ihr Cluster korrekt installiert und konfiguriert ist, bevor Sie IBM Spectrum Protect installieren.

### Vorgehensweise


Um IBM Spectrum Protect in einem Microsoft Failovercluster zu konfigurieren, führen Sie die folgenden Schritte aus:

- Stellen Sie sicher, dass das Windows-Betriebssystem auf allen Computern installiert ist, die zum Cluster gehören. Aktuelle Informationen zu unterstützten Windows-Betriebssystemen finden Sie in der Technote 1243309.
- Melden Sie sich mit der Domänenbenutzer-ID an. Der Domänenbenutzer muss sich in derselben Domäne wie der IBM Spectrum Protect-Server befinden.
- Stellen Sie sicher, dass der Failovercluster für alle Computer im Cluster installiert und konfiguriert ist.  
Wenn Sie planen, den IBM Spectrum Protect-Server unter dem Betriebssystem Windows Server 2012 zu installieren, installieren Sie zunächst den Server für Failoverclusterautomatisierung und die Failovercluster-Befehlsschnittstelle. Um diese Komponenten

zu installieren, geben Sie in Windows 2.0 PowerShell die folgenden Befehle aus:

```
Install-WindowsFeature -Name RSAT-Clustering-AutomationServer  
Install-WindowsFeature -Name RSAT-Clustering-CmdInterface
```

4. Prüfen Sie, ob jeder Knoten und jede gemeinsam genutzte Platte im Cluster betriebsbereit ist.
  5. Stellen Sie sicher, dass die gemeinsam genutzten Bandeinheiten betriebsbereit sind, wenn IBM Spectrum Protect-Bandübernahmeunterstützung verwendet wird.
-  Windows-Betriebssysteme Microsoft Failoverclustergruppe für einen virtuellen Basisserver vorbereiten  
Jede IBM Spectrum Protect-Serverinstanz erfordert eine Clusterressourcengruppe.
  -  Windows-Betriebssysteme IBM Spectrum Protect in einem Microsoft Failovercluster installieren  
Installieren Sie den IBM Spectrum Protect-Server auf jedem Knoten in dem Cluster, der einen IBM Spectrum Protect-Cluster-Server enthält.
  -  Windows-Betriebssysteme IBM Spectrum Protect-Server für einen Microsoft Failovercluster auf dem Primärknoten initialisieren  
Nachdem Sie IBM Spectrum Protect auf den Knoten im Cluster installiert haben, müssen Sie den Server auf dem Primärknoten initialisieren.
  -  Windows-Betriebssysteme Konfiguration von IBM Spectrum Protect in einem Microsoft Failovercluster überprüfen  
Nachdem Sie die Konfiguration von IBM Spectrum Protect in einem Microsoft Failovercluster beendet haben, können Sie das Zusammenfassungsfenster 'Failovercluster-Manager' überprüfen. Stellen Sie sicher, dass das Clustering erfolgreich ausgeführt wurde und der IBM Spectrum Protect-Server gestartet wurde.
  -  Windows-Betriebssysteme Übernahmetest für Ihren Cluster ausführen  
Führen Sie nach Abschluss der Clusterkonfiguration einen Übernahmetest aus, um sicherzustellen, dass die Knoten ordnungsgemäß arbeiten.

 Windows-Betriebssysteme

## Microsoft Failoverclustergruppe für einen virtuellen Basisserver vorbereiten

Jede IBM Spectrum Protect-Serverinstanz erfordert eine Clusterressourcengruppe.

### Vorbereitende Schritte

Verwenden Sie das Programm 'Failovercluster-Manager' auf dem Computer, der Eigner der gemeinsam genutzten Platte oder Bandressource ist, um Ihre Ressourcengruppe vorzubereiten. Anfänglich darf die Gruppe nur Plattenressourcen enthalten. Sie können eine Gruppe erstellen und Plattenressourcen auf sie versetzen. Sie können auch eine vorhandene Ressourcengruppe umbenennen, die nur Plattenressourcen enthält.

Bei der Erstellung Ihrer Ressourcengruppen müssen Sie Folgendes berücksichtigen:

- Stellen Sie sicher, dass jede Ressourcengruppe über einen eindeutigen Namen verfügt. Ändern Sie die Namen nach der Erstellung der Gruppe nicht, da dies eine fehlerhafte Konfiguration zur Folge haben kann.
- Stellen Sie sicher, dass alle Knoten im Cluster online sind.
- Stellen Sie sicher, dass die Gruppe online ist und den Knoten als Eigner hat, auf dem die erste Serverinstanz installiert wird.

### Vorgehensweise

Um eine Ressourcengruppe für die Clusterkonfiguration vorzubereiten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie das Programm 'Failovercluster-Manager'. Klicken Sie mit der rechten Maustaste auf Dienste und Anwendungen und wählen Sie dann Weitere Aktionen > Leeren Dienst oder leere Anwendung erstellen aus.
2. Klicken Sie mit der rechten Maustaste auf Neuer Dienst oder neue Anwendung, wählen Sie Namen ändern aus und geben Sie einen neuen Namen, wie beispielsweise TSMGROUP, für die Ressourcengruppe an.
3. Klicken Sie mit der rechten Maustaste auf die Ressourcengruppe TSMGROUP und wählen Sie Speicherbereich hinzufügen aus.
4. Wählen Sie in der Anzeige 'Speicherbereich hinzufügen' den gemeinsam genutzten Datenträger oder die gemeinsam genutzten Datenträger für IBM Spectrum Protect aus und klicken Sie auf OK. Die Ressourcengruppe TSMGROUP, die die gerade hinzugefügten Plattendatenträger enthält, wird angezeigt.

 Windows-Betriebssysteme

## IBM Spectrum Protect in einem Microsoft Failovercluster installieren

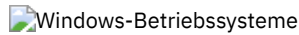
Installieren Sie den IBM Spectrum Protect-Server auf jedem Knoten in dem Cluster, der einen IBM Spectrum Protect-Cluster-Server enthält.

## Vorgehensweise

---

Führen Sie die folgenden Schritte für jeden Knoten in Ihrem Cluster aus, um den IBM Spectrum Protect-Server zu installieren:

1. Melden Sie sich mit einer Administrator-ID oder einer Domänenbenutzer-ID an. Der Domänenbenutzer muss ein Mitglied der Gruppe der Domänenadministratoren sein.
2. Installieren Sie den IBM Spectrum Protect-Server auf einer lokalen Platte auf jedem Knoten. Verwenden Sie für jeden Knoten denselben Laufwerksbuchstaben für die lokale Platte.
3. Starten Sie das System nach Beendigung der Serverinstallation erneut.



## IBM Spectrum Protect-Server für einen Microsoft Failovercluster auf dem Primärknoten initialisieren

---

Nachdem Sie IBM Spectrum Protect auf den Knoten im Cluster installiert haben, müssen Sie den Server auf dem Primärknoten initialisieren.

### Vorgehensweise

---

1. Stellen Sie sicher, dass alle Systeme nach der Installation erneut gestartet werden. Stellen Sie sicher, dass alle Systeme korrekt ausgeführt werden.
2. Melden Sie sich mit einer Administrator-ID oder einer Domänenbenutzer-ID an. Der Domänenbenutzer muss sich in derselben Domäne wie der IBM Spectrum Protect-Server befinden.
3. Öffnen Sie das Programm Failovercluster-Manager und stellen Sie sicher, dass die Ressourcen online und für den Primärknoten verfügbar sind.
4. Beginnen Sie die Initialisierungsprozedur auf dem Primärknoten in Ihrem Cluster. Stellen Sie im Programm Failovercluster-Manager sicher, dass der Eigner der Ressourcengruppe der Primärknoten in Ihrem Cluster ist.
5. Klicken Sie im Menü Start auf Alle Programme > IBM Spectrum Protect-Server > Konfigurationsassistent.
6. Befolgen Sie die Anweisungen im Assistenten, indem Sie jeweils auf Weiter klicken, während Sie den Assistenten schrittweise durchlaufen. Wenn Sie zur Eingabe der Benutzer-ID aufgefordert werden, geben Sie den Namen des Domänenkontos ein, das dem Cluster zugeordnet werden soll.
7. Wenn die Initialisierung abgeschlossen ist, klicken Sie auf Fertig.



## Konfiguration von IBM Spectrum Protect in einem Microsoft Failovercluster überprüfen

---

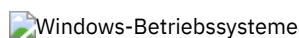
Nachdem Sie die Konfiguration von IBM Spectrum Protect in einem Microsoft Failovercluster beendet haben, können Sie das Zusammenfassungsfenster 'Failovercluster-Manager' überprüfen. Stellen Sie sicher, dass das Clustering erfolgreich ausgeführt wurde und der IBM Spectrum Protect-Server gestartet wurde.

### Vorgehensweise

---

Um zu überprüfen, ob die IBM Spectrum Protect-Serverinstanz in einem Microsoft Failovercluster erstellt und korrekt konfiguriert wurde, führen Sie die folgenden Schritte aus:

1. Wählen Sie im Failovercluster-Manager die Serverinstanz aus. Der von Ihnen konfigurierte Netzname wird im Bereich 'Servername' angezeigt.
2. Stellen Sie sicher, dass die Serverinstanz und die IBM® DB2-Serverressource im Bereich 'Andere Ressourcen' angezeigt werden.
3. Klicken Sie mit der rechten Maustaste auf die IBM Spectrum Protect-Serverinstanz und wählen Sie Diese Ressource online schalten aus.



## Übernahmetest für Ihren Cluster ausführen


---

Führen Sie nach Abschluss der Clusterkonfiguration einen Übernahmetest aus, um sicherzustellen, dass die Knoten ordnungsgemäß arbeiten.

### Vorgehensweise

---

1. Öffnen Sie Failovercluster-Manager. Klicken Sie unter 'Andere Ressourcen' mit der rechten Maustaste auf die Ressource für die IBM Spectrum Protect-Instanz(x). Wählen Sie Diese Ressource online schalten aus.
2. Um die Übernahme zu testen, klicken Sie mit der rechten Maustaste auf die IBM Spectrum Protect-Clusterressourcengruppe und wählen Sie Diesen Dienst oder diese Anwendung in einen anderen Knoten verschieben aus.
3. Prüfen Sie, ob die Übernahme vom zweiten Knoten auf den ersten Knoten erfolgreich ausgeführt wird.

 Windows-Betriebssysteme

## Clusterumgebung verwalten

---

Nach der Konfiguration Ihres ersten Clusters oder Ihrer ersten Cluster ist der Verwaltungsaufwand minimal.

Überprüfen Sie Ihr Windows-Ereignisprotokoll regelmäßig, wenn nicht sogar täglich, um die Aktivitäten der Knoten im Cluster zu überwachen. Überprüfen Sie mithilfe des Protokolls, ob ein Knoten fehlschlägt und Verwaltung erfordert.

Die folgenden Themen beschreiben Situationen, die Auswirkungen auf die Konfiguration oder das Format Ihres Clusters haben können, nachdem er betriebsbereit ist.

-  **Windows-Betriebssysteme** Vorhandenen IBM Spectrum Protect-Server in einen Cluster umlagern  
Der Grund für das Versetzen von Clientdaten in einen Cluster ist mit dem Grund für das Hinzufügen eines Servers zu einem Cluster vergleichbar. Es dient der Verbesserung der Datenverfügbarkeit und -zuverlässigkeit für alle Benutzer. Da der Server Teil des Clusters ist, wird eine zusätzliche Sicherheitsstufe bereitgestellt, indem sichergestellt wird, dass keine Transaktionen aufgrund eines ausgefallenen Servers verloren gehen. Durch das von Ihnen definierte Übernahmemuster werden zukünftige Fehler verhindert.
-  **Windows-Betriebssysteme** IBM Spectrum Protect-Server mit Sicherung und Zurückschreibung hinzufügen  
Wenn Ihre Hardwareressourcen begrenzt sind, können Sie mit einer Sicherungs- und Zurückschreibungsprozedur einen vorhandenen IBM Spectrum Protect-Server einem Cluster hinzufügen.
-  **Windows-Betriebssysteme** Virtuellen IBM Spectrum Protect-Server in einem Cluster verwalten  
Bei den meisten Tasks können Sie einen virtuellen IBM Spectrum Protect-Server wie einen Server ohne Cluster verwalten. Zur Ausführung von Tasks, wie beispielsweise das Starten und Stoppen des Servers oder das Versetzen einer Ressourcengruppe auf einen anderen Knoten zur Ausführung der Systemwartung, müssen Sie die Microsoft Cluster Administrator-Schnittstelle verwenden.
-  **Windows-Betriebssysteme** Bandübernahme in einem Cluster verwalten  
Überprüfen Sie im Rahmen Ihrer regelmäßigen Routinearbeiten das Ereignisprotokoll, um sicherzustellen, dass die Konfiguration ordnungsgemäß funktioniert. Wenn ein Serverfehler auftritt, wird der Fehler protokolliert. Das Protokoll liefert Ihnen Informationen, die erläutern, warum der Fehler aufgetreten ist.
-  **Windows-Betriebssysteme** Fehlerbehebung mit dem IBM Spectrum Protect-Clusterprotokoll  
Die IBM Spectrum Protect-Clusterressourcen-DLL meldet Ereignisse und Fehler an das Clusterprotokoll. Das Clusterprotokoll ist ein nützliches Tool zur Fehlerbehebung. Wenn dieses Protokoll aktiviert ist, zeichnet es die Aktionen aller Komponenten des Cluster-Service (Clusterdienst) als Ergebnis der einzelnen Aktionen auf.

 Windows-Betriebssysteme

## Vorhandenen IBM Spectrum Protect-Server in einen Cluster umlagern


---

Der Grund für das Versetzen von Clientdaten in einen Cluster ist mit dem Grund für das Hinzufügen eines Servers zu einem Cluster vergleichbar. Es dient der Verbesserung der Datenverfügbarkeit und -zuverlässigkeit für alle Benutzer. Da der Server Teil des Clusters ist, wird eine zusätzliche Sicherheitsstufe bereitgestellt, indem sichergestellt wird, dass keine Transaktionen aufgrund eines ausgefallenen Servers verloren gehen. Durch das von Ihnen definierte Übernahmemuster werden zukünftige Fehler verhindert.

### Informationen zu diesem Vorgang

---

Um einen vorhandenen IBM Spectrum Protect-Server in einen Cluster umzulagern, können Sie entweder die Clients versetzen oder eine Sicherungs- und Zurückschreibungsprozedur ausführen. Ihre Auswahl hängt in erster Linie von der Verfügbarkeit und Kapazität der anderen IBM Spectrum Protect-Server-Computer an Ihrem Standort und Ihren Kenntnissen der Sicherungs- und Zurückschreibungsprozedur ab.

-  **Windows-Betriebssysteme** Clients versetzen  
Wenn Sie Clients von einem IBM Spectrum Protect-Server-Computer ohne Clustering auf einen Computer mit Clustering versetzen, können Sie Ihre Benutzer ohne Serviceunterbrechung schrittweise auf das neue System versetzen. Sie müssen jedoch über die korrekte Hardware verfügen, die erforderlich ist, um zwei IBM Spectrum Protect-Server gleichzeitig auszuführen.

#### Zugehörige Tasks:

Server installieren und Upgrade für den Server durchführen



## IBM Spectrum Protect-Server mit Sicherung und Zurückschreibung hinzufügen

---

Wenn Ihre Hardwareressourcen begrenzt sind, können Sie mit einer Sicherungs- und Zurückschreibungsprozedur einen vorhandenen IBM Spectrum Protect-Server einem Cluster hinzufügen.

### Informationen zu diesem Vorgang

---

Angenommen, mit Ausnahme der beiden Serversysteme, die für das Clustering konfiguriert werden sollen, verfügen Sie über keine andere Hardware. Sie planen, den Computer, auf dem der IBM Spectrum Protect-Server ausgeführt wird, als Knoten zu verwenden. Führen Sie diese Prozedur aus, um IBM Spectrum Protect vom Computer zu entfernen und erneut im Cluster zu installieren:

### Vorgehensweise

---

1. Sichern Sie alle Plattenspeicherpools in einem Kopierspeicherpool.
2. Sichern Sie die Datenbank des vorhandenen IBM Spectrum Protect-Servers.
3. Führen Sie die Installation und Konfiguration des Clusters durch.
4. Schreiben Sie die Datenbank auf den IBM Spectrum Protect-Cluster-Server zurück.
5. Schreiben Sie die Datenträger des Plattenspeicherpools vom Kopierspeicherpool zurück.
6. Löschen Sie den alten Server, nachdem Sie überprüft haben, ob alle Daten auf dem Cluster-Server vorhanden sind.

## Virtuellen IBM Spectrum Protect-Server in einem Cluster verwalten

---

Bei den meisten Tasks können Sie einen virtuellen IBM Spectrum Protect-Server wie einen Server ohne Cluster verwalten. Zur Ausführung von Tasks, wie beispielsweise das Starten und Stoppen des Servers oder das Versetzen einer Ressourcengruppe auf einen anderen Knoten zur Ausführung der Systemwartung, müssen Sie die Microsoft Cluster Administrator-Schnittstelle verwenden.

### Informationen zu diesem Vorgang

---

Die Microsoft Cluster Administrator-Schnittstelle ist über die Programmgruppe 'Verwaltung' verfügbar. Die Schnittstelle ist eine Detailsicht der Konfiguration eines virtuellen Servers. Die Konfiguration des virtuellen Servers umfasst Details wie die physischen Windows-Server, die Teil des Clusters sind, sowie ihre Ressourcen, ihre Netzverbindungen und ihren Status. Mithilfe dieser Schnittstelle können Sie die Komponenten der Konfiguration eines virtuellen Servers anzeigen und einen virtuellen Server starten oder stoppen oder ein Failback für den Server ausführen. Verwalten Sie einen virtuellen IBM Spectrum Protect-Server mithilfe der Microsoft Cluster Administrator-Schnittstelle, um Serverfehler und Fehlernachrichten zu verhindern. Wenn Sie beispielsweise den Windows-Dienststeuerungsmanager (Service Control Manager) zum Herunterfahren des Servers verwenden, empfangen Sie unter Umständen Nachrichten, die angeben, dass der Server fehlgeschlagen ist.

Falls gewünscht, können Sie einen virtuellen IBM Spectrum Protect-Server versetzen, wenn der Windows-Server als Primärknoten agiert und dieser Server eine Hardware- oder Systemwartung erfordert. Verwenden Sie die Microsoft Cluster Administrator-Schnittstelle, um die Verwaltung des virtuellen IBM Spectrum Protect-Servers auf den Sekundärknoten übertragen, bis die Wartung beendet ist.

## Bandübernahme in einem Cluster verwalten

---

Überprüfen Sie im Rahmen Ihrer regelmäßigen Routinearbeiten das Ereignisprotokoll, um sicherzustellen, dass die Konfiguration ordnungsgemäß funktioniert. Wenn ein Serverfehler auftritt, wird der Fehler protokolliert. Das Protokoll liefert Ihnen Informationen, die erläutern, warum der Fehler aufgetreten ist.

### Informationen zu diesem Vorgang

---

Manchmal muss ein Knoten wieder in den Cluster eingebunden werden, z. B. in den folgenden Fällen:

- Ein Knotenfehler ist aufgetreten.
- Eine neue Fibre Channel-HBA-Karte (Ausrüstungsänderungen) wird hinzugefügt.

### Vorgehensweise

---

Führen Sie die folgenden Tasks in beliebiger Reihenfolge aus, um sicherzustellen, dass ein Knoten erfolgreich in den Cluster eingebunden werden kann:

- Aktualisieren Sie, falls erforderlich, das Laufwerk und das Speicherarchiv, die das IBM Spectrum Protect-Cluster-Tool verwenden.
- Schalten Sie den IBM Spectrum Protect-Server offline, bis der fehlerhafte Knoten wieder in den Cluster eingebunden wird. Mit dieser Aktion kann sichergestellt werden, dass der IBM Spectrum Protect-Server, der auf dem anderen Knoten ausgeführt wird, nicht betroffen ist.



## Fehlerbehebung mit dem IBM Spectrum Protect-Clusterprotokoll

---

Die IBM Spectrum Protect-Clusterressourcen-DLL meldet Ereignisse und Fehler an das Clusterprotokoll. Das Clusterprotokoll ist ein nützliches Tool zur Fehlerbehebung. Wenn dieses Protokoll aktiviert ist, zeichnet es die Aktionen aller Komponenten des Cluster-Service (Clusterdienst) als Ergebnis der einzelnen Aktionen auf.

Im Vergleich zum Ereignisprotokoll von Microsoft Windows ist das Clusterprotokoll eine vollständige Aufzeichnung der Clusteraktivität. Das Clusterprotokoll zeichnet die Aktivität des Cluster-Service auf, die im Ereignisprotokoll aufgezeichnet wird. Das Ereignisprotokoll kann Sie zwar auf ein Problem aufmerksam machen, aber das Clusterprotokoll hilft Ihnen, das Problem zu lösen.

Das Clusterprotokoll ist in Windows standardmäßig aktiviert. Seine Ausgabe wird als Protokolldatei in %SystemRoot%\Cluster gedruckt. Weitere Informationen finden Sie in der Windows-Onlinehilfe.

## Clients für Anwendungen, virtuelle Maschinen und Systeme konfigurieren

---

Der Server schützt Daten für Clients, die Anwendungen, virtuelle Maschinen und Systeme umfassen können. Um Clientdaten schützen zu können, müssen Sie den Clientknoten beim Server registrieren und einen Sicherheitszeitplan zum Schützen der Clientdaten auswählen.

- Clients hinzufügen  
Nach der Implementierung einer Datenschutzlösung mit IBM Spectrum Protect können Sie die Lösung durch Hinzufügen von Clients erweitern.
- Maßnahmen anpassen  
Die Ziele eines Unternehmens zum Schützen und Aufbewahren von Daten werden normalerweise durch Führungskräfte, Rechtsberater oder andere Personen in Führungspositionen definiert. *Maßnahmen* sind das Mittel, um den Einsatz von IBM Spectrum Protect und die Datenschutz- und Datenaufbewahrungsziele Ihres Unternehmens aufeinander abzustimmen.

## Clients hinzufügen

---

Nach der Implementierung einer Datenschutzlösung mit IBM Spectrum Protect können Sie die Lösung durch Hinzufügen von Clients erweitern.

### Informationen zu diesem Vorgang

---

Die Prozedur beschreibt grundlegende Schritte zum Hinzufügen eines Clients. Spezifischere Anweisungen zum Konfigurieren von Clients enthält die Dokumentation für das auf dem Clientknoten installierte Produkt. Folgende Typen von Clients können vorhanden sein:

#### Anwendungsclientknoten

Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

#### Systemclientknoten

Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

#### VM-Clientknoten

Clientknoten virtueller Maschinen bestehen aus einem einzelnen Gasthost in einem Hypervisor. Jede virtuelle Maschine wird als ein Dateibereich dargestellt.

## Vorgehensweise

---

Um einen Client hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Wählen Sie die Software aus, die auf dem Clientknoten installiert werden soll, und planen Sie die Installation. Führen Sie die Anweisungen in Client-Software auswählen und Installation planen aus.
2. Geben Sie an, wie Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in Regeln zum Sichern und Archivieren von Clientdaten angeben aus.
3. Geben Sie an, wann Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in Sicherungs- und Archivierungsoperationen planen aus.
4. Um Clients das Herstellen einer Verbindung zum Server zu ermöglichen, registrieren Sie den Client. Führen Sie die Anweisungen in Clients registrieren aus.
5. Um einen Clientknoten zu schützen, installieren und konfigurieren Sie die ausgewählte Software auf dem Clientknoten. Führen Sie die Anweisungen in Clients installieren und konfigurieren aus.

## Client-Software auswählen und Installation planen

Unterschiedliche Typen von Daten erfordern unterschiedliche Typen von Schutz. Geben Sie den Typ der Daten an, die geschützt werden müssen, und wählen Sie die geeignete Software aus.

### Informationen zu diesem Vorgang

Das bevorzugte Verfahren ist die Installation des Clients für Sichern/Archivieren auf allen Clientknoten, sodass Sie den Clientakzeptor auf dem Clientknoten konfigurieren und starten können. Der Clientakzeptor ist für die effiziente Ausführung geplanter Operationen konzipiert.

Der Clientakzeptor führt Zeitpläne für die folgenden Produkte aus: Client für Sichern/Archivieren, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail und IBM Spectrum Protect for Virtual Environments. Wenn Sie ein Produkt installieren, für das der Clientakzeptor keine Zeitpläne ausführt, müssen Sie die Konfigurationsanweisungen in der Produktdokumentation ausführen, um sicherzustellen, dass geplante Operationen ausgeführt werden können.

### Vorgehensweise

Wählen Sie abhängig von Ihrer Zielsetzung die zu installierenden Produkte aus und lesen Sie die Installationsanweisungen. Tipp: Wenn Sie die Client-Software jetzt installieren, müssen Sie auch die in Clients installieren und konfigurieren beschriebenen Clientkonfigurationstasks ausführen, bevor Sie den Client verwenden können.

| Ziel  | Produkt und Beschreibung  | Installationsanweisungen   |
|---|---|--|
| Schutz eines Dateiservers oder einer Workstation  | Der Client für Sichern/Archivieren sichert und archiviert Dateien und Verzeichnisse von Dateiservern und Workstations in Speicher. Es ist auch möglich, Sicherungsversionen und archivierte Kopien von Dateien zurückzuschreiben und abzurufen.   | <ul style="list-style-type: none"> <li>• Anforderungen für den Client für Sichern/Archivieren</li> <li>• UNIX- und Linux-Clients für Sichern/Archivieren installieren</li> <li>• Windows-Client für Sichern/Archivieren installieren</li> </ul>  |
| Schutz von Anwendungen mit Momentaufnahme sicherungs- und -zurückschreibungs funktionalität | IBM Spectrum Protect Snapshot schützt Daten mit integrierter anwendungsgesteuerter Momentaufnahmesicherungs- und -zurückschreibungs funktionalität. Sie können Daten schützen, die von IBM DB2-Datenbanksoftware sowie SAP-, Oracle-, Microsoft Exchange Server- und Microsoft SQL Server-Anwendungen gespeichert werden. | <ul style="list-style-type: none"> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen</li> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen</li> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen</li> </ul> |
| Schutz einer E-Mail-Anwendung auf einem IBM Domino-Server                                   | IBM Spectrum Protect for Mail: Data Protection for IBM® Domino automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass IBM Domino-Server heruntergefahren werden.  | <ul style="list-style-type: none"> <li>• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0)</li> <li>• Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0)</li> </ul>  |

| Ziel   | Produkt und Beschreibung   | Installationsanweisungen   |
|--|--|--|
| Schutz einer E-Mail-Anwendung auf einem Server mit Microsoft Exchange Server | IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass Server mit Microsoft Exchange Server heruntergefahren werden.  | Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server   |
| Schutz einer IBM DB2-Datenbank   | Mithilfe der Anwendungsprogrammierschnittstelle (API) des Clients für Sichern/Archivieren können DB2-Daten auf dem IBM Spectrum Protect-Server gesichert werden.   | IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)  |
| Schutz einer IBM Informix-Datenbank  | Mithilfe der API des Clients für Sichern/Archivieren können Informix-Daten auf dem IBM Spectrum Protect-Server gesichert werden.   | IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)  |
| Schutz einer Microsoft SQL-Datenbank   | IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server schützt Microsoft SQL-Daten.  | Data Protection for SQL Server unter Windows Server Core installieren  |
| Schutz einer Oracle-Datenbank  | IBM Spectrum Protect for Databases: Data Protection for Oracle schützt Oracle-Daten.   | Installation von Data Protection for Oracle  |
| Schutz einer SAP-Umgebung  | IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP stellt Schutz bereit, der für SAP-Umgebungen angepasst ist. Das Produkt dient der Verbesserung der Verfügbarkeit von SAP-Datenbankservern und der Verringerung des Verwaltungsaufwands.   | <ul style="list-style-type: none"> <li>IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 installieren</li> <li>IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle installieren</li> </ul>                  |
| Schutz einer virtuellen Maschine   | <p>IBM Spectrum Protect for Virtual Environments stellt Schutz bereit, der für virtuelle Microsoft Hyper-V- und VMware-Umgebungen angepasst ist. Mithilfe von IBM Spectrum Protect for Virtual Environments können Sie immer inkrementelle Sicherungen erstellen, die auf einem zentralen Server gespeichert werden, Sicherungsmaßnahmen erstellen und virtuelle Maschinen oder einzelne Dateien zurückschreiben.</p> <p>Sie können auch stattdessen den Client für Sichern/Archivieren zum Sichern und Zurückschreiben einer vollständigen virtuellen VMware- oder Microsoft Hyper-V-Maschine verwenden. Es ist auch möglich, Dateien oder Verzeichnisse von einer virtuellen VMware-Maschine zu sichern und zurückzuschreiben.</p> | <ul style="list-style-type: none"> <li>Data Protection for Microsoft Hyper-V installieren</li> <li>Installation und Upgrade für Data Protection for VMware durchführen</li> <li>IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)</li> </ul> |

Tipp: Um den Client für die Speicherbereichsverwaltung zu verwenden, können Sie IBM Spectrum Protect for Space Management oder IBM Spectrum Protect HSM for Windows installieren.

## Regeln zum Sichern und Archivieren von Clientdaten angeben

Stellen Sie vor dem Hinzufügen eines Clients sicher, dass entsprechende Regeln zum Sichern und Archivieren der Clientdaten angegeben sind. Während des Clientregistrierungsprozesses ordnen Sie den Clientknoten einer Maßnahmendomäne zu, die die Regeln enthält, die die Regeln enthält, die steuern, wie und wann Clientdaten gespeichert werden.

### Vorbereitende Schritte

Legen Sie die weitere Vorgehensweise fest:

- Wenn Sie mit den Maßnahmen, die für Ihre Lösung konfiguriert sind, vertraut sind und wissen, dass für die Maßnahmen keine Änderungen erforderlich sind, fahren Sie mit Sicherungs- und Archivierungsoperationen planen fort.

- Wenn Sie mit den Maßnahmen nicht vertraut sind, führen Sie die Schritte in dieser Prozedur aus.

## Informationen zu diesem Vorgang

---

Maßnahmen haben Auswirkungen auf das Datenvolumen, das im Laufe der Zeit gespeichert wird, und den Zeitraum, den Daten aufbewahrt werden und für die Zurückschreibung durch Clients verfügbar sind. Um Datenschutzziele zu erreichen, können Sie die Standardmaßnahme aktualisieren und eigene Maßnahmen erstellen. Eine Maßnahme umfasst die folgenden Regeln:

- Angabe, wie und wann Dateien in Serverspeicher gesichert und archiviert werden
- Anzahl Kopien einer Datei und Zeitraum, den Kopien im Serverspeicher aufbewahrt werden

Während des Clientregistrierungsprozesses ordnen Sie einen Client einer *Maßnahmendomäne* zu. Die Maßnahme für einen bestimmten Client wird durch die Regeln in der Maßnahmendomäne festgelegt, der der Client zugeordnet ist. In der Maßnahmendomäne befinden sich die Regeln, die wirksam sind, in der aktiven *Maßnahmengruppe*.

Wenn ein Client eine Datei sichert oder archiviert, wird die Datei an eine Verwaltungsklasse in der aktiven Maßnahmengruppe der Maßnahmendomäne gebunden. Eine *Verwaltungsklasse* ist die wichtigste Gruppe von Regeln zur Verwaltung von Clientdaten. Die Sicherungs- und Archivierungsoperationen auf dem Client verwenden die Einstellungen in der Standardverwaltungsklasse der Maßnahmendomäne, es sei denn, Sie passen die Maßnahme weiter an. Eine Maßnahme kann angepasst werden, indem weitere Verwaltungsklassen definiert werden und ihre Verwendung über Clientoptionen zugeordnet wird.

Clientoptionen können in einer lokalen, editierbaren Datei auf dem Clientsystem und in einer Clientoptionsgruppe auf dem Server angegeben werden. Die Optionen in der Clientoptionsgruppe auf dem Server können die Optionen in der lokalen Clientoptionsdatei überschreiben oder den Optionen in der lokalen Clientoptionsdatei hinzugefügt werden.

## Vorgehensweise

---

1. Überprüfen Sie die Maßnahmen, die für Ihre Lösung konfiguriert sind, indem Sie die Anweisungen in Maßnahmen anzeigen ausführen.
2. Wenn geringfügige Änderungen erforderlich sind, um die Datenaufbewahrungsanforderungen zu erfüllen, führen Sie die Anweisungen in Maßnahmen editieren aus.
3. Optional: Wenn Maßnahmendomänen erstellt oder umfangreiche Änderungen an Maßnahmen durchgeführt werden müssen, um Datenaufbewahrungsanforderungen zu erfüllen, lesen Sie die Informationen in Maßnahmen anpassen.

## Maßnahmen anzeigen

---

Zeigen Sie Maßnahmen an, um zu bestimmen, ob die Maßnahmen zur Erfüllung Ihrer Anforderungen editiert werden müssen.

## Vorgehensweise

---

1. Um die aktive Maßnahmengruppe für eine Maßnahmendomäne anzuzeigen, führen Sie die folgenden Schritte aus:
  - a. Wählen Sie auf der Seite Services im Operations Center eine Maßnahmendomäne aus und klicken Sie auf Details.
  - b. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen.  
Tipp: Um sicherzustellen, dass Sie Daten nach einer Ransomware-Attacke wiederherstellen können, beachten Sie die folgenden Richtlinien:
    - Stellen Sie sicher, dass der Wert in der Spalte 'Sicherungen' mindestens 2 beträgt. Der bevorzugte Wert ist 3, 4 oder höher.
    - Stellen Sie sicher, dass der Wert in der Spalte 'Zusätzliche Sicherungen aufbewahren' mindestens 14 Tage beträgt. Der bevorzugte Wert ist 30 Tage oder mehr.
    - Stellen Sie sicher, dass der Wert in der Spalte 'Archivierungen aufbewahren' mindestens 30 Tage beträgt.

Wenn IBM Spectrum Protect for Space Management-Software auf dem Client installiert ist, stellen Sie sicher, dass diese Daten vor ihrer Umlagerung gesichert werden. Geben Sie im Befehl DEFINE MGMTCLASS oder UPDATE MGMTCLASS MIGREQUIRESBKUP=YES an. Befolgen Sie dann die Richtlinien im Tipp.
2. Um inaktive Maßnahmengruppen für eine Maßnahmendomäne anzuzeigen, führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf der Seite Maßnahmengruppen auf die Umschaltfläche Konfigurieren. Jetzt können Sie die inaktiven Maßnahmengruppen anzeigen und editieren.
  - b. Blättern Sie mithilfe der vorwärts und rückwärts gerichteten Pfeile durch die inaktiven Maßnahmengruppen. Wenn Sie eine inaktive Maßnahmengruppe anzeigen, sind die unterschiedlichen Einstellungen für die inaktive und aktive Maßnahmengruppe hervorgehoben.
  - c. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppen sind nicht mehr editierbar.

## Maßnahmen editieren

---

Um die Regeln zu ändern, die für eine Maßnahmendomäne gelten, editieren Sie die aktive Maßnahmengruppe für die Maßnahmendomäne. Sie können auch eine andere Maßnahmengruppe für eine Domäne aktivieren.

## Vorbereitende Schritte

Änderungen an Maßnahmen können sich auf die Datenaufbewahrung auswirken. Stellen Sie sicher, dass weiterhin Daten gesichert werden, die für Ihr Unternehmen von entscheidender Bedeutung sind, sodass Sie diese Daten in einem Katastrophenfall zurückschreiben können. Stellen Sie außerdem sicher, dass Ihr System über genügend Speicherbereich für geplante Sicherungsoperationen verfügt.

## Informationen zu diesem Vorgang

Sie editieren eine Maßnahmengruppe, indem Sie eine oder mehrere Verwaltungsklassen in der Maßnahmengruppe ändern. Wenn Sie die aktive Maßnahmengruppe editieren, stehen die Änderungen den Clients erst zur Verfügung, nachdem Sie die Maßnahmengruppe reaktiviert haben. Um die editierte Maßnahmengruppe Clients zur Verfügung zu stellen, aktivieren Sie die Maßnahmengruppe.

Obwohl Sie mehrere Maßnahmengruppen für eine Maßnahmendomäne definieren können, kann nur eine einzige Maßnahmengruppe aktiv sein. Wenn Sie eine andere Maßnahmengruppe aktivieren, ersetzt diese die momentan aktive Maßnahmengruppe.

Informationen zu bevorzugten Verfahren zum Definieren von Maßnahmen finden Sie in Maßnahmen anpassen.

## Vorgehensweise

1. Wählen Sie auf der Seite Services im Operations Center eine Maßnahmendomäne aus und klicken Sie auf Details.
2. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen.

Die Seite Maßnahmengruppen gibt den Namen der aktiven Maßnahmengruppe an und listet alle Verwaltungsklassen für diese Maßnahmengruppe auf.

3. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppe ist editierbar.
4. Optional: Um eine Maßnahmengruppe zu editieren, die nicht aktiv ist, klicken Sie auf die vorwärts und rückwärts gerichteten Pfeile, um die Maßnahmengruppe zu lokalisieren.
5. Editieren Sie die Maßnahmengruppe, indem Sie eine der folgenden Aktionen ausführen:

| Option  | Bezeichnung   |
|---|---|
| <b>Verwaltungsklasse hinzufügen</b>   | <ol style="list-style-type: none"><li>a. Klicken Sie in der Tabelle 'Maßnahmengruppen' auf + Verwaltungsklasse.</li><li>b. Um die Regeln zum Sichern und Archivieren von Daten anzugeben, füllen Sie die Felder im Fenster Verwaltungsklasse hinzufügen aus.</li><li>c. Um die Verwaltungsklasse als Standardverwaltungsklasse festzulegen, wählen Sie das Kontrollkästchen Als Standardwert definieren aus.</li><li>d. Klicken Sie auf Hinzufügen.</li></ol>   |
| <b>Verwaltungsklasse löschen</b>  | Klicken Sie in der Spalte 'Verwaltungsklasse' auf -.<br>Tipp: Um die Standardverwaltungsklasse zu löschen, müssen Sie zunächst eine andere Verwaltungsklasse als Standardverwaltungsklasse zuordnen.  |
| <b>Legen Sie eine Verwaltungsklasse als Standardverwaltungsklasse fest.</b> | Klicken Sie in der Spalte 'Standard' für die Verwaltungsklasse auf das Optionsfeld.<br>Tipp: Die Standardverwaltungsklasse verwaltet Clientdateien, wenn einer Datei keine andere Verwaltungsklasse zugeordnet ist oder keine andere Verwaltungsklasse zur Verwaltung geeignet ist. Um sicherzustellen, dass Clients immer Dateien sichern und archivieren können, wählen Sie eine Standardverwaltungsklasse aus, die sowohl Regeln für das Sichern als auch für das Archivieren von Dateien enthält. |
| <b>Verwaltungsklasse ändern</b>   | Um die Merkmale einer Verwaltungsklasse zu ändern, aktualisieren Sie die Felder in der Tabelle.   |

6. Klicken Sie auf Sichern.  
Achtung: Wenn Sie eine neue Maßnahmengruppe aktivieren, können Daten verloren gehen. Daten, die unter einer Maßnahmengruppe geschützt werden, werden möglicherweise unter einer anderen Maßnahmengruppe nicht geschützt. Daher müssen Sie vor dem Aktivieren einer Maßnahmengruppe sicherstellen, dass die Unterschiede zwischen der vorherigen Maßnahmengruppe und der neuen Maßnahmengruppe keinen Datenverlust zur Folge haben.
7. Klicken Sie auf Aktivieren. Es wird eine Zusammenfassung der Unterschiede zwischen der aktiven Maßnahmengruppe und der neuen Maßnahmengruppe angezeigt. Stellen Sie sicher, dass die Änderungen in der neuen Maßnahmengruppe mit Ihren Datenaufbewahrungsanforderungen konsistent sind, indem Sie die folgenden Schritte ausführen:
  - a. Überprüfen Sie die Unterschiede zwischen entsprechenden Verwaltungsklassen in den beiden Maßnahmengruppen und wägen Sie die Konsequenzen für Clientdateien ab. Clientdateien, die an Verwaltungsklassen in der aktiven Maßnahmengruppe gebunden sind, werden in der neuen Maßnahmengruppe an die Verwaltungsklassen mit denselben Namen gebunden.

- b. Ermitteln Sie Verwaltungsklassen in der aktiven Maßnahmengruppe, die in der neuen Maßnahmengruppe keine Entsprechung haben und wägen Sie die Konsequenzen für Clientdateien ab. Clientdateien, die an diese Verwaltungsklassen gebunden sind, werden von der Standardverwaltungsklasse in der neuen Maßnahmengruppe verwaltet.
- c. Wenn die Änderungen, die durch die Maßnahmengruppe implementiert werden sollen, akzeptabel sind, wählen Sie das Kontrollkästchen Ich weiß, dass diese Aktualisierungen zu einem Datenverlust führen können aus und klicken Sie auf Aktivieren.

## Sicherungs- und Archivierungsoperationen planen

Bevor Sie einen neuen Client beim Server registrieren, müssen Sie sicherstellen, dass ein Zeitplan verfügbar ist, um anzugeben, wann Sicherungs- und Archivierungsoperationen ausgeführt werden. Während des Registrierungsprozesses können Sie dem Client einen Zeitplan zuordnen.

### Vorbereitende Schritte

Legen Sie die weitere Vorgehensweise fest:

- Wenn Sie mit den Zeitplänen, die für die Lösung konfiguriert sind, vertraut sind und für die Zeitpläne keine Änderungen erforderlich sind, fahren Sie mit Clients registrieren fort.
- Wenn Sie mit den Zeitplänen nicht vertraut sind oder für die Zeitpläne Änderungen erforderlich sind, führen Sie die Schritte in dieser Prozedur aus.


### Informationen zu diesem Vorgang

Normalerweise müssen Sicherungsoperationen für alle Clients täglich ausgeführt werden. Planen Sie Client- und Server-Workloads mit Bedacht, um die beste Leistung für Ihre Speicherumgebung zu erzielen. Um die Überschneidung von Client- und Serveroperationen zu verhindern, planen Sie die Ausführung von Clientsicherungs- und -archivierungsoperationen gegebenenfalls für die Nacht. Wenn sich Client- und Serveroperationen überschneiden oder ihnen nicht genügend Zeit und Ressourcen zur Verarbeitung zur Verfügung gestellt werden, können eine Verschlechterung der Systemleistung, fehlgeschlagene Operationen und andere Probleme die Folge sein.


### Vorgehensweise

1. Überprüfen Sie die verfügbaren Zeitpläne, indem Sie den Mauszeiger in der Menüleiste des Operations Center über Clients bewegen. Klicken Sie auf Zeitpläne.
2. Optional: Ändern oder Erstellen Sie einen Zeitplan, indem Sie die folgenden Schritte ausführen:

| Option                    | Bezeichnung   |
|---------------------------|---|
| <b>Zeitplan ändern</b>    | <ul style="list-style-type: none"> <li>a. Wählen Sie in der Sicht Zeitpläne den Zeitplan aus und klicken Sie auf Details.</li> <li>b. Zeigen Sie auf der Seite Zeitplandetails Details an, indem Sie auf die blauen Pfeile am Anfang der Zeilen klicken.</li> <li>c. Ändern Sie die Einstellungen im Zeitplan und klicken Sie auf Sichern.</li> </ul> |
| <b>Zeitplan erstellen</b> | Klicken Sie in der Sicht Zeitpläne auf +Zeitplan und führen Sie die Schritte zum Erstellen eines Zeitplans aus.   |

3. Optional: Verwenden Sie zum Konfigurieren von Zeitplaneinstellungen, die im Operations Center nicht sichtbar sind, einen Serverbefehl. Angenommen, Sie möchten eine Clientoperation planen, mit der ein bestimmtes Verzeichnis gesichert und einer anderen Verwaltungsklasse als der Standardverwaltungsklasse zugeordnet wird.
  - a. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.
  - b. Geben Sie zum Erstellen eines Zeitplans den Befehl DEFINE SCHEDULE und zum Ändern eines Zeitplans den Befehl UPDATE SCHEDULE aus. Ausführliche Informationen zu den Befehlen finden Sie in DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren) bzw. UPDATE SCHEDULE (Clientzeitplan aktualisieren).

#### Zugehörige Tasks:

-  Zeitplan für tägliche Operationen optimieren

## Clients registrieren

Registrieren Sie einen Client, um sicherzustellen, dass der Client die Verbindung zum Server herstellen und der Server Clientdaten schützen kann.

### Vorbereitende Schritte

Bestimmen Sie, ob der Client eine Benutzer-ID mit Administratorberechtigung mit Clienteignerberechtigung für den Clientknoten erfordert. Informationen zum Bestimmen der Clients, die eine Benutzer-ID mit Administratorberechtigung erfordern, finden Sie in Technote 7048963.

Einschränkung: Bei einigen Clienttypen müssen der Clientknotenname und die Benutzer-ID mit Administratorberechtigung übereinstimmen. Sie können diese Clients nicht mithilfe der in Version 7.1.7 eingeführten LDAP-Authentifizierungsmethode authentifizieren. Ausführliche Informationen zu dieser Authentifizierungsmethode, die manchmal als integrierter Modus bezeichnet wird, finden Sie in Benutzer mithilfe einer Active Directory-Datenbank authentifizieren.

## Vorgehensweise

Um einen Client zu registrieren, führen Sie eine der folgenden Aktionen aus.

- Wenn der Client eine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Befehl REGISTER NODE unter Angabe des Parameters USERID:

```
register node Knotenname Kennwort userid=Knotenname
```

Dabei gibt *Knotenname* den Knotennamen und *Kennwort* das Knotenkennwort an. Ausführliche Informationen finden Sie in Knoten registrieren.

- Wenn der Client keine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Assistenten 'Client hinzufügen' im Operations Center. Führen Sie die folgenden Schritte aus:
  - a. Klicken Sie in der Menüleiste des Operations Center auf Clients.
  - b. Klicken Sie in der Tabelle 'Clients' auf + Client.
  - c. Führen Sie die Schritte im Assistenten Client hinzufügen aus:
    - i. Geben Sie an, dass redundante Daten sowohl auf dem Client als auch auf dem Server gelöscht werden können. Wählen Sie im Bereich 'Clientseitige Datendeduplizierung' das Kontrollkästchen Aktivieren aus.
    - ii. Kopieren Sie im Fenster Konfiguration die Werte für die Optionen TCPSERVERADDRESS, TCPPORT, NODENAME und DEDUPLICATION.  
Tipp: Notieren Sie die Optionswerte und bewahren Sie die Unterlagen an einem sicheren Ort auf. Nachdem Sie die Clientregistrierung abgeschlossen und die Software auf dem Clientknoten installiert haben, verwenden Sie die Werte zum Konfigurieren des Clients.
    - iii. Führen Sie die Anweisungen im Assistenten aus, um die Maßnahmendomäne, den Zeitplan und die Optionsgruppe anzugeben.
    - iv. Legen Sie fest, wie Risiken für den Client angezeigt werden, indem Sie die Einstellung für die Gefährdung angeben.
    - v. Klicken Sie auf Client hinzufügen.

### Zugehörige Verweise:

- ➔ DECOMMISSION NODE (Clientknoten stilllegen)
- ➔ DECOMMISSION VM (Virtuelle Maschine stilllegen)
- ➔ QUERY NODE (Knoten abfragen)
- ➔ REMOVE REPLNODE (Clientknoten aus Replikation entfernen)

## Clients installieren und konfigurieren

Bevor Sie einen Clientknoten schützen können, müssen Sie die ausgewählte Software installieren und konfigurieren.

## Vorgehensweise

Wenn Sie die Software bereits installiert haben, starten Sie mit Schritt 2.

1. Führen Sie eine der folgenden Aktionen aus:
  - Um Software auf einem Anwendungs- oder Clientknoten zu installieren, führen Sie die Anweisungen aus.

| Software  | Link zu Anweisungen   |
|---|---|
| IBM Spectrum Protect-Client für Sichern/Archivieren | <ul style="list-style-type: none"><li>■ UNIX- und Linux-Clients für Sichern/Archivieren installieren</li><li>■ Windows-Client für Sichern/Archivieren installieren</li></ul> <p>Tipp: Vorhandene Clients können auch mithilfe des Operations Center aktualisiert werden. Anweisungen finden Sie in Clientaktualisierungen planen.</p> |
| IBM Spectrum Protect for Databases                  | <ul style="list-style-type: none"><li>■ Installation von Data Protection for Oracle</li><li>■ Data Protection for SQL Server unter Windows Server Core installieren</li></ul>   |



| Software  | Link zu Anweisungen   |
|---|---|
| IBM Spectrum Protect for Mail                         | <ul style="list-style-type: none"> <li>■ Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0)</li> <li>■ Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0)</li> <li>■ Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li> </ul> |
| IBM Spectrum Protect Snapshot                         | <ul style="list-style-type: none"> <li>■ Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen</li> <li>■ Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen</li> <li>■ Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen</li> </ul>  |
| IBM Spectrum Protect for Enterprise Resource Planning | <ul style="list-style-type: none"> <li>■ IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 installieren</li> <li>■ IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle installieren</li> </ul>   |

- o Um Software auf einem VM-Clientknoten zu installieren, führen Sie die Anweisungen für den ausgewählten Sicherungstyp aus.

| Sicherungstyp   | Link zu Anweisungen  |
|---|--|
| Wenn Sie planen, VMware-Gesamtsicherungen virtueller Maschinen zu erstellen, installieren und konfigurieren Sie den IBM Spectrum Protect-Client für Sichern/Archivieren.  | <ul style="list-style-type: none"> <li>■ UNIX- und Linux-Clients für Sichern/Archivieren installieren</li> <li>■ Windows-Client für Sichern/Archivieren installieren</li> </ul>  |
| Wenn Sie planen, immer inkrementelle Gesamtsicherungen virtueller Maschinen zu erstellen, installieren und konfigurieren Sie IBM Spectrum Protect for Virtual Environments und den Client für Sichern/Archivieren auf demselben Clientknoten oder auf unterschiedlichen Clientknoten. | <ul style="list-style-type: none"> <li>■ IBM Spectrum Protect for Virtual Environments-Onlineproduktokumentation</li> </ul> <p>Tipp: Die Software für IBM Spectrum Protect for Virtual Environments und den Client für Sichern/Archivieren sind im IBM Spectrum Protect for Virtual Environments-Installationspaket enthalten.</p> |

2. Um Clients das Herstellen einer Verbindung zum Server zu ermöglichen, fügen Sie die Werte für die Optionen TCPSERVERADDRESS, TCPPORT und NODENAME in der Clientoptionsdatei hinzu oder aktualisieren Sie diese. Verwenden Sie die Werte, die Sie beim Registrieren des Clients notiert haben (Clients registrieren).
  - o Fügen Sie für Clients, die unter einem AIX-, Linux-, Mac OS X- oder Oracle Solaris-Betriebssystem installiert sind, die Werte der Clientsystemoptionsdatei dsm.sys hinzu.
  - o Fügen Sie für Clients, die unter einem Windows-Betriebssystem installiert sind, die Werte der Clientsystemoptionsdatei dsm.opt hinzu.

Standardmäßig befinden sich die Optionsdateien im Installationsverzeichnis.
3. Wenn ein Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem installiert wurde, installieren Sie den Clientverwaltungsservice auf dem Client. Führen Sie die Anweisungen in Diagnoseinformationen mit Clientverwaltungsservices erfassen aus.
4. Konfigurieren Sie den Client für die Ausführung geplanter Operationen. Führen Sie die Anweisungen in Client für die Ausführung geplanter Operationen konfigurieren aus.
5. Optional: Konfigurieren Sie die Kommunikation durch eine Firewall. Führen Sie die Anweisungen in Client/Server-Kommunikation durch eine Firewall konfigurieren aus.
6. Führen Sie eine Testsicherung aus, um sicherzustellen, dass Daten wie geplant geschützt werden. Führen Sie beispielsweise für einen Client für Sichern/Archivieren die folgenden Schritte aus:
  - a. Wählen Sie auf der Seite 'Clients' im Operations Center den Client aus, der gesichert werden soll, und klicken Sie auf Sichern.
  - b. Überprüfen Sie, ob die Sicherung erfolgreich ausgeführt wird und keine Warnungen oder Fehlernachrichten vorhanden sind.
7. Überwachen Sie die Ergebnisse der geplanten Operationen für den Client im Operations Center.

## Nächste Schritte

Wenn geändert werden muss, welche Daten vom Client gesichert werden, führen Sie die Anweisungen in Bereich einer Clientsicherung ändern aus.

## Client für die Ausführung geplanter Operationen konfigurieren

---

Sie müssen einen Client-Scheduler auf dem Clientknoten konfigurieren und starten. Der Client-Scheduler ermöglicht die Kommunikation zwischen dem Client und dem Server, sodass geplante Operationen erfolgen können. Beispielsweise umfassen geplante Operationen normalerweise das Sichern von Dateien von einem Client.

### Informationen zu diesem Vorgang

---

Die bevorzugte Methode ist die Installation des Clients für Sichern/Archivieren auf allen Clientknoten, sodass Sie den Clientakzeptor auf dem Clientknoten konfigurieren und starten können. Der Clientakzeptor ist für die effiziente Ausführung geplanter Operationen konzipiert. Der Clientakzeptor verwaltet den Client-Scheduler derart, dass der Scheduler nur in erforderlichen Fällen ausgeführt wird:

- Wenn der Zeitpunkt erreicht ist, an dem der Server nach der nächsten geplanten Operation abgefragt werden soll
- Wenn der Zeitpunkt erreicht ist, an dem die nächste geplante Operation gestartet werden soll

Durch die Verwendung des Clientakzeptors ist es möglich, die Anzahl Hintergrundprozesse auf dem Client zu reduzieren und Probleme in Bezug auf die Speicheraufbewahrungsdauer zu vermeiden.

Der Clientakzeptor führt Zeitpläne für die folgenden Produkte aus: Client für Sichern/Archivieren, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail und IBM Spectrum Protect for Virtual Environments. Wenn Sie ein Produkt installiert hatten, für das der Clientakzeptor keine Zeitpläne ausführt, führen Sie die Konfigurationsanweisungen in der Produktdokumentation aus, um sicherzustellen, dass geplante Operationen ausgeführt werden können.

Wenn Ihr Unternehmen standardmäßig ein Zeitplanungstool eines anderen Anbieters verwendet, können Sie statt des Clientakzeptors dieses Zeitplanungstool verwenden. Normalerweise starten Zeitplanungstools anderer Anbieter Clientprogramme direkt mithilfe von Betriebssystembefehlen. Informationen zum Konfigurieren eines Zeitplanungstools eines anderen Anbieters enthält die Produktdokumentation.

### Vorgehensweise

---

Um den Client-Scheduler mithilfe des Clientakzeptors zu konfigurieren und zu starten, führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

AIX und Oracle Solaris

- Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
- Klicken Sie auf die Registerkarte Web-Client.
- Klicken Sie im Feld Optionen für verwaltete Services auf Zeitplan. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option Beides.
- Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, setzen Sie in der Datei `dsm.sys` die Option `passwordaccess` auf `generate`.
- Um das Clientknotenkenntwort zu speichern, geben Sie den folgenden Befehl aus und geben Sie auf Anforderung das Clientknotenkenntwort ein:

```
dsmc query sess
```

- Starten Sie den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

```
/usr/bin/dsmcad
```

- Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie der Systemstartdatei (normalerweise `/etc/inittab`) den folgenden Eintrag hinzu:

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Clientakzeptordämon
```

Linux

- Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
- Klicken Sie auf die Registerkarte Web-Client.
- Klicken Sie im Feld Optionen für verwaltete Services auf Zeitplan. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option Beides.
- Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, setzen Sie in der Datei `dsm.sys` die Option `passwordaccess` auf `generate`.
- Um das Clientknotenkenntwort zu speichern, geben Sie den folgenden Befehl aus und geben Sie auf Anforderung das Clientknotenkenntwort ein:

```
dsmc query sess
```

f. Starten Sie den Clientakzeptor, indem Sie sich mit der Rootbenutzer-ID anmelden und den folgenden Befehl ausgeben:

```
service dsmcad start
```

g. Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie den Service hinzu, indem Sie in einer Shelleingabeaufforderung den folgenden Befehl ausgeben:

```
# chkconfig --add dsmcad
```

## MAC OS X

- Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
- Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, klicken Sie auf Berechtigung, wählen Sie Kennwort generieren aus und klicken Sie auf Anwenden.
- Um anzugeben, wie Services verwaltet werden, klicken Sie auf Web-Client, wählen Sie Zeitplan aus, klicken Sie auf Anwenden und dann auf OK.
- Um sicherzustellen, dass das generierte Kennwort gespeichert wird, starten Sie den Client für Sichern/Archivieren erneut.
- Starten Sie den Clientakzeptor mithilfe der Anwendung 'IBM Spectrum Protect Tools for Administrators'.

## Windows

- Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Dienstprogramme > Setup-Assistent > Hilfe zum Konfigurieren des Client-Schedulers. Klicken Sie auf Weiter.
- Lesen Sie die Informationen auf der Seite Schedulerassistent und klicken Sie auf Weiter.
- Wählen Sie auf der Seite Scheduler-Task die Option Neuen oder zusätzlichen Scheduler installieren aus und klicken Sie auf Weiter.
- Geben Sie auf der Seite Schedulername und -position einen Namen für den Client-Scheduler an, der hinzugefügt wird. Wählen Sie dann Scheduler mit Clientakzeptordämon (CAD) verwalten aus, um den Scheduler zu verwalten, und klicken Sie auf Weiter.
- Geben Sie den Namen ein, der diesem Clientakzeptor zugeordnet werden soll. Der Standardname ist 'Clientakzeptor'. Klicken Sie auf Weiter.
- Schließen Sie die Konfiguration ab, indem Sie den Assistenten durchlaufen.
- Aktualisieren Sie die Clientoptionsdatei, dsm.opt, und setzen Sie die Option passwordaccess auf generate.
- Um das Clientknotenkenntwort zu speichern, geben Sie den folgenden Befehl in der Eingabeaufforderung aus:

```
dsmc query sess
```

Geben Sie auf Anforderung das Clientknotenkenntwort ein.

- Starten Sie den Clientakzeptorservice über die Seite Systemsteuerung. Wenn Sie beispielsweise den Standardnamen verwendet haben, starten Sie den Service 'Clientakzeptor'. Starten Sie nicht den Scheduler-Service, den Sie auf der Seite Schedulername und -position angegeben haben. Der Scheduler-Service wird wie erforderlich automatisch vom Clientakzeptorservice gestartet und gestoppt.

## Client/Server-Kommunikation durch eine Firewall konfigurieren

---

Wenn ein Client durch eine Firewall mit einem Server kommunizieren muss, müssen Sie die Client/Server-Kommunikation durch die Firewall ermöglichen.

### Vorbereitende Schritte

---

Wenn Sie den Assistenten 'Client hinzufügen' zum Registrieren eines Clients verwendet hatten, bestimmen Sie die Optionswerte in der Clientoptionsdatei, die während dieses Prozesses abgerufen wurden. Sie können die Werte zur Angabe von Ports verwenden.

### Informationen zu diesem Vorgang

---

Achtung: Konfigurieren Sie eine Firewall nicht derart, dass dies eine Beendigung der Sitzungen zur Folge hätte, die von einem Server oder Speicheragenten verwendet werden. Die Beendigung einer gültigen Sitzung kann zu unvorhersehbaren Ergebnissen führen. Prozesse und Sitzungen scheinen unter Umständen aufgrund von Ein-/Ausgabebefehlen gestoppt zu werden. Um das Ausschließen von Sitzungen von Zeitlimitbeschränkungen zu erleichtern, konfigurieren Sie bekannte Ports für IBM Spectrum Protect-Komponenten. Stellen Sie sicher, dass die Serveroption KEEPALIVE auf den Standardwert YES gesetzt bleibt. Auf diese Art und Weise kann sichergestellt werden, dass die Client/Server-Kommunikation unterbrechungsfrei erfolgt. Anweisungen zum Definieren der Serveroption KEEPALIVE finden Sie in KEEPALIVE.

### Vorgehensweise

---

Öffnen Sie die folgenden Ports, um Zugriff durch die Firewall zu ermöglichen:

TCP/IP-Port für den Client für Sichern/Archivieren, den Verwaltungsbefehlszeilenclient und den Client-Scheduler  
Geben Sie den Port über die Option `tcpport` in der Clientoptionsdatei an. Die Option `tcpport` in der Clientoptionsdatei muss mit der Option `TCPPORT` in der Serveroptionsdatei übereinstimmen. Der Standardwert ist 1500. Wenn ein anderer Wert als der Standardwert verwendet werden soll, geben Sie eine Zahl zwischen 1024 und 32767 an.

HTTP-Port, um die Kommunikation zwischen dem Web-Client und fernen Workstations zu ermöglichen  
Geben Sie den Port für die ferne Workstation an, indem Sie die Option `httpport` in der Clientoptionsdatei der fernen Workstation festlegen. Der Standardwert ist 1581.

TCP/IP-Ports für die ferne Workstation  
Der Standardwert von 0 (null) hat zur Folge, dass zwei freie Portnummern der fernen Workstation nach dem Zufallsprinzip zugeordnet werden. Wenn die Portnummern nicht nach dem Zufallsprinzip zugeordnet werden sollen, geben Sie über die Option `webports` in der Clientoptionsdatei der fernen Workstation Werte an.

TCP/IP-Port für Verwaltungssitzungen  
Geben Sie den Port an, an dem der Server auf Anforderungen von Verwaltungsclientsitzungen wartet. Der Wert der Clientoption `tcpadminport` muss mit dem Wert der Serveroption `TCPADMINPORT` übereinstimmen. Auf diese Art und Weise können Sie sichere Verwaltungssitzungen in einem privaten Netz gewährleisten.

## Clientaktualisierungen planen

---

Planen Sie die automatische Installation von Software-Updates für IBM Spectrum Protect-Clients für Sichern/Archivieren. Diese Funktion wird manchmal als *Clientimplementierung* bezeichnet.

## Vorbereitende Schritte

---

Um Clientaktualisierungen mithilfe des Operations Center zu planen, müssen Sie Ihre Umgebung so konfigurieren, dass sie die folgenden Voraussetzungen erfüllt:

### Servervoraussetzungen

IBM Spectrum Protect-Server müssen die folgenden Voraussetzungen erfüllen:

- IBM Spectrum Protect Version 8.1.3 oder höher muss auf den Hub- und Peripherieservern installiert sein.
- Für Hub- und Peripherieserver müssen eine Adresse der höheren Ebene und eine Adresse der unteren Ebene angegeben sein. Sie können diese Einstellungen mithilfe der Befehle `SET SERVERHLADDRESS` und `SET SERVERLLADDRESS` konfigurieren.
- Für den Hub-Server muss ein Serverkennwort angegeben sein. Sie können diese Einstellung mithilfe des Befehls `SET SERVERPASSWORD` konfigurieren.
- Der Hub-Server muss für die Peripherieserver definiert sein. Diese Definition erfolgt nicht automatisch, wenn Peripherieserver dem Operations Center hinzugefügt werden. Um den Hub-Server zu definieren, geben Sie den Befehl `DEFINE SERVER` unter Verwendung der zweiten Syntaxoption in der Befehlsdokumentation aus. Geben Sie beispielsweise den folgenden Befehl auf jedem Peripherieserver aus:

```
DEFINE SERVER Name_des_Hub-Servers SERVERPASSWORD=Kennwort_des_Hub-Servers HLA=IP-Adresse_des_Hub-Servers  
LLA=Port_des_Hub-Servers SSL=NO SESSIONSECURITY=TRANSITIONAL
```

Dabei geben die Variablen die folgenden Einstellungen für den Hub-Server an: *Name\_des\_Hub-Servers* ist der Servername, *Kennwort\_des\_Hub-Servers* ist das Serverkennwort, *IP-Adresse\_des\_Hub-Servers* ist die Adresse der höheren Ebene und *Port\_des\_Hub-Servers* ist die Adresse der unteren Ebene.

- Der Port, der durch die Serveroption `RESTHTTPSPORT` angegeben wird, muss offen sein, um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server zu ermöglichen. Die Standardportnummer ist 8443.
- Peripherieserver müssen über einen Verzeichniscontainerspeicherpool oder einen FILE-Speicherpool zum Speichern von Aktualisierungspaketen verfügen. Das Operations Center wählt automatisch einen Speicherpool für die Verwendung aus.

### Clientvoraussetzungen

IBM Spectrum Protect-Clients für Sichern/Archivieren, die mithilfe des Operations Center aktualisiert werden sollen, müssen die folgenden Voraussetzungen erfüllen:

- Die Option `passwordaccess` muss auf `generate` gesetzt sein.
- Die Clientoption `autodeploy` muss auf einen anderen Wert als `no` gesetzt sein. Weitere Informationen finden Sie in der Beschreibung der Option `Autodeploy`.
- 32-Bit-Clients für Sichern/Archivieren werden nicht unterstützt. Wenn ein 32-Bit-Client für Sichern/Archivieren auf einem 64-Bit-Betriebssystem erkannt wird, wird für den Client ein Upgrade auf die 64-Bit-Version durchgeführt.
- Der Client-Scheduler muss aktiv sein.
- Das Clientsystem muss aktiv sein und der Client muss mindestens einmal eine Verbindung zum IBM Spectrum Protect-Server hergestellt haben.

Microsoft Windows-Clients müssen außerdem die folgenden Voraussetzungen erfüllen:

- Der Client-Scheduler muss als Windows-Dienst und nicht über die Befehlszeile gestartet werden. Um die Wahrscheinlichkeit eines Neustarts auf ein Mindestmaß zu reduzieren, wird der Scheduler-Service vor der Installation des neuen Clients beendet und nach der Installation erneut gestartet. Wenn der Scheduler nicht als Windows-Dienst ausgeführt wird, ist ein Neustart erforderlich, wenn der Client aktualisiert wird.
- Die Befehlszeilenversion des Windows-Registrierungsdienstprogramms (reg.exe) ist erforderlich. Dieses Tool wird im Allgemeinen im Rahmen der Betriebssysteminstallation auf unterstützten Windows-Betriebssystemen installiert.

## Informationen zu diesem Vorgang

---

Mithilfe des Operations Center können Sie mehrere Clients gleichzeitig zu einem geplanten Zeitpunkt aktualisieren.

Aktualisierungspakete werden automatisch auf den Hub-Server heruntergeladen, importiert und auf Peripherieserver repliziert. Wenn ein Plan für die Aktualisierung ausgeführt wird, werden Dateien aus dem Installationspaket auf das Clientsystem kopiert und der Client auf die angegebene Softwareversion aktualisiert.

Einschränkungen:

- Sie können nur Aktualisierungen des Clients für Sichern/Archivieren planen. Aktualisierungen für andere Clienttypen müssen manuell installiert werden.
- Die Software des Clients für Sichern/Archivieren kann nicht von verschiedenen IBM Spectrum Protect Deployment Managern gleichzeitig aktualisiert werden.
- Die Microsoft Windows-Cluster-Services-Umgebung wird nicht unterstützt.
- Planen Sie keine automatischen Clientimplementierungen für Systeme, auf denen eine der folgenden Anwendungen installiert ist:
  - IBM Spectrum Protect for Virtual Environments
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Enterprise Resource Planning
- Für die Verwaltung von Aktualisierungen erstellt das Operations Center Maßnahmenobjekte, einschließlich Einheitenklassen, Speicherpools und Domänen, auf den Hub- und Peripherieservern. Für diese Objekte wird die folgende Namenskonvention verwendet: `IBM_DEPLOY_CLIENTS`. Um Konflikte bei Aktualisierungsoperationen zu vermeiden, dürfen diese Objekte nicht geändert werden.
- Wenn Sie die Clientimplementierung für eine frühere Serverversion manuell konfiguriert haben, müssen Sie die Maßnahmenobjekte, die Sie vor der Planung von Clientaktualisierungen mithilfe des Operations Center definiert hatten, löschen.
- Sie können Aktualisierungen nur für vorhandene Clients planen. Sie können das Operations Center nicht für die Installation eines neuen Clients verwenden.

Informationen zur manuellen Installation der Software des Clients für Sichern/Archivieren finden Sie in IBM Spectrum Protect-Clients für Sichern/Archivieren installieren in der IBM Spectrum Protect-Dokumentation.

Informationen zur Installation anderer IBM Spectrum Protect-Clients finden Sie in Produktsuites und zugehörige Produkte.

## Vorgehensweise

---

1. Klicken Sie in der Menüleiste des Operations Center auf Aktualisierungen > Clients. Die Seite Aktualisierungen des Clients für Sichern/Archivieren wird geöffnet.
2. Bestimmen Sie anhand der Informationen auf der Seite das zu installierende Release, klicken Sie auf Aktualisierung planen und führen Sie die Schritte im Assistenten aus.

## Nächste Schritte

---

Um Aktualisierungen zu überwachen, abzurechnen oder erneut zu planen, klicken Sie auf Aktualisierungen > Geplant.

Informationen zur Diagnose und Behebung von Problemen finden Sie in Technote 2007749.

### Zugehörige Informationen:

SET SERVERHLADDRESS (Adresse der höheren Ebene für einen Server definieren)  
SET SERVERLLADDRESS (Adresse der unteren Ebene für einen Server definieren)  
SET SERVERPASSWORD (Kennwort für Server festlegen)  
DEFINE SERVER (Server für Übertragung zwischen Servern definieren)  
RESTHTTPSPORT

## Maßnahmen anpassen

---

Die Ziele eines Unternehmens zum Schützen und Aufbewahren von Daten werden normalerweise durch Führungskräfte, Rechtsberater oder andere Personen in Führungspositionen definiert. *Maßnahmen* sind das Mittel, um den Einsatz von IBM Spectrum Protect und die Datenschutz- und Datenaufbewahrungsziele Ihres Unternehmens aufeinander abzustimmen.

## Informationen zu diesem Vorgang

---

Um Datenschutz und Datenaufbewahrung automatisch verwalten zu können, definieren Sie Maßnahmen; dies sind Regeln, die Sie auf dem Server festlegen. Maßnahmen haben Auswirkungen darauf, wie viele Daten im Laufe der Zeit gespeichert werden und wie lange Daten aufbewahrt werden und für die Zurückschreibung durch Clients verfügbar sind. Passen Sie Maßnahmen an, um die Datenschutzziele Ihres Unternehmens zu erreichen.

Die Auswahl der Maßnahme, mit der die Daten eines Clients verwaltet werden, erfolgt über die Zuordnung des Clients zu einer Maßnahmendomäne. Clients unterschiedlicher Typen haben unterschiedliche Aufbewahrungsanforderungen und die Anpassung und Erstellung von Maßnahmen ist normalerweise erforderlich.

Wenn ein Server installiert wird, verfügt er standardmäßig über exakt eine Maßnahme in exakt einer Maßnahmendomäne. Sie können diese Maßnahme anpassen und eigene Maßnahmen erstellen.

- **Maßnahmenkonzepte**  
Die Maßnahme für einen bestimmten Client wird durch die Einstellungen in der Maßnahmendomäne festgelegt, der ein Client hinzugefügt wird.
- **Maßnahme anpassen**  
Sie können vorhandene Maßnahmen anpassen, um neue oder überarbeitete Datenaufbewahrungsanforderungen Ihres Unternehmens zu erfüllen. Eine typische Möglichkeit zum Starten der Maßnahmenanpassung ist das Ändern einer Maßnahmendomäne oder das Kopieren einer vorhandenen Maßnahmendomäne.
- **Maßnahme durch Kopieren einer vorhandenen Maßnahme erstellen**  
Sie können neue Maßnahmen erstellen, indem Sie eine vorhandene Maßnahme kopieren und dann die Teile aktualisieren, die geändert werden sollen.
- **Maßnahmendomäne erstellen**  
Möglicherweise möchten Sie für jeden Typ von Client, der vom Server geschützt wird, eine neue Maßnahmendomäne erstellen. Möglicherweise möchten Sie auch die Zuständigkeit für Clients auf mehrere Administratoren verteilen, indem Sie Ihnen Berechtigung für bestimmte Maßnahmendomänen erteilen.
- **Clientoperationen über Clientoptionsgruppen steuern**  
Mithilfe von Clientoptionsgruppen können Sie die Verarbeitungsoptionen, die Clients für Operationen wie Sicherungen verwenden, zentral steuern. Mithilfe von Clientoptionsgruppen kann sichergestellt werden, dass Daten konsistent gemäß Ihren Anforderungen geschützt werden. Eine Clientoptionsgruppe kann Optionen in einer lokalen Clientoptionsdatei überschreiben oder Optionen hinzufügen, die unter Umständen nicht in der lokalen Clientoptionsdatei vorhanden sind.

## Maßnahmenkonzepte

---

Die Maßnahme für einen bestimmten Client wird durch die Einstellungen in der Maßnahmendomäne festgelegt, der ein Client hinzugefügt wird.

Während des Clientregistrierungsprozesses ordnen Sie einen Client einer *Maßnahmendomäne* zu. Die Maßnahme für jeden Client wird durch die Regeln in der Maßnahmendomäne festgelegt, der der Client zugeordnet ist. In der Maßnahmendomäne befinden sich die Regeln, die wirksam sind, in der aktiven *Maßnahmengruppe*.

Wenn ein Client eine Datei sichert oder archiviert, wird die Datei an eine Verwaltungsklasse in der aktiven Maßnahmengruppe der Maßnahmendomäne gebunden. Eine *Verwaltungsklasse* ist die wichtigste Gruppe von Regeln zur Verwaltung von Clientdaten. Die Sicherungs- und Archivierungsoperationen auf dem Client verwenden die Einstellungen in der Standardverwaltungsgruppe der Maßnahmendomäne, es sei denn, Sie passen die Maßnahme an.

Eine Maßnahme kann angepasst werden, indem weitere Verwaltungsklassen in der Maßnahmengruppe definiert werden, die Maßnahmengruppe aktiviert wird und die Verwendung der neuen Verwaltungsklassen über Clientoptionen zugeordnet wird.

Clientoptionen können in einer lokalen, editierbaren Datei auf dem Clientsystem und in einer Clientoptionsgruppe auf dem Server angegeben werden. Die Optionen in der Clientoptionsgruppe auf dem Server können die Optionen in der lokalen Clientoptionsdatei überschreiben oder den Optionen in der lokalen Clientoptionsdatei hinzugefügt werden.

Der Server verwendet die Maßnahme in Verwaltungsklassen, um Dateien abhängig davon, ob Dateiversionen aktiv oder inaktiv sind, zu verwalten. Die neueste Sicherungskopie oder archivierte Kopie einer Datei ist die *aktive Version*. Aktive Versionen werden nie aus dem Serverspeicher gelöscht.

Sicherungsversionen, die älter als die neueste Version sind, werden als *inaktive Versionen* bezeichnet. Eine aktive Version einer Datei wird inaktiv, wenn eines der folgenden Ereignisse eintritt:

- Die Datei wird erneut gesichert, wodurch eine neuere Version der Datei im Serverspeicher erstellt wird.
- Die Datei wird aus dem Speicher auf dem Clientknoten gelöscht und anschließend wird eine Teilsicherungsoperation ausgeführt. Bei einer *Teilsicherung*, der typischen Sicherungsoperation für einen Client, werden nur die Dateien gesichert, die sich seit der letzten Sicherung geändert haben.

Die Einstellungen in der Verwaltungsklasse, die an eine Datei gebunden ist, legen fest, wie lange und wie viele inaktive Versionen der Datei aufbewahrt werden.

Die *Verfallsverarbeitung* bestimmt mithilfe von Maßnahmen, wann inaktive Versionen nicht mehr benötigt werden, d. h., wann die Versionen verfallen. Der Verfallsprozess auf dem Server setzt Maßnahmen um, die Sie für die Datenaufbewahrung definieren; Sie müssen die regelmäßige Ausführung des Verfallsprozesses planen. Wenn beispielsweise eine Maßnahme die Aufbewahrung von maximal vier Versionen erfordert, verfällt die fünfte und älteste Version. Während der Verfallsverarbeitung entfernt der Server Einträge für verfallene Versionen aus der Datenbank, wodurch die Versionen tatsächlich aus dem Serverspeicher gelöscht werden.

- **Aufbewahrung und Verfall von Sicherungsversionen**  
Mehrere Versionen von Dateisicherungen sind wichtig, da Benutzer fortlaufend Dateien aktualisieren können und eine Datei möglicherweise mit dem Stand eines anderen Zeitpunkts zurückspeichern müssen. Richtlinieneinstellungen steuern die Sicherungsversionen, die der Server im Serverspeicher aufbewahrt, und haben Auswirkungen darauf, welche Daten Benutzer zurückschreiben können.
- **Aktivierung der Maßnahme nach Aktualisierungen**  
Wenn Sie Aktualisierungen an einer Maßnahme vornehmen, werden die Aktualisierungen erst wirksam, wenn Sie die aktualisierte Maßnahme aktivieren.

#### Zugehörige Konzepte:

➔ Vollständige Teilsicherung und partielle Teilsicherung

## Aufbewahrung und Verfall von Sicherungsversionen

---

Mehrere Versionen von Dateisicherungen sind wichtig, da Benutzer fortlaufend Dateien aktualisieren können und eine Datei möglicherweise mit dem Stand eines anderen Zeitpunkts zurückspeichern müssen. Richtlinieneinstellungen steuern die Sicherungsversionen, die der Server im Serverspeicher aufbewahrt, und haben Auswirkungen darauf, welche Daten Benutzer zurückschreiben können.

Mithilfe der Einstellungen in der Verwaltungsklasse können Sie die Versionen angeben, die der Server im Serverspeicher aufbewahrt:

- Geben Sie die Anzahl Tage für die Aufbewahrung von Sicherungsversionen an.  
Die Anzahl Tage für die Aufbewahrung von Sicherungsversionen wird über Einstellungen im Operations Center angegeben:
  - Zusätzliche Sicherungen aufbewahren; dies ist die Anzahl Tage für die Aufbewahrung inaktiver Sicherungsversionen. Die Tage werden ab dem Tag gezählt, an dem die Version inaktiv wird.

Wenn Sie Befehle verwenden, verwenden Sie den Befehl `DEFINE COPYGROUP` mit dem Parameter `RETEXTRA`.

Tipp: Um sicherstellen zu können, dass Dateien nach einem Malwarevorfall, wie beispielsweise einer Ransomware-Attacke, wiederhergestellt werden können, geben Sie einen Wert von mindestens 14 Tagen an. Der bevorzugte Wert ist 30 Tage oder mehr.

- Gelöschte Sicherungen aufbewahren; dies ist die Anzahl Tage für die Aufbewahrung der letzten Sicherungsversion einer Datei, die aus dem Clientdateisystem gelöscht wurde.

Wenn Sie Befehle verwenden, verwenden Sie den Befehl `DEFINE COPYGROUP` mit dem Parameter `REONLY`.

Tipp: Um sicherstellen zu können, dass Dateien nach einem Malwarevorfall, wie beispielsweise einer Ransomware-Attacke, wiederhergestellt werden können, geben Sie einen Wert von mindestens 30 Tagen an.

- Geben Sie die Anzahl aufzubewahrender Versionen an.  
Die Anzahl aufzubewahrender Sicherungsversionen wird über Einstellungen im Operations Center angegeben:
  - Sicherungen; dies ist die Anzahl aufzubewahrender Versionen einer Datei, die noch auf dem Clientdateisystem vorhanden ist.

Wenn Sie Befehle verwenden, verwenden Sie den Befehl `DEFINE COPYGROUP` mit dem Parameter `VEREXISTS`.

Tipp: Um sicherstellen zu können, dass Dateien nach einem Malwarevorfall, wie beispielsweise einer Ransomware-Attacke, wiederhergestellt werden können, geben Sie einen Wert von mindestens 2 an. Bevorzugte Werte sind 3, 4 oder höher.

- Gelöschte Sicherungen; dies ist die Anzahl aufzubewahrender Versionen einer Datei, die aus dem Clientdateisystem gelöscht wurde.

Wenn Sie Befehle verwenden, verwenden Sie den Befehl `DEFINE COPYGROUP` mit dem Parameter `VERDELETED`.

- Geben Sie eine Kombination aus Anzahl Versionen und Anzahl Tage für deren Aufbewahrung an.

Die Interaktion der Einstellungen legt fest, welche Sicherungsversionen der Server aufbewahrt. Sie müssen wissen, welche Einstellungen Vorrang haben und welche Interaktionen erfolgen können:

- Wenn die Anzahl inaktiver Sicherungsversionen die Anzahl in den Einstellungen Sicherungen und Gelöschte Sicherungen überschreitet, verfällt die älteste Version und der Server löscht die Datei bei der nächsten Ausführung der Verfallsverarbeitung aus der Datenbank.
  - Die Anzahl inaktiver Versionen, die der Server aufbewahrt, wird auch von der Einstellung Zusätzliche Sicherungen aufbewahren beeinflusst. Inaktive Versionen verfallen, wenn die Anzahl Tage, die sie inaktiv sind, den Wert für die Aufbewahrung von Extraversionen überschreitet; dies ist selbst dann der Fall, wenn die zulässige Anzahl Versionen nicht überschritten wird.
- **Dateiverfall und Verfallsverarbeitung**  
Dateien verfallen, wenn sie die Aufbewahrungskriterien, die in der Maßnahme angegeben sind, nicht mehr erfüllen. Durch die Verfallsverarbeitung auf dem Server werden verfallene Dateien aus der Serverdatenbank entfernt und die Dateien aus dem Serverspeicher gelöscht.
  - **Beispiel: Aufbewahrung, wenn eine Maßnahme nur Zeitsteuerelemente verwendet**  
Die einfachste Möglichkeit zur Verwaltung der Datenaufbewahrung besteht in der ausschließlichen Verwendung zeitbasierter Maßnahmen. Wenn die Maßnahme nur zeitbasierte Steuerelemente enthält, werden Dateiversionen auf der Basis der Anzahl Tage aufbewahrt, nachdem die Versionen inaktiv werden.
  - **Beispiel: Aufbewahrung, wenn eine Maßnahme sowohl Versions- als auch Zeitsteuerelemente verwendet**  
Wenn sowohl die Versions- als auch die Zeitsteuerelemente in einer Maßnahme verwendet werden, ermöglicht dies Flexibilität bei der Handhabung der Datenaufbewahrung, hat jedoch auch Komplexität zur Folge. Studieren Sie zum besseren Verständnis der Interaktion zwischen Steuerelementen die Beispielmaßnahmen und ihre Auswirkungen auf die Aufbewahrung von Sicherungsversionen einer einzelnen Datei für die Dauer eines Monats.
  - **Interaktionen zwischen Maßnahmeneinstellungen**  
Zeitbasierte und versionsbasierte Maßnahmeneinstellungen interagieren, wenn sie gemeinsam in einer Verwaltungsklasse für eine Maßnahme verwendet werden. Die Häufigkeit von Clientsicherungen wirkt sich auch auf die Sicherungsversionen aus, die für einen Client gespeichert werden.

## Dateiverfall und Verfallsverarbeitung

---

Dateien verfallen, wenn sie die Aufbewahrungskriterien, die in der Maßnahme angegeben sind, nicht mehr erfüllen. Durch die Verfallsverarbeitung auf dem Server werden verfallene Dateien aus der Serverdatenbank entfernt und die Dateien aus dem Serverspeicher gelöscht.

Dateien verfallen unter folgenden Bedingungen:

- Benutzer löschen Dateibereiche von Clientknoten.
- Benutzer definieren Dateien mit dem Befehl EXPIRE auf dem Client als verfallen.
- Eine Sicherungsversion einer Datei erfüllt nicht mehr die Kriterien für die Aufbewahrung von Sicherungen (Aufbewahrungsdauer einer Datei und Anzahl inaktiver Versionen einer Datei, die aufbewahrt werden).
- Eine archivierte Datei erfüllt nicht mehr die Kriterien für die Aufbewahrung archivierter Dateien (Aufbewahrungsdauer archivierter Kopien).
- Eine Sicherungsgruppe überschreitet den Aufbewahrungszeitraum, der für die Sicherungsgruppe angegeben ist.

Der Server löscht verfallene Dateien nur während der Verfallsverarbeitung aus der Serverdatenbank. Nachdem verfallene Dateien aus der Datenbank gelöscht wurden, kann der Server den Speicherbereich in den Speicherpools, den die verfallenen Dateien belegten, wiederverwenden. Stellen Sie sicher, dass die Verfallsverarbeitung regelmäßig ausgeführt wird, damit der Server den Speicherbereich wiederverwenden kann.

## Einschränkungen bei der Verfallsverarbeitung

---

Die Verwendung einiger Funktionen wirkt sich auf die Verfallsverarbeitung aus.

### Replikation

Wenn Sie ungleiche Maßnahmen auf dem Quellenserver und dem Zielsystem verwenden, werden Dateien, die auf dem Quellenreplikationsserver für den sofortigen Verfall markiert sind, erst gelöscht, nachdem sie auf den Zielreplikationsserver repliziert wurden. Wenn Sie keine ungleichen Maßnahmen verwenden, werden Dateien, die auf dem Quellenreplikationsserver für den sofortigen Verfall markiert sind, sofort gelöscht.

Auf dem Zielreplikationsserver werden Dateien, die als verfallen markiert sind, gelöscht, wenn der Zielreplikationsserver die Verfallsverarbeitung ausführt.

### Ereignisgesteuerte Aufbewahrung für Archivierungsdaten

Eine Archivierungsdatei kann nicht für die Verfallsverarbeitung ausgewählt werden, wenn die Datei den Status 'Löschen unzulässig' hat. Wenn eine Datei nicht den Status 'Löschen unzulässig' hat, wird sie gemäß der vorhandenen Verfallsverarbeitung verarbeitet.



## Zugehörige Tasks:

☛ Verfall/Löschen anhalten und freigeben

# Beispiel: Aufbewahrung, wenn eine Maßnahme nur Zeitsteuerelemente verwendet

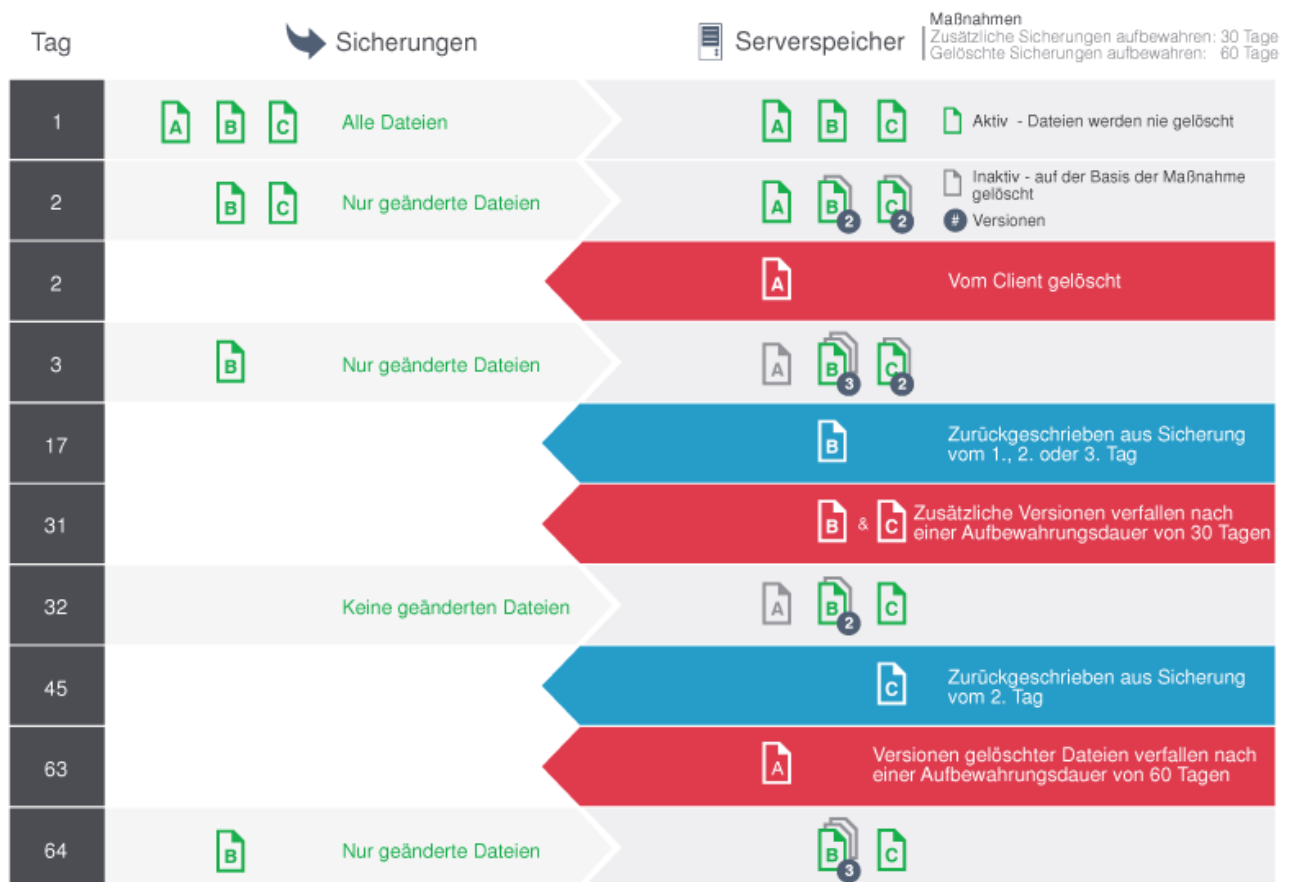
Die einfachste Möglichkeit zur Verwaltung der Datenaufbewahrung besteht in der ausschließlichen Verwendung zeitbasierter Maßnahmen. Wenn die Maßnahme nur zeitbasierte Steuerelemente enthält, werden Dateiversionen auf der Basis der Anzahl Tage aufbewahrt, nachdem die Versionen inaktiv werden.

Für eine Maßnahme, die nur auf der Zeit basiert, verwenden Sie die Steuerelemente **Zusätzliche Sicherungen aufbewahren** und **Gelöschte Sicherungen aufbewahren**. Mit diesem Typ von Maßnahme wird nicht die Anzahl Dateiversionen begrenzt. Wenn Clients häufig Sicherungen ausführen, stellen Sie sicher, dass der Serverspeicher die potenzielle Anzahl Dateiversionen handhaben kann.

Die folgende Abbildung zeigt die Handhabung von Dateien eines Clients durch den Server im Laufe der Zeit, wenn der Client täglich eine Teilsicherung ausführt.

In diesem Beispiel hat die Maßnahme die folgenden Merkmale:

- Die neueste Version einer Datei wird immer aufbewahrt, solange die Datei noch auf dem Clientsystem vorhanden ist. Die neueste Version ist die aktive Version. Dieses Merkmal ist Teil jeder Maßnahme auf dem Server.
- Die Einstellung **Zusätzliche Sicherungen aufbewahren** ist auf 30 Tage gesetzt. Wenn eine neuere Sicherung erstellt wird, wird eine Dateiversion inaktiv und im Serverspeicher 30 Tage lang aufbewahrt.
- Die Einstellung **Gelöschte Sicherungen aufbewahren** ist auf 60 Tage gesetzt. Wenn eine Datei aus dem Clientsystem gelöscht wird, werden alle Versionen der Datei im Serverspeicher inaktiv. Diese inaktiven Versionen werden 60 Tage lang aufbewahrt, nachdem die Dateiversionen inaktiv werden.



# Beispiel: Aufbewahrung, wenn eine Maßnahme sowohl Versions- als auch Zeitsteuerelemente verwendet

Wenn sowohl die Versions- als auch die Zeitsteuerelemente in einer Maßnahme verwendet werden, ermöglicht dies Flexibilität bei der Handhabung der Datenaufbewahrung, hat jedoch auch Komplexität zur Folge. Studieren Sie zum besseren Verständnis der Interaktion zwischen Steuerelementen die Beispielmaßnahmen und ihre Auswirkungen auf die Aufbewahrung von Sicherungsversionen einer einzelnen Datei für die Dauer eines Monats.

Siehe Tabelle 1 und Abbildung 1. Ein Client sichert die Datei REPORT.TXT vier Mal in einem Monat (vom 23. März bis zum 23. April). Die Einstellungen in der Sicherungskopiengruppe der Verwaltungsklasse, an die REPORT.TXT gebunden ist, legen fest, wie der Server diese Sicherungsversionen handhabt. In Tabelle 2 wird gezeigt, wie sich unterschiedliche Kopiengruppeneinstellungen am 24. April (ein Tag, nachdem die Datei zuletzt gesichert wurde) auf die Versionen auswirken.

Tabelle 1. Status der Sicherungsversionen von REPORT.TXT am 24. April

| Version   | Erstellungsdatum | Tage seit die Version inaktiv wurde |
|-----------|------------------|-------------------------------------|
| Aktiv     | 23. April        | (nicht zutreffend)                  |
| Inaktiv 1 | 13. April        | 1 (seit 13. April)                  |
| Inaktiv 2 | 31. März         | 11 (seit 13. April)                 |
| Inaktiv 3 | 23. März         | 24 (seit 31. März)                  |

Abbildung 1. Aktive und inaktive Versionen von REPORT.TXT

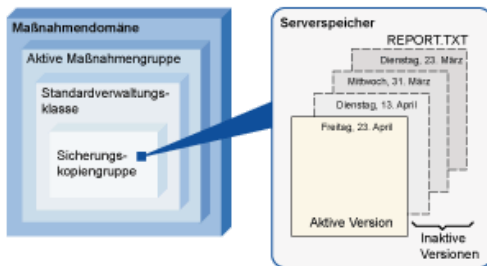


Tabelle 2. Auswirkungen der Maßnahme auf die Aufbewahrung von Sicherungsversionen für REPORT.TXT am 24. April

| Sicherungen | Gelöschte Sicherungen | Zusätzliche Sicherungen aufbewahren | Gelöschte Sicherungen aufbewahren | Ergebnisse  |
|-------------|-----------------------|-------------------------------------|-----------------------------------|---|
| 4 Versionen | 2 Versionen           | 60 Tage                             | 180 Tage                          | <p>Die Einstellungen Sicherungen und Zusätzliche Sicherungen aufbewahren steuern den Verfall der Versionen. Die am 23. März erstellte Version wird so lange beibehalten, bis die Datei erneut gesichert wird (und damit eine vierte inaktive Version erstellt wird) oder die Version eine Inaktivität von 60 Tagen erreicht.</p> <p>Wenn der Benutzer die Datei REPORT.TXT aus dem Clientdateisystem löscht, erkennt der Server die Löschung bei der nächsten vollständigen Teilsicherungsoperation durch den Client. Ab diesem Punkt sind die Einstellungen Gelöschte Sicherungen und Gelöschte Sicherungen aufbewahren auch für die Aufbewahrung wirksam. Alle Versionen sind jetzt inaktiv.</p> <p>Zwei der vier Versionen verfallen sofort (die Versionen vom 23. März und 31. März verfallen). Die Version vom 13. April verfällt nach einer Inaktivität von 60 Tagen (am 23. Juni). Der Server bewahrt die letzte noch verbleibende inaktive Version (die Version vom 23. April) 180 Tage lang auf, nachdem sie inaktiv wird.</p> |

| Sicherungen      | Gelöschte Sicherungen | Zusätzliche Sicherungen aufbewahren | Gelöschte Sicherungen aufbewahren | Ergebnisse   |
|------------------|-----------------------|-------------------------------------|-----------------------------------|--|
| Keine Begrenzung | 2 Versionen           | 60 Tage                             | 180 Tage                          | <p>Die Einstellung Zusätzliche Sicherungen aufbewahren steuert den Verfall der Versionen. Die inaktiven Versionen (mit Ausnahme der letzten verbleibenden Version) verfallen nach einer Inaktivität von 60 Tagen.</p> <p>Wenn der Benutzer die Datei REPORT.TXT aus dem Clientknoten löscht, erkennt der Server die Löschung bei der nächsten vollständigen Teilsicherungsoperation durch den Client. Ab diesem Punkt sind die Einstellungen Gelöschte Sicherungen und Gelöschte Sicherungen aufbewahren auch für die Aufbewahrung wirksam. Alle Versionen sind jetzt inaktiv.</p> <p>Zwei der vier Versionen verfallen sofort (die Versionen vom 23. März und 31. März verfallen), da nur zwei Versionen zulässig sind. Die Version vom 13. April verfällt nach einer Inaktivität von 60 Tagen (am 22. Juni). Der Server bewahrt die letzte noch verbleibende inaktive Version (die Version vom 23. April) 180 Tage lang auf, nachdem sie inaktiv wird.</p> |
| Keine Begrenzung | Keine Begrenzung      | 60 Tage                             | 180 Tage                          | <p>Die Einstellung Zusätzliche Sicherungen aufbewahren steuert den Verfall der Versionen. Der Server lässt inaktive Versionen nicht aufgrund der maximalen Anzahl Sicherungskopien verfallen. Die inaktiven Versionen (mit Ausnahme der letzten verbleibenden Version) verfallen nach einer Inaktivität von 60 Tagen.</p> <p>Wenn der Benutzer die Datei REPORT.TXT aus dem Clientknoten löscht, erkennt der Server die Löschung bei der nächsten vollständigen Teilsicherungsoperation durch den Clientknoten. Ab diesem Punkt ist die Einstellung Gelöschte Sicherungen aufbewahren auch für die Aufbewahrung wirksam. Alle Versionen sind jetzt inaktiv.</p> <p>Drei der vier Versionen verfallen nach einer Inaktivität von jeweils 60 Tagen. Der Server bewahrt die letzte noch verbleibende inaktive Version (die Version vom 23. April) 180 Tage lang auf, nachdem sie inaktiv wird.</p>  |
| 4 Versionen      | 2 Versionen           | Keine Begrenzung                    | Keine Begrenzung                  | <p>Die Einstellung Sicherungen steuert den Verfall der Versionen, bis ein Benutzer die Datei aus dem Clientknoten löscht. Der Server lässt inaktive Versionen nicht aufgrund ihres Alters verfallen.</p> <p>Wenn der Benutzer die Datei REPORT.TXT aus dem Clientknoten löscht, erkennt der Server die Löschung bei der nächsten vollständigen Teilsicherungsoperation durch den Clientknoten. Ab diesem Punkt steuert die Einstellung Gelöschte Sicherungen den Verfall. Alle Versionen sind jetzt inaktiv.</p> <p>Zwei der vier Versionen verfallen sofort (die Versionen vom 23. März und 31. März verfallen), da nur zwei Versionen zulässig sind. Der Server bewahrt die beiden verbleibenden inaktiven Versionen unbegrenzt auf.</p>   |

#### Zugehörige Konzepte:

➔ Vollständige Teilsicherung und partielle Teilsicherung

## Interaktionen zwischen Maßnahmeneinstellungen

Zeitbasierte und versionsbasierte Maßnahmeneinstellungen interagieren, wenn sie gemeinsam in einer Verwaltungsklasse für eine Maßnahme verwendet werden. Die Häufigkeit von Clientsicherungen wirkt sich auch auf die Sicherungsversionen aus, die für einen Client gespeichert werden.

Betrachten Sie bei einem Clientsystem, für das zweimal am Tag eine Sicherung ausgeführt werden muss, die Auswirkungen der folgenden Auswahlangaben für die Maßnahme für eine Datei, die sich häufig ändert:

- Die Einstellung Zusätzliche Sicherungen aufbewahren wird auf 30 Tage gesetzt. Die Einstellung Sicherungen wird auf Keine Begrenzung gesetzt, sodass die Maßnahme die Anzahl Versionen nicht begrenzt. Nach 30 Tagen könnte der Server über 60 Sicherungsversionen der Datei verfügen, wenn sich die Datei zwischen jeder der beiden Sicherungsoperationen, die täglich ausgeführt werden, ändert. Für den Client kann wahlweise jede der 60 Versionen der vergangenen 30 Tage zurückgeschrieben werden.

- Die Einstellung **Zusätzliche Sicherungen aufbewahren** wird auf **Keine Begrenzung** und die Einstellung **Sicherungen** auf **30 Versionen** gesetzt. Wenn sich die Datei zwischen jeder der beiden Sicherungsoperationen, die täglich ausgeführt werden, ändert, verfügt der Server nach 15 Tagen über 30 Sicherungsversionen. Nach 30 Tagen verfügt der Server immer noch nur über 30 Sicherungsversionen, da für die Anzahl Versionen eine Begrenzung festgelegt wurde. Wenn sich die Datei weiterhin zwischen jeder der beiden Sicherungsoperationen, die täglich ausgeführt werden, ändert, stammen die Sicherungsversionen unter Umständen nur aus den letzten 15 Tagen. Für den Client kann wahlweise eine der 30 Versionen, die möglicherweise nicht älter als 15 Tage sind, zurückgeschrieben werden.

Die Beispiele zeigen, dass unter der Voraussetzung, dass Sicherungsversionen für eine bestimmte Anzahl Tage verfügbar sein müssen, die einfachste Möglichkeit zur Implementierung dieser Voraussetzung in der Verwendung einer zeitbasierten Maßnahme besteht. Setzen Sie die Einstellung **Zusätzliche Sicherungen aufbewahren** auf die spezifische Anzahl Tage und die Einstellung **Sicherungen** auf **Keine Begrenzung**.

Die Auswirkungen des Werts **Keine Begrenzung** in den Maßnahmeneinstellungen sind von den anderen definierten Steuerelementen für die Maßnahme abhängig:

#### Zusätzliche Sicherungen aufbewahren

Wenn Sie **Keine Begrenzung** angeben, werden inaktive Sicherungsversionen auf der Basis der Einstellung **Sicherungen** oder **Gelöschte Sicherungen** gelöscht.

Um Clientknoten die Zurückschreibung von Dateien mit dem Stand eines bestimmten Zeitpunkts zu ermöglichen, setzen Sie die Einstellung **Sicherungen** oder **Gelöschte Sicherungen** auf **Keine Begrenzung**. Setzen Sie die Einstellung **Zusätzliche Sicherungen aufbewahren** auf die Anzahl Tage, für die Clients voraussichtlich Dateiversionen für eine mögliche Zurückschreibung nach Zeitpunkt benötigen. Um beispielsweise Clients die Zurückschreibung von Dateien mit dem Stand eines Zeitpunkts zu ermöglichen, der 60 Tage in der Vergangenheit liegt, setzen Sie die Einstellung **Zusätzliche Sicherungen aufbewahren** auf 60.

#### Gelöschte Sicherungen aufbewahren

Wenn Sie **Keine Begrenzung** angeben, wird die letzte Version unbegrenzt aufbewahrt, es sei denn, die Datei wird von einem Benutzer oder einem Administrator aus dem Serverspeicher gelöscht.

#### Sicherungen

Wenn der Wert auf **Keine Begrenzung** gesetzt wird, ist möglicherweise mehr Speicher erforderlich; in einigen Situationen kann die Angabe dieses Werts jedoch erforderlich sein. Um beispielsweise Clientknoten die Zurückschreibung von Dateien mit dem Stand eines bestimmten Zeitpunkts zu ermöglichen, setzen Sie den Wert für **Sicherungen** auf **Keine Begrenzung**. Indem Versionen keine Begrenzung auferlegt wird, wird sichergestellt, dass der Server Versionen gemäß der Einstellung **Zusätzliche Sicherungen aufbewahren** aufbewahrt.

#### Gelöschte Sicherungen

Wenn der Wert auf **Keine Begrenzung** gesetzt wird, ist möglicherweise mehr Speicher erforderlich; in einigen Situationen kann die Angabe dieses Werts jedoch erforderlich sein. Setzen Sie beispielsweise den Wert für die Einstellung **Gelöschte Sicherungen** auf **Keine Begrenzung**, um Clients die Zurückschreibung von Dateien mit dem Stand eines bestimmten Zeitpunkts zu ermöglichen. Indem Versionen keine Begrenzung auferlegt wird, wird sichergestellt, dass der Server Versionen gemäß der Einstellung **Zusätzliche Sicherungen aufbewahren** aufbewahrt.

## Querverweis für Felder des Operations Center und Serverbefehlsparameter

In der folgenden Tabelle sind die Felder des Operations Center mit den entsprechenden Parametern des Befehls `DEFINE COPYGROUP TYPE=BACKUP` aufgeführt.

| Feldname in Sichten des Operations Center | Parameter im Befehl <code>DEFINE COPYGROUP TYPE=BACKUP</code> |
|---|---|
| Zusätzliche Sicherungen aufbewahren       | REXTRA  |
| Gelöschte Sicherungen aufbewahren         | REONLY  |
| Sicherungen                               | VEREXISTS   |
| Gelöschte Sicherungen                     | VERDELETED  |

## Aktivierung der Maßnahme nach Aktualisierungen

Wenn Sie Aktualisierungen an einer Maßnahme vornehmen, werden die Aktualisierungen erst wirksam, wenn Sie die aktualisierte Maßnahme aktivieren.

Mit der Aktivierung der Maßnahmengruppe werden die durchgeführten Aktualisierungen wirksam. Beispielsweise werden die folgenden Aktualisierungstypen wirksam, wenn Sie die Maßnahmengruppe aktivieren:

- Sie definieren eine neue Maßnahmendomäne mit einer Maßnahmengruppe und einer oder mehreren Verwaltungsklassen.
- Sie fügen einer Maßnahmengruppe eine Verwaltungsklasse hinzu.
- Sie ändern die Einstellungen für die Aufbewahrung von Sicherungen in einer vorhandenen Verwaltungsklasse.

## Prüfung der Maßnahmengruppe vor der Aktivierung

Im Operations Center ist die Prüfung kein separater Schritt. Wenn Sie Befehle verwenden, ist die Prüfung ein optionaler Befehl, der Ihnen die Gelegenheit gibt, eine Vorschau der Auswirkungen der Aktivierung einer geänderten Maßnahmengruppe anzuzeigen. Wenn Sie eine Maßnahmengruppe prüfen, meldet der Server Bedingungen zurück, die beim Aktivieren der Maßnahmengruppe Probleme verursachen können.

Die Prüfung schlägt fehl, wenn die Maßnahmengruppe keine Standardverwaltungs-kategorie enthält. Die Prüfung hat Warnungen zur Folge, wenn eine der in Tabelle 1 aufgeführten Bedingungen erfüllt ist.

Tabelle 1. Bedingungen, die während der Prüfung der Maßnahmengruppe Warnungen zur Folge haben

| Bedingung   | Grund für Warnung   |
|---|---|
| Die für Sicherungs-, Archivierungs- oder Umlagerungsoperationen angegebenen Speicherziele sind keine definierten Speicherpools.   | Ein Speicherpool muss vorhanden sein, bevor er als Ziel angegeben werden kann.  |
| Ein für Sicherungs-, Archivierungs- oder Umlagerungsoperationen angegebenes Speicherziel ist ein Kopierspeicherpool oder ein Pool für aktive Daten.   | Das Speicherziel muss ein primärer Speicherpool sein.   |
| Die Standardverwaltungs-kategorie enthält keine Sicherungs- oder Archivierungseinstellungen.  | Wenn die Standardverwaltungs-kategorie keine Sicherungs- oder Archivierungseinstellungen enthält, werden alle Dateien, die an die Standardverwaltungs-kategorie gebunden sind, nicht gesichert oder archiviert.   |
| In der aktuellen aktiven Maßnahmengruppe ist eine Verwaltungskategorie angegeben, die in der Maßnahmengruppe, die geprüft wird, nicht definiert ist.  | Wenn Sie Dateien sichern, die an eine Verwaltungskategorie gebunden wurden, die in der aktiven Maßnahmengruppe nicht mehr vorhanden ist, werden Sicherungs-versionen erneut an die Standardverwaltungs-kategorie gebunden.<br><br>Wenn die Verwaltungskategorie, an die eine Archivierungskopie gebunden ist, nicht mehr vorhanden ist und die Standardverwaltungs-kategorie keine Archivierungseinstellungen enthält, verwendet der Server für die Aufbewahrung der Archivierungskopie den Aufbewahrungszeitraum für Archivierung.<br><br>Der Aufbewahrungszeitraum für Archivierung wird für eine Maßnahmendomäne definiert und diese Einstellung wird nur verwendet, wenn zur Verwaltung einer Archivierungskopie keine andere Maßnahmeneinstellung verfügbar ist. |
| Die aktuelle aktive Maßnahmengruppe enthält Sicherungseinstellungen, die in der Maßnahmengruppe, die geprüft wird, nicht definiert sind.  | Wenn ein Client eine Datei sichert und die Verwaltungskategorie, an die die Datei gebunden ist, keine Sicherungseinstellungen mehr enthält, werden die Sicherungs-versionen gemäß der Standardverwaltungs-kategorie verwaltet.<br><br>Wenn die Standardverwaltungs-kategorie keine Sicherungseinstellungen enthält, verwendet der Server den Aufbewahrungszeitraum für Sicherung zur Verwaltung von Dateiversionen. Die Datei wird jedoch bei der nächsten Sicherungsoperation nicht gesichert.<br><br>Der Aufbewahrungszeitraum für Sicherung wird für eine Maßnahmendomäne definiert und diese Einstellung wird nur verwendet, wenn zur Verwaltung einer Sicherungs-version keine andere Maßnahmeneinstellung verfügbar ist.  |
| Eine Verwaltungskategorie gibt an, dass eine Sicherungs-version vorhanden sein muss, bevor eine Datei aus einem Clientknoten umgelagert werden kann, die Verwaltungskategorie enthält jedoch keine Sicherungseinstellungen. | Diese Warnung gilt nur, wenn Sie das Produkt IBM Spectrum Protect for Space Management verwenden. Die Konflikte innerhalb der Verwaltungskategorie können Probleme für IBM Spectrum Protect for Space Management-Clients zur Folge haben.   |

## Aktivierung der Maßnahmengruppe

Wenn Sie eine Maßnahmengruppe aktivieren, prüft der Server den Inhalt der Maßnahmengruppe und kopiert die Maßnahmengruppe als aktive Maßnahmengruppe. Um den Inhalt der aktiven Maßnahmengruppe später ändern zu können, muss eine weitere Maßnahmengruppe erstellt oder geändert und anschließend aktiviert werden.

Einige Aktualisierungen an einer Maßnahme werden sofort wirksam, wenn die Maßnahme aktiviert wird, einige andere Aktualisierungen hingegen nicht:

- Aktualisierungen der Einstellungen Zusätzliche Sicherungen aufbewahren und Gelöschte Sicherungen aufbewahren werden sofort auf die Daten angewendet, die bereits im Serverspeicher vorhanden sind, sowie auf zukünftige Sicherungen.

Bei der Verwendung von Befehlen betrifft dies die Parameter RETEXTRA und RETONLY für den Befehl DEFINE COPYGROUP oder UPDATE COPYGROUP.

- Aktualisierungen der Einstellungen Sicherungen und Gelöschte Sicherungen werden für Clientdaten erst wirksam, wenn die Clients die nächste Sicherungsoperation ausführen.

Bei der Verwendung von Befehlen betrifft dies die Parameter VEREXISTS und VERDELETED für den Befehl DEFINE COPYGROUP oder UPDATE COPYGROUP.

## Einschränkungen für Server, die die Funktion für den Datenaufbewahrungsschutz verwenden

Wenn die Funktion für den Datenaufbewahrungsschutz aktiv ist, gelten weitere Regeln, wenn Sie eine Maßnahmengruppe prüfen und aktivieren. Die Funktion für den Datenaufbewahrungsschutz wird aktiviert, indem der Befehl SET ARCHIVERETENTIONPROTECTION auf einem Server ausgegeben wird, der noch nicht über Clientdaten verfügt.

Wenn der Datenaufbewahrungsschutz für einen Server aktiv ist, müssen weitere Regeln erfüllt sein, bevor die Maßnahme aktiviert wird:

- Wenn eine Verwaltungsklasse in der aktiven Maßnahmengruppe vorhanden ist, muss eine Verwaltungsklasse mit demselben Namen in der Maßnahmengruppe vorhanden sein, die aktiviert wird.
- Alle Verwaltungsklassen in der Maßnahmengruppe, die aktiviert wird, müssen Einstellungen für den Aufbewahrungszeitraum für Archivierung enthalten.
- Wenn die aktive Maßnahmengruppe Einstellungen für den Aufbewahrungszeitraum für Archivierung in einer Verwaltungsklasse enthält, muss die Maßnahmengruppe, die aktiviert wird, Werte für den Aufbewahrungszeitraum für Archivierung enthalten, die mindestens so groß wie die entsprechenden Werte in der aktiven Maßnahmengruppe sind.

Wenn der Server ein verwalteter Server in einer unternehmensweiten Konfiguration ist, empfängt der Server möglicherweise Maßnahmenaktualisierungen von dem Server, der als Konfigurationsmanager definiert ist. Maßnahmenaktualisierungen, die der verwaltete Server vom Konfigurationsmanager empfängt, müssen ebenfalls die vorhergehenden Regeln erfüllen.

### **Zugehörige Konzepte:**

 Unternehmensweite Konfiguration (Version 7.1.1)

### **Zugehörige Verweise:**

SET ARCHIVERETENTIONPROTECTION (Aufbewahrungsschutz für Daten aktivieren)

## Maßnahme anpassen

Sie können vorhandene Maßnahmen anpassen, um neue oder überarbeitete Datenaufbewahrungsanforderungen Ihres Unternehmens zu erfüllen. Eine typische Möglichkeit zum Starten der Maßnahmenanpassung ist das Ändern einer Maßnahmendomäne oder das Kopieren einer vorhandenen Maßnahmendomäne.

## Informationen zu diesem Vorgang

Die wichtigsten Maßnahmeneinstellungen befinden sich in Verwaltungsklassen. In Verwaltungsklassen können Sie sowohl die Anzahl Sicherungsversionen als auch die Anzahl Tage für die Aufbewahrung von Sicherungsversionen im Serverspeicher steuern. Wenn Sie beide Steuerungstypen verwenden, ist die Maßnahme komplexer. Wenn die Steuerung nur über die Anzahl Tage für die Aufbewahrung von Sicherungsversionen erfolgt, können Sie einfacher definieren, wie lange gesicherte Daten aufbewahrt werden.

Stellen Sie sicher, dass die Standardverwaltungsklasse in einer Maßnahmendomäne geeignete Datenaufbewahrungseinstellungen für die meisten oder alle Clients hat, die der Domäne zugeordnet sind. Die Aufbewahrungseinstellungen in der Standardverwaltungsklasse werden auf die Daten angewendet, wenn für Clientoperationen keine Verwaltungsklasse angegeben ist.

Sie können Aktualisierungen an einer Maßnahme durchführen und die Änderungen für einen späteren Zeitpunkt speichern. Wenn die Änderungen am Entwurf abgeschlossen sind, können Sie die aktualisierte Maßnahmengruppe aktivieren, damit die Änderungen wirksam werden.

## Vorgehensweise

1. Klicken Sie auf der Seite Übersicht im Operations Center auf das Menü Services.
2. Wählen Sie die Maßnahmendomäne aus und klicken Sie auf Details. Klicken Sie auf Maßnahmengruppen.
3. Klicken Sie auf die Umschaltfläche Konfigurieren, um die Einstellungen aktualisieren zu können.
4. Passen Sie die Einstellungen in der Verwaltungsklasse an.
  - a. Geben Sie Auswahlangaben für Sicherungsservices an. Aktualisieren Sie beispielsweise die folgenden Einträge, sodass inaktive Sicherungsversionen für die Clients 30 Tage lang aufbewahrt werden:
    - Sicherungen: Keine Begrenzung
    - Zusätzliche Sicherungen aufbewahren: 30 Tage
    - Gelöschte Sicherungen: 1
    - Gelöschte Sicherungen aufbewahren: Keine Begrenzung
  - b. Optional: Geben Sie Auswahlangaben für Archivierungsservices an. Ändern Sie beispielsweise die Einstellung Archivierungen aufbewahren in 1 Jahr.
  - c. Klicken Sie auf Sichern.
5. Optional: Klicken Sie auf +Verwaltungsklasse, um eine Verwaltungsklasse hinzuzufügen.
  - a. Geben Sie Auswahlangaben für Basiseinstellungen an und klicken Sie auf Hinzufügen.
  - b. Passen Sie weitere Einstellungen in der neuen Verwaltungsklasse an. Geben Sie für Sicherungsservices Auswahlangaben in den folgenden Spalten an: Sicherungsziel, Sicherungen, Zusätzliche Sicherungen aufbewahren, Gelöschte Sicherungen und Gelöschte Sicherungen aufbewahren. Geben Sie für Archivierungsservices Auswahlangaben in den Spalten Archivierungsziel und Archivierungen aufbewahren an.
  - c. Klicken Sie auf Sichern.
6. Stellen Sie sicher, dass in der Spalte Standard eine entsprechende Verwaltungsklasse als Standardverwaltungsklasse ausgewählt ist. Die Aufbewahrungseinstellungen in der Standardverwaltungsklasse werden angewendet, wenn für Clientoperationen keine Verwaltungsklasse angegeben ist. Eine Verwaltungsklasse kann angegeben werden, wenn eine Clientoperation ausgeführt wird. Eine Verwaltungsklasse kann auch in einer Clientoptionsdatei auf dem Clientsystem oder in einer Clientoptionsgruppe, die auf dem Server definiert ist, angegeben werden.
7. Aktivieren Sie die Maßnahmengruppe, indem Sie auf Aktivieren klicken.
8. Ordnen Sie der neuen Maßnahmendomäne Clientknoten zu, indem Sie entweder vorhandene Clientknoten aktualisieren oder neue Knoten registrieren.
  - Um der Maßnahmendomäne neue Clients hinzuzufügen, klicken Sie auf +Client.
  - Um einen vorhandenen Client in die Maßnahmendomäne zu versetzen, wählen Sie den Client aus, klicken Sie auf Details und klicken Sie dann auf die Registerkarte Merkmale. Wählen Sie die neue Maßnahmendomäne aus und klicken Sie auf Sichern.

Die Datenaufbewahrung für den Client, den Sie der Maßnahmendomäne zuordnen, wird jetzt durch diese Maßnahme gesteuert. Voraussetzung: Wenn ein Client bei der Zuordnung zu einer neuen Domäne aktiv ist, müssen Sie den Client stoppen und erneut starten, damit die Änderung wirksam wird.

#### Zugehörige Tasks:


Clientoperationen über Clientoptionsgruppen steuern

## Maßnahme durch Kopieren einer vorhandenen Maßnahme erstellen

Sie können neue Maßnahmen erstellen, indem Sie eine vorhandene Maßnahme kopieren und dann die Teile aktualisieren, die geändert werden sollen.

### Vorgehensweise

Sie können eine Maßnahme erstellen, indem Sie eine Maßnahmendomäne kopieren, die Verwaltungsklassen aktualisieren und dann der neuen Domäne Clients zuordnen.

1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.
2. Kopieren Sie eine Maßnahmendomäne mit dem Befehl COPY DOMAIN. Kopieren Sie beispielsweise die Standardmaßnahmendomäne STANDARD in eine neue Maßnahmendomäne, NEWDOMAIN:

```
copy domain standard newdomain
```

Mit dieser Operation werden die Maßnahmendomäne und alle zugehörigen Maßnahmengruppen und Verwaltungsklassen kopiert. In diesem Beispiel werden mit der Operation die folgenden Elemente in die Maßnahmendomäne NEWDOMAIN kopiert:

- Eine Maßnahmengruppe mit dem Namen STANDARD
  - Die Verwaltungsklasse mit dem Namen STANDARD, die sich in der Maßnahmengruppe STANDARD befindet
  - Die Kopiengruppen, die in der Verwaltungsklasse STANDARD enthalten sind:
    - Die Sicherungskopiengruppe mit dem Namen STANDARD
    - Die Archivierungskopiengruppe mit dem Namen STANDARD
3. Klicken Sie auf der Seite Übersicht im Operations Center auf das Menü Services.
  4. Wählen Sie die neue Maßnahmendomäne aus und klicken Sie auf Details. Klicken Sie auf Maßnahmengruppen.

5. Klicken Sie auf die Umschaltfläche Konfigurieren, um die Einstellungen aktualisieren zu können.
6. Passen Sie die Einstellungen in den Verwaltungsklassen an.
  - a. Geben Sie Auswahlangaben für Sicherungsservices an. Aktualisieren Sie beispielsweise die folgenden Einträge, sodass inaktive Sicherungsversionen für die Clients 30 Tage lang aufbewahrt werden:
    - Sicherungen: Keine Begrenzung
    - Zusätzliche Sicherungen aufbewahren: 30 Tage
    - Gelöschte Sicherungen: 1
    - Gelöschte Sicherungen aufbewahren: Keine Begrenzung
  - b. Optional: Geben Sie Auswahlangaben für Archivierungsservices an. Ändern Sie beispielsweise die Einstellung Archivierungen aufbewahren in 1 Jahr.
  - c. Klicken Sie auf Sichern.
7. Optional: Nehmen Sie weitere Aktualisierungen und Hinzufügungen vor, wie beispielsweise das Hinzufügen einer Verwaltungsklasse.
  - a. Klicken Sie auf +Verwaltungsklasse, um eine Verwaltungsklasse hinzuzufügen. Geben Sie Auswahlangaben für Basiseinstellungen an und klicken Sie auf Hinzufügen.
  - b. Passen Sie weitere Einstellungen in der neuen Verwaltungsklasse an. Geben Sie für Sicherungsservices Auswahlangaben in den folgenden Spalten an: Sicherungsziel, Sicherungen, Zusätzliche Sicherungen aufbewahren, Gelöschte Sicherungen und Gelöschte Sicherungen aufbewahren. Geben Sie für Archivierungsservices Auswahlangaben in den Spalten Archivierungsziel und Archivierungen aufbewahren an.
  - c. Klicken Sie auf Sichern.
8. Wählen Sie in der Spalte Standard die Standardverwaltungsklasse aus, die von Clients verwendet wird. Klicken Sie auf Sichern. Die Aufbewahrungseinstellungen in der Standardverwaltungsklasse werden angewendet, wenn für Clientoperationen keine Verwaltungsklasse angegeben ist. Eine Verwaltungsklasse kann angegeben werden, wenn eine Clientoperation ausgeführt wird. Eine Verwaltungsklasse kann auch in einer Clientoptionsdatei auf dem Clientsystem oder in einer Clientoptionsgruppe, die auf dem Server definiert ist, angegeben werden.
9. Aktivieren Sie die Maßnahmengruppe, indem Sie auf Aktivieren klicken.
10. Ordnen Sie der neuen Maßnahmendomäne Clientknoten zu, indem Sie entweder vorhandene Clientknoten aktualisieren oder neue Knoten registrieren.
  - Um der Maßnahmendomäne neue Clients hinzuzufügen, klicken Sie auf +Client.
  - Um einen vorhandenen Client in die Maßnahmendomäne zu versetzen, wählen Sie den Client aus, klicken Sie auf Details und klicken Sie dann auf die Registerkarte Merkmale. Wählen Sie die neue Maßnahmendomäne aus und klicken Sie auf Sichern.

Die Datenaufbewahrung für den Client, den Sie der Maßnahmendomäne zuordnen, wird jetzt durch diese Maßnahme gesteuert. Wenn Sie beispielsweise das Beispiel in Schritt 6 implementiert haben, werden inaktive Sicherungsversionen für die Clients standardmäßig 30 Tage lang aufbewahrt.

Voraussetzung: Wenn ein Client bei der Zuordnung zu einer neuen Domäne aktiv ist, müssen Sie den Client stoppen und erneut starten, damit die Änderung wirksam wird.

#### Zugehörige Tasks:

Clientoperationen über Clientoptionsgruppen steuern

## Maßnahmendomäne erstellen

---

Möglicherweise möchten Sie für jeden Typ von Client, der vom Server geschützt wird, eine neue Maßnahmendomäne erstellen.

Möglicherweise möchten Sie auch die Zuständigkeit für Clients auf mehrere Administratoren verteilen, indem Sie Ihnen Berechtigung für bestimmte Maßnahmendomänen erteilen.

### Informationen zu diesem Vorgang

---


Die Erstellung einer neuen Maßnahmendomäne kann unter den folgenden Umständen hilfreich sein:

- Anwendungen, Systeme oder virtuelle Maschinen erfordern unterschiedliche Datenaufbewahrungseinstellungen. Für jeden Clienttyp können Sie eine Maßnahmendomäne mit einer für diesen Typ geeigneten Standardmaßnahme erstellen.
- Administratoren sind für unterschiedliche Gruppen von Clients verantwortlich. Für jeden Administrator können Sie eine Maßnahmendomäne erstellen, der Sie die Clients zuordnen, die von diesem Administrator verwaltet werden sollen.

### Vorgehensweise

---

Die folgenden Schritte sind eine Zusammenfassung der Vorgehensweise beim Erstellen einer Maßnahmendomäne.

1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.
2. Definieren Sie eine Maßnahme mit dem Befehl DEFINE DOMAIN.
3. Definieren Sie eine Maßnahmengruppe für die Domäne mit dem Befehl DEFINE POLICYSET.



4. Klicken Sie auf der Seite Übersicht im Operations Center auf das Menü Services.
5. Wählen Sie die Maßnahmendomäne aus und klicken Sie auf Details. Klicken Sie auf Maßnahmengruppen.
6. Klicken Sie auf die Umschaltfläche Konfigurieren, um die Einstellungen aktualisieren zu können.
7. Klicken Sie auf +Verwaltungsklasse, um eine Verwaltungsklasse hinzuzufügen. Geben Sie Auswahlangaben für Basiseinstellungen an und klicken Sie auf Hinzufügen.
8. Optional: Passen Sie weitere Einstellungen in der neuen Verwaltungsklasse an:
  - a. Geben Sie für Sicherungsservices Auswahlangaben in den folgenden Spalten an: Sicherungsziel, Sicherungen, Zusätzliche Sicherungen aufbewahren, Gelöschte Sicherungen und Gelöschte Sicherungen aufbewahren.
  - b. Geben Sie für Archivierungsservices Auswahlangaben in den Spalten Archivierungsziel und Archivierungen aufbewahren an.
  - c. Klicken Sie auf Sichern.
9. Optional: Klicken Sie auf +Verwaltungsklasse, um weitere Verwaltungsklassen hinzuzufügen.
10. Stellen Sie sicher, dass in der Spalte 'Standard' eine Standardverwaltungsklasse ausgewählt ist.
11. Aktivieren Sie die Maßnahmengruppe, indem Sie auf Aktivieren klicken.
12. Ordnen Sie der neuen Maßnahmendomäne Clients zu. Klicken Sie in der Menüleiste des Operations Center auf Clients.
  - o Um der Maßnahmendomäne neue Clients hinzuzufügen, klicken Sie auf +Client.
  - o Um einen vorhandenen Client in die Maßnahmendomäne zu versetzen, wählen Sie den Client aus, klicken Sie auf Details und klicken Sie dann auf die Registerkarte Merkmale. Wählen Sie die neue Maßnahmendomäne aus und klicken Sie auf Sichern.

**Zugehörige Verweise:**

DEFINE DOMAIN (Neue Maßnahmendomäne definieren)

DEFINE POLICYSET (Maßnahmengruppe definieren)

## Clientoperationen über Clientoptionsgruppen steuern

---

Mithilfe von Clientoptionsgruppen können Sie die Verarbeitungsoptionen, die Clients für Operationen wie Sicherungen verwenden, zentral steuern. Mithilfe von Clientoptionsgruppen kann sichergestellt werden, dass Daten konsistent gemäß Ihren Anforderungen geschützt werden. Eine Clientoptionsgruppe kann Optionen in einer lokalen Clientoptionsdatei überschreiben oder Optionen hinzufügen, die unter Umständen nicht in der lokalen Clientoptionsdatei vorhanden sind.

### Informationen zu diesem Vorgang

---

Indem Clientoptionsgruppen erstellt und zugeordnet werden, müssen Sie die lokale Clientoptionsdatei weniger häufig aktualisieren und der Aufwand für Sie bzw. Ihre Benutzer wird geringer.

Sie können beispielsweise eine Clientoptionsgruppe definieren, um eine Einschluss-/Ausschlussliste anzugeben, in der festgelegt ist, welche Daten gesichert werden, welche Daten von der Sicherung ausgeschlossen sind und welche Verwaltungsklassen zur Verwaltung der Datenaufbewahrung verwendet werden. Andere Clientoptionen, die gegebenenfalls für die zentrale Steuerung in einer Clientoptionsgruppe hilfreich sind, sind die Optionen compression und deduplication.

Sie können Clientoptionsgruppen für Clients mit ähnlichen Anforderungen erstellen, wie beispielsweise Clients unter demselben Betriebssystem, Clients, die dieselbe Software verwenden, oder Clients, die von einer bestimmten Abteilung verwendet werden. Sie können beispielsweise Clientoptionsgruppen für Windows-Workstations oder für die Lohnbuchhaltung erstellen. Nachdem die Clientoptionsgruppe erstellt wurde, ordnen Sie die Clientoptionsgruppe allen Clients desselben Typs zu.

In einer Clientoptionsgruppe auf dem Server können nicht alle Clientoptionen angegeben werden. Informationen dazu, welche Clientoptionen zentral in einer Clientoptionsgruppe gesteuert werden können, finden Sie in Clientoptionen, die vom Server definiert werden können.

### Vorgehensweise

---

1. Definieren Sie eine Clientoptionsgruppe mit dem Befehl DEFINE CLOPTSET. Um beispielsweise eine Clientoptionsgruppe mit dem Namen PAYROLLBACKUP zu definieren, geben Sie den folgenden Befehl aus:

```
define cloptset payrollbackup description='Sicherungsoptionen für die Lohnbuchhaltung'
```

2. Fügen Sie der Clientoptionsgruppe mit dem Befehl DEFINE CLIENTOPT Clientoptionen hinzu. Angenommen, die Optionen include und exclude sollen der Clientoptionsgruppe mit dem Namen PAYROLLBACKUP hinzugefügt werden, um die folgenden Ziele zu erreichen:
  - o Temporäre Internetverzeichnisdateien von Sicherungsoperationen ausschließen
  - o Alle Dateien im Verzeichnis C:\Data und die zugehörigen Unterverzeichnisse in eine Sicherung einschließen und die Dateien für die Datenaufbewahrung der Verwaltungsklasse PAYCLASS zuordnen

Geben Sie die folgenden Befehle aus:

```
define clienopt payrollbackup inclexcl "exclude.dir '*:\..\Temporäre Internet-Dateien'"
define clienopt payrollbackup inclexcl "include C:\Data\..\* payclass"
```

3. Um einem Client eine Clientoptionsgruppe zuzuordnen, führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients.
  - b. Wählen Sie einen Client aus und klicken Sie auf Details.
  - c. Klicken Sie auf Merkmale.
  - d. Wählen Sie im Bereich 'Allgemein' eine Optionsgruppe aus und klicken Sie auf Sichern.

#### Zugehörige Verweise:

DEFINE CLOPTSET (Clientoptionsgruppennamen definieren)

DEFINE CLIENOPT (Option für eine Optionsgruppe definieren)

🔗 Clientoption 'compression'

🔗 Clientoption 'deduplication'

## Speicher konfigurieren

---

Wählen Sie abhängig von der erforderlichen Speicherfunktionalität den korrekten Typ von Speichermedien aus. Optimieren und steuern Sie Ihre Speicherpools für verschiedene Typen von Daten.

- **Speicherpooltypen**  
Um den Speicherpooltyp bestimmen zu können, der Ihre Speichieranforderungen am besten erfüllt, sollten Sie die Merkmale jedes Speicherpooltyps bewerten.
- **Dateneduplizierungsoptionen**  
Verwenden Sie die Inline-Dateneduplizierung, um Daten gleichzeitig zu deduplizieren und in einen Containerspeicherpool zu schreiben. Verwenden Sie die nachgeordnete Dateneduplizierung, um doppelte Daten aus Speicherpools mit sequenziellem Zugriff (FILE) zu löschen.
- **Speichereinheiten konfigurieren**  
Konfigurieren Sie Speichereinheiten, indem Sie Einheiten anschließen, Einheitentreiber konfigurieren und die Objekte erstellen, die die Einheiten für den Server darstellen.
- **Verzeichniscontainerspeicherpool für die Datenspeicherung konfigurieren**  
Sie können Verzeichniscontainerspeicherpools für die Verwendung der Inline-Dateneduplizierung zum Speichern deduplizierter Daten konfigurieren.
- **Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren**  
Sie können deduplizierte Daten und nicht deduplizierte Daten in einem Cloud-Containerspeicherpool speichern und die Daten nach Bedarf zurückschreiben. Sie können Cloud-Containerspeicherpools für die Verwendung einer der folgenden Service-Provider und Protokolle konfigurieren: Amazon Web Services (AWS) mit Simple Storage Service (S3), IBM® Cloud Object Storage mit Swift oder S3 (und IBM SoftLayer), Microsoft Azure und OpenStack mit Swift unter Verwendung von Keystone Version 1 oder Version 2. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.
- **Speicherregel für Cloud-Tiering definieren**  
Sie können eine Speicherregel für die Implementierung von Cloud-Tiering definieren, mit dem Daten aus einem Verzeichniscontainerspeicherpool auf Platte in einen Cloud-Containerspeicherpool versetzt werden. Mithilfe der Speicherregel wird das Cloud-Tiering aus Verzeichniscontainerspeicherpools in Cloud-Containerspeicherpools geplant.
- **Leistung für Cloudobjektspeicher optimieren**  
Sie können IBM Spectrum Protect so konfigurieren, dass Daten während der Datenaufnahme vorübergehend in einem oder mehreren lokalen Speicherpoolverzeichnissen gespeichert werden. Die Daten werden dann aus dem lokalen Speicher in die Cloud übertragen. Auf diese Art und Weise können Sie die Datensicherungs- und -archivierungsleistung verbessern.
- **Speicherbereich in Containerspeicherpools verwalten**  
Nachdem Sie IBM Spectrum Protect konfiguriert und Speicherbereich hinzugefügt haben, müssen Sie Ihre Daten und Ihren Speicherbereich im Speicherpool effektiv verwalten, um die ordnungsgemäße Funktion zu gewährleisten. Maximieren Sie Ihren Speicherbereich und die Serverleistung mithilfe von Containerspeicherpools.
- **Speicherpoolcontainer prüfen**  
Mit der Prüfung eines Speicherpoolcontainers wird auf Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Speicherpool geprüft.
- **Speichersystemvoraussetzungen und Reduzierung des Risikos fehlerhafter Daten**  
Für den IBM Spectrum Protect-Server können viele Typen von Speicher verwendet werden. Wenn Sie Plattenblockspeicher, Solid-State-Laufwerke (SSDs) oder an das Netz angeschlossene Dateisysteme als Serverspeicher verwenden, müssen Sie sicherstellen, dass der Speicher die Voraussetzungen erfüllt.

## Speicherpooltypen

---

Um den Speicherpooltyp bestimmen zu können, der Ihre Speichieranforderungen am besten erfüllt, sollten Sie die Merkmale jedes Speicherpooltyps bewerten.

Bewerten Sie jeden Speicherpooltyp mithilfe der folgenden Tabelle.

| Speicherpooltyp                        | Beschreibung  | Verwendungen  |
|--|---|---|
| Verzeichniscontainerspeicherpool       | Ein primärer Speicherpool, der von einem Server zum Speichern von Daten verwendet wird. Daten, die in Verzeichniscontainerspeicherpools gespeichert werden, verwenden entweder die Inline-Datendeduplizierung oder die clientseitige Datendeduplizierung. Mithilfe von Cloud-Tiering können Daten aus Verzeichniscontainerspeicherpools in Cloud-Containerspeicherpools versetzt werden.  | Verwenden Sie diesen Speicherpooltyp bei der Inline-Datendeduplizierung. Durch die Verwendung von Verzeichniscontainerspeicherpools entfällt die Notwendigkeit zur Datenträgerkonsolidierung, wodurch die Serverleistung verbessert und die Kosten der Speicherhardware gesenkt werden.<br><br>Sie können diesen Speicherpooltyp nicht für Speicherpoolsicherungs-, Umlagerungs-, Konsolidierungs-, Import- oder Exportoperationen verwenden. |
| Cloud-Containerspeicherpool            | Ein primärer Speicherpool, der von einem Server zum Speichern von Daten verwendet wird. Verwenden Sie Cloud-Containerspeicherpools, um Daten in einem objektspeicherbasierten Cloudspeicherprovider zu speichern. Daten, die in Cloud-Containerspeicherpools gespeichert werden, verwenden entweder die Inline-Datendeduplizierung oder die clientseitige Datendeduplizierung.  | Das Speichern von Daten in Cloud-Containerspeicherpools ermöglicht es Ihnen, die von Clouds gebotenen Vorteile der Kosten pro Einheit zusammen mit der vom Cloudspeicher bereitgestellten Skalierungsfunktionalität zu nutzen.<br><br>Sie können diesen Speicherpooltyp nicht für Speicherpoolsicherungs-, Umlagerungs-, Konsolidierungs-, Import- oder Exportoperationen verwenden.  |
| Speicherpool mit wahlfreiem Zugriff    | Eine Gruppe von Datenträgern, die der Server zum Speichern von Sicherungsversionen von Dateien, Dateien, die Archivierungskopien sind, und Dateien, die umgelagert werden, verwendet. Dateien werden auf DISK-Einheiten gespeichert.  | Verwenden Sie diesen Speicherpooltyp, um eine Kopie Ihrer Daten auf DISK-Einheiten aufzubewahren. Sie können Daten aus den folgenden Typen von Speicherpools in diesen Speicherpool oder aus diesem Speicherpool umlagern: <ul style="list-style-type: none"> <li>• Speicherpools mit wahlfreiem Zugriff</li> <li>• Speicherpools mit sequenziellem Zugriff</li> </ul>  |
| Speicherpool mit sequenziellem Zugriff | Eine Gruppe von Datenträgern, die der Server zum Speichern von Sicherungsversionen von Dateien, Dateien, die Archivierungskopien sind, und Dateien, die aus Clientknoten umgelagert werden, verwendet. Dateien werden auf Band- oder FILE-Einheiten gespeichert. Daten, die in Speicherpools mit sequenziellem Zugriff gespeichert werden, verwenden sowohl die nachgeordnete Datendeduplizierung als auch die clientseitige Datendeduplizierung. Einschränkung: Die nachgeordnete Datendeduplizierung ist nur in Version 7.1.2 und früheren Versionen verfügbar. | Verwenden Sie diesen Speicherpooltyp, um eine Kopie Ihrer Daten auf FILE- und TAPE-Einheiten aufzubewahren. Sie können Daten in diesen Typ von Speicherpool umlagern.   |
| Kopierspeicherpool                     | Eine benannte Gruppe von Datenträgern, die Kopien von Dateien enthalten, die in primären Speicherpools gespeichert sind. Kopierspeicherpools werden nur zum Sichern der Daten verwendet, die in primären Speicherpools gespeichert sind. Ein Kopierspeicherpool kann nicht als Ziel für eine Sicherungskopiengruppe, eine Archivierungskopiengruppe oder eine Verwaltungsklasse (für speicher verwaltete Dateien) verwendet werden.   | Verwenden Sie Kopierspeicherpools, um über eine Kopie der aktiven und inaktiven Daten zu verfügen, die nach einem Katastrophenfall oder einem Ausfall in einen primären Speicherpool zurückgeschrieben werden kann.<br><br>Sie können keine Inline-Datendeduplizierung, Komprimierung, Replikation oder Datendeduplizierung mit diesem Typ von Speicherpool verwenden.  |

| Speicherpooltyp               | Beschreibung  | Verwendungen  |
|-------------------------------|---|---|
| Containerkopienspeicherpool   | <p>Eine Gruppe von Banddatenträgern, die eine Kopie der deduplizierten Speicherbereiche enthalten, die in einem Verzeichniscontainerspeicherpool gespeichert sind.</p> <p>Containerkopienspeicherpools werden nur zum Schützen der Daten verwendet, die in Verzeichniscontainerspeicherpools gespeichert sind.</p> <p>Containerkopienspeicherpools werden zum Reparieren einer Beschädigung in einem Verzeichniscontainerspeicherpool oder zum Zurückschreiben eines Verzeichniscontainerspeicherpools verwendet, wenn ein Katastrophenfall eintritt. Containerkopienspeicherpools sind auf sequenziellen Datenträgern gespeichert.</p> | <p>Verwenden Sie Containerkopienspeicherpools, um Kopien von Verzeichniscontainerspeicherpools vor Ort oder an einem anderen Standort aufzubewahren. Beschädigte Daten in Verzeichniscontainerspeicherpools können mithilfe der deduplizierten Speicherbereiche in einem Containerkopienspeicherpool repariert werden.</p>  |
| Speicherpool für aktive Daten | <p>Eine benannte Gruppe von Speicherpooldatenträgern, die nur aktive Versionen von Clientsicherungsdaten enthalten.</p>   | <p>Verwenden Sie Speicherpools für aktive Daten, um nach einem Katastrophenfall oder Ausfall nur aktive Daten in primäre Speicherpools zurückzuschreiben. Wenn nur aktive Daten zurückgeschrieben werden, können Sie Clientdaten schneller zurückschreiben und verwenden weniger Bandbreite.</p> <p>Sie können keine Inline-Dateneduplizierung, Komprimierung, Replikation oder Dateneduplizierung mit diesem Typ von Speicherpool verwenden.</p> |

Vergleichen Sie anhand der folgenden Tabelle die Speicherpoolfunktionalität und wählen Sie abhängig von Ihren Speicheranforderungen den Speicherpool aus, der Ihre Geschäftsanforderungen am besten erfüllt.

| Benutzerziel  | Verzeichniscontainerspeicherpool | Cloud-Containerspeicherpool | Speicherpool mit wahlfreiem Zugriff | Speicherpool mit sequenziellem Zugriff | Kopienspeicherpool | Containerkopienspeicherpool | Speicherpool für aktive Daten |
|---|----------------------------------|-----------------------------|-------------------------------------|--|--------------------|-----------------------------|-------------------------------|
| Schützen von Speicherpooldaten mithilfe der Knotenreplikation         | ✓                                |                             | ✓                                   | ✓                                      | ✓                  |                             | ✓                             |
| Reduzieren des Speicherbedarfs mithilfe der Inline-Komprimierung      | ✓                                | ✓                           |                                     |  |                    |                             |                               |
| Reduzieren des Speicherbedarfs mithilfe der Inline-Dateneduplizierung | ✓                                | ✓                           |                                     |  |                    |                             |                               |

| Benutzerziel  | Verzeichniscontainerspeicherpool | Cloud-Containerspeicherpool | Speicherpool mit wahlfreiem Zugriff | Speicherpool mit sequenziellem Zugriff | Kopierspeicherpool | Containerkopierspeicherpool | Speicherpool für aktive Daten |
|---|----------------------------------|-----------------------------|-------------------------------------|--|--------------------|-----------------------------|-------------------------------|
| Reduzieren des Speicherbedarfs mithilfe der clientseitigen Datendeduplizierung  | ✓                                | ✓                           |                                     | ✓                                      |                    |                             |                               |
| Reduzieren des Speicherbedarfs mithilfe der nachgeordneten Datendeduplizierung  |                                  |                             |                                     | ✓                                      |                    |                             |                               |
| Schützen von Speicherpooldaten mithilfe von Speicherpoolschutz  | ✓                                |                             |                                     |  |                    | ✓                           |                               |
| Sichern von Speicherpooldaten mithilfe von Kopierspeicherpools auf Platte oder Band   |                                  |                             | ✓                                   | ✓                                      |                    |                             |                               |
| Speichern von Daten in einer Cloud  |                                  | ✓                           |                                     |  |                    |                             |                               |
| Verwenden Sie Cloud-Tiering, um Daten aus einem Verzeichniscontainerspeicherpool in einen Cloud-Containerspeicherpool zu versetzen. | ✓                                |                             |                                     |  |                    |                             |                               |

## Datendeduplizierungsoptionen

Verwenden Sie die Inline-Datendeduplizierung, um Daten gleichzeitig zu deduplizieren und in einen Containerspeicherpool zu schreiben. Verwenden Sie die nachgeordnete Datendeduplizierung, um doppelte Daten aus Speicherpools mit sequenziellem Zugriff (FILE) zu löschen.

Für die Inline-Datendeduplizierung müssen Verzeichniscontainerspeicherpools oder Cloud-Containerspeicherpools verwendet werden. Durch die Verwendung von Verzeichniscontainer- oder Cloud-Containerspeicherpools verringert sich die Notwendigkeit zur Offlinereorganisation, wodurch die Serverleistung verbessert wird und die Kosten der Speicherhardware gesenkt werden. Mit diesen Speicherpooltypen dürfen keine Einheitenklassen oder Datenträger verwendet werden.

Bei der nachgeordneten Datendeduplizierung identifiziert der Server zunächst die Daten und entfernt dann die doppelten Daten aus dem Speicherpool. Es wird nur eine einzige Instanz der Daten auf Speichermedien aufbewahrt. Andere Instanzen derselben Daten werden durch einen Zeiger auf die aufbewahrte Instanz ersetzt. Wenn Sie die doppelten Daten entfernen, können Sie Speicherbereich in dem Speicherpool konsolidieren.

Weitere Informationen zur nachgeordneten Datendeduplizierung finden Sie in Daten deduplizieren (Version 7.1.1).

Bei der clientseitigen Datendeduplizierung werden nur komprimierte, deduplizierte Daten an den Server gesendet. Die Verarbeitung während eines Sicherungsprozesses wird auf den Server und den Client verteilt.

Die folgende Tabelle enthält einen Vergleich der Datendeduplizierungsoptionen.

| Typ der Datendeduplizierung   | Vorteile  | Nachteile  |
|---|---|--|
| Nachgeordnet<br>Einschränkung: Sie können die nachgeordnete Datendeduplizierung nur für Speicherpools mit sequenziellem Zugriff (FILE) verwenden. | <ul style="list-style-type: none"> <li>Nach der Datendeduplizierung können Sie den Speicherpool konsolidieren.</li> </ul>   | <ul style="list-style-type: none"> <li>Längere Verarbeitungszeiten, da die Daten zunächst identifiziert werden müssen, bevor die doppelten Daten aus dem Speicherpool entfernt werden.</li> </ul>  |
| Inline<br>Einschränkung: Sie können die Inline-Datendeduplizierung nur für Verzeichniscontainer- und Cloud-Containerspeicherpools verwenden.      | <ul style="list-style-type: none"> <li>Dedupliziert Daten, wenn die Daten in einen Containerspeicherpool geschrieben werden.</li> <li>Verringert die Notwendigkeit zur Offlinereorganisation, wodurch die Serverleistung verbessert wird.</li> <li>Geringere Kosten für Speicherhardware</li> </ul> | <ul style="list-style-type: none"> <li>Höhere Prozessorauslastung durch den Server</li> </ul>  |
| Clientseite   | <ul style="list-style-type: none"> <li>Die Verarbeitung während eines Sicherungsprozesses wird auf den Server und den Client verteilt.</li> </ul>   | <ul style="list-style-type: none"> <li>Höhere Prozessorauslastung durch den Client</li> <li>Längere abgelaufene Zeit für Clientoperationen, wie beispielsweise Sicherungen</li> <li>Nur komprimierte, deduplizierte Daten werden an den Server gesendet</li> </ul> |

**Zugehörige Tasks:**




- Datendeduplizierung konfigurieren (Plattenspeicherlösung für mehrere Standorte)
- Datendeduplizierung konfigurieren (Plattenspeicherlösung für einen einzelnen Standort)
- Speicherpools vergleichen

## Speichereinheiten konfigurieren

Konfigurieren Sie Speichereinheiten, indem Sie Einheiten anschließen, Einheitentreiber konfigurieren und die Objekte erstellen, die die Einheiten für den Server darstellen.

### Informationen zu diesem Vorgang

Wenn Sie nicht die Plattenspeicherlösung für einen einzelnen Standort oder die Plattenspeicherlösung für mehrere Standorte verwenden, konfigurieren und verwalten Sie Speichereinheiten anhand der Anweisungen in der Dokumentation zu Version 7.1.1:

-  AIX-Betriebssysteme  Linux-Betriebssysteme Speichereinheiten konfigurieren und verwalten
-  Windows-Betriebssysteme Speichereinheiten konfigurieren und verwalten

## Verzeichniscontainerspeicherpool für die Datenspeicherung konfigurieren

Sie können Verzeichniscontainerspeicherpools für die Verwendung der Inline-Datendeduplizierung zum Speichern deduplizierter Daten konfigurieren.

### Vorgehensweise

Um Daten in einem Verzeichniscontainerspeicherpool zu speichern, führen Sie die folgenden Schritte aus:


- Erstellen Sie einen Verzeichniscontainerspeicherpool, indem Sie die folgenden Schritte ausführen:
  - Klicken Sie in der Menüleiste des Operations Center auf Speicher > Speicherpools.
  - Klicken Sie auf der Seite Speicherpools auf + Speicherpool.

- c. Führen Sie die Schritte im Assistenten Speicherpool hinzufügen aus. Wählen Sie Verzeichnis als Typ des containerbasierten Speichers aus.
2. Aktualisieren Sie, nachdem der Speicherpool vom Assistenten erstellt wurde, Ihre Verwaltungsklassen und Maßnahmengruppen für die Verwendung des neuen Pools. Um eine Verwaltungsklasse für die Verwendung des neuen Pools zu aktualisieren, führen Sie die folgenden Schritte aus:
  - a. Klicken Sie in der Menüleiste des Operations Center auf Services.
  - b. Wählen Sie auf der Seite Maßnahmen eine Maßnahmendomäne aus und klicken Sie auf Details.
  - c. Klicken Sie auf der Seite Details auf die Registerkarte Maßnahmengruppen.
  - d. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppen sind editierbar.
  - e. Optional: Um eine Maßnahmengruppe zu editieren, die nicht aktiv ist, klicken Sie auf die vorwärts und rückwärts gerichteten Pfeile, um die Maßnahmengruppe zu lokalisieren.
  - f. Aktualisieren Sie eine oder mehrere Verwaltungsklassen für die Verwendung des neuen Pools, indem Sie das Feld Sicherungsziel der Tabelle editieren.
  - g. Klicken Sie auf Sichern.
3. Aktivieren Sie die geänderte Maßnahmengruppe, indem Sie die folgenden Schritte ausführen:
  - a. Klicken Sie auf Aktivieren. Da das Ändern der aktiven Maßnahmengruppe unter Umständen einen Datenverlust zur Folge haben kann, wird eine Zusammenfassung der Unterschiede zwischen der aktiven Maßnahmengruppe und der neuen Maßnahmengruppe angezeigt.
  - b. Studieren Sie die Unterschiede zwischen entsprechenden Verwaltungsklassen in den beiden Maßnahmengruppen und wägen Sie die Auswirkungen auf Clientdateien ab. Clientdateien, die an Verwaltungsklassen in der derzeit aktiven Maßnahmengruppe gebunden sind, werden nach der Aktivierung in der neuen Maßnahmengruppe an die Verwaltungsklassen mit denselben Namen gebunden.
  - c. Ermitteln Sie Verwaltungsklassen in der derzeit aktiven Maßnahmengruppe, die in der neuen Maßnahmengruppe keine Entsprechung haben, und wägen Sie die Auswirkungen auf Clientdateien ab. Clientdateien, die an diese Verwaltungsklassen gebunden sind, werden nach der Aktivierung von der Standardverwaltungsklasse in der neuen Maßnahmengruppe verwaltet.
  - d. Wenn die Änderungen, die durch die Maßnahmengruppe implementiert werden, akzeptabel sind, wählen Sie das Kontrollkästchen Ich weiß, dass diese Aktualisierungen zu einem Datenverlust führen können aus und klicken Sie auf Aktivieren.
4. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppen sind nicht mehr editierbar.

## Nächste Schritte

---

Um einen Verzeichniscontainerspeicherpool zu schützen, geben Sie den Befehl PROTECT STGPOOL aus. Anweisungen finden Sie in PROTECT STGPOOL (Daten schützen, die zu einem Speicherpool gehören) und Verzeichniscontainerspeicherpools auf Band kopieren.

 Linux-Betriebssysteme Wenn Sie einen Verzeichniscontainerspeicherpool schützen, indem Sie die Daten auf einen fernen Server kopieren, und Netzprobleme auftreten, lesen Sie in Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann nach.

- Verzeichniscontainerspeicherpools auf Band kopieren  
Sie können Daten in einem Verzeichniscontainerspeicherpool schützen, indem Sie die Daten in Containerkopierspeicherpools kopieren, die durch Banddatenträger dargestellt werden. Die Bandkopie wird zur Reparatur von Beschädigungen an einem Verzeichniscontainerspeicherpool verwendet.
- Banddatenträger ohne Konfiguration von DRM im Rotationsprinzip auslagern  
Wenn Ihre Speicherlösung Containerkopierspeicherpools umfasst, die durch Banddatenträger dargestellt werden, die Funktion 'Disaster Recovery Manager' (DRM) jedoch nicht konfiguriert wurde, können Sie eine manuelle Prozedur verwenden, um die Banddatenträger im Rotationsprinzip auszulagern. Indem Sie Kopien von Daten in ausgelagerten Banddatenträgern aufbewahren, können Sie die Daten in einem Katastrophenfall zurückschreiben.
- Schwellenwert für Datenträgerkonsolidierung für Containerkopierspeicherpools ändern  
Standardmäßig ist die Konsolidierung von Banddatenträgern für Containerkopierspeicherpools aktiviert. Um sicherzustellen, dass Banddatenträger effizient verwendet werden, können Sie den Schwellenwert für Datenträgerkonsolidierung ändern.
- Banddatenträger in Containerkopierspeicherpools konsolidieren  
Sie können Banddatenträger in Containerkopierspeicherpools konsolidieren, ohne eine Schutzoperation auszuführen, wenn nicht ausreichend Zeit zur Verfügung steht, um sowohl Schutz- als auch Konsolidierungsoperationen zu ermöglichen.
- Bestimmen, ob Containerkopierspeicherpools für den Schutz vor Katastrophen verwendet werden können  
Bestimmen, ob Containerkopierspeicherpools Ihre Anforderungen für den Schutz vor Katastrophen erfüllen

## Verzeichniscontainerspeicherpools auf Band kopieren

---

Sie können Daten in einem Verzeichniscontainerspeicherpool schützen, indem Sie die Daten in Containerkopierspeicherpools kopieren, die durch Banddatenträger dargestellt werden. Die Bandkopie wird zur Reparatur von Beschädigungen an einem Verzeichniscontainerspeicherpool verwendet.

## Vorbereitende Schritte

---

Definieren Sie mit dem Befehl `DEFINE LIBRARY` mindestens ein Bandarchiv für den Server. Stellen Sie genügend Bandlaufwerke und Arbeitsdatenträger zur Erfüllung Ihrer Speicheranforderungen bereit. Weitere Informationen zur Verwaltung von Sicherungsdatenträgern und zur Konfiguration von Disaster Recovery Manager (DRM) finden Sie in Disaster Recovery Manager (Version 7.1.1).

## Informationen zu diesem Vorgang

---

Um die Daten in Verzeichniscontainerspeicherpools auf Band zu kopieren, wird vom Operations Center ein Zeitplan zur Ausführung des Befehls `PROTECT STGPOOL` erstellt. Wenn der Zeitplan für den Schutz ausgeführt wird, wird eine einzelne Bandkopie erstellt. Wenn der Zeitplan für den Schutz ausgeführt wird, muss mindestens ein Datenträger verfügbar sein. Andernfalls schlägt die Operation fehl.

Sie können bis zu zwei Bandkopien erstellen, Sie müssen jedoch die Befehlszeilenschnittstelle verwenden, um einen zweiten Containerkopierspeicherpool zu erstellen. Eine Bandkopie kann an einen anderen Standort zur Wiederherstellung nach einem Katastrophenfall transportiert werden. Die andere Kopie kann vor Ort aufbewahrt werden, um eine schnelle Wiederherstellung bei weniger kritischen Fehlern zu ermöglichen.

Einschränkungen:

- Virtuelle Bandarchive werden, unabhängig davon, welcher Speicherarchivtyp definiert wird, nicht unterstützt. Es wird nur physisches Band unterstützt.
- Containerkopierspeicherpools können zum Reparieren geringfügiger bis moderater Beschädigungen an Speicherpools, einschließlich beschädigter Container oder Verzeichnisse, verwendet werden. Containerkopierspeicherpools können auch zum Schutz vor Katastrophen verwendet werden; Sie müssen jedoch sicherstellen, dass die Wiederherstellungszeiten Ihre Anforderungen erfüllen. Weitere Informationen finden Sie in Bestimmen, ob Containerkopierspeicherpools für den Schutz vor Katastrophen verwendet werden können.
- Die Replikation kann nicht für einen Containerkopierspeicherpool als Ziel verwendet werden.  
Tipp: Sie können eine Bandkopie der Daten im Verzeichniscontainerspeicherpool am Standort für die Wiederherstellung nach einem Katastrophenfall erstellen, indem Sie mithilfe dieser Prozedur einen Containerkopierspeicherpool auf dem Zielreplikationsserver erstellen. Planen Sie dann die Ausführung der Befehle `PROTECT STGPOOL` und `REPLICATE NODE` auf dem Quellenreplikationsserver, um Ihre Daten auf dem Zielreplikationsserver zu schützen.
- Die folgende Prozedur kann nicht verwendet werden, wenn dem Verzeichniscontainerspeicherpool bereits ein Containerkopierspeicherpool zugeordnet wurde. Um einen zweiten Containerkopierspeicherpool zu erstellen, führen Sie die Anweisungen in Schritt 5 aus.

Wenn Sie einen Containerkopierspeicherpool im Rahmen des Assistenten Speicherpool hinzufügen erstellt hatten, müssen Sie diese Prozedur nicht verwenden. Bei der Ausführung des Assistenten wurden vom Operations Center der Containerkopierspeicherpool und ein Zeitplan für den Schutz konfiguriert.

## Vorgehensweise

---

Um Speicherpoolschutz für das Kopieren auf Band für einen vorhandenen Verzeichniscontainerspeicherpool zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Menüleiste des Operations Center auf Speicher > Speicherpools.
2. Wählen Sie auf der Seite Speicherpools den Verzeichniscontainerspeicherpool aus, der auf Band geschützt werden soll.
3. Klicken Sie auf Weitere > Containerkopienpool hinzufügen.
4. Führen Sie die Anweisungen im Fenster Containerkopienpool hinzufügen aus, um den Schutz für das Kopieren auf Band zu planen.
5. Nachdem Sie die vorherigen Schritte ausgeführt haben, können Sie mithilfe der Befehlszeilenschnittstelle einen zweiten Containerkopierspeicherpool hinzufügen. Führen Sie wahlweise die folgenden Schritte aus, um einen Containerkopierspeicherpool hinzuzufügen:
  - a. Erstellen Sie einen Containerkopierspeicherpool, indem Sie den Befehl `DEFINE STGPOOL` ausgeben.
  - b. Ordnen Sie den Containerkopierspeicherpool dem Verzeichniscontainerspeicherpool zu, indem Sie den Befehl `UPDATE STGPOOL` für den Verzeichniscontainerspeicherpool ausgeben.

## Ergebnisse

---

Nachdem die Konfiguration abgeschlossen ist, werden die Daten in dem Verzeichniscontainerspeicherpool abhängig von dem definierten Zeitplan für den Schutz in einen Containerkopierspeicherpool kopiert.

## Nächste Schritte

---

1. Wenn Sie eine Bandkopie für die Aufbewahrung an einem anderen Standort erstellt hatten, aktivieren Sie den Containerkopierspeicherpool an dem anderen Standort für DRM-Operationen, indem Sie den Befehl `SET DRMCOPYCONTAINERSTGPOOL` ausgeben. Stellen Sie sicher, dass die Banddatenträger Ihren Zeitplänen für die Rotation



ausgelagerter Bänder hinzugefügt werden. Wenn DRM nicht konfiguriert ist, müssen Sie DRM konfigurieren oder eine Alternativmethode für die Auslagerung von Bändern im Rotationsprinzip verwenden. Anweisungen zu der Alternativmethode finden Sie in Banddatenträger ohne Konfiguration von DRM im Rotationsprinzip auslagern. Überprüfen Sie mithilfe des Befehls `QUERY DRMSTATUS`, ob Containerkopierspeicherpools an einem anderen Standort für DRM aktiviert sind.

Anweisungen zur Konfiguration von DRM finden Sie in Disaster Recovery Manager (Version 7.1.1).

2. Bestätigen Sie, dass der Schwellenwert für Konsolidierung für Ihren Containerkopierspeicherpool Ihre Anforderungen erfüllt.

Standardmäßig ist die Konsolidierung von Banddatenträgern für neue Containerkopierspeicherpools, die mit dem Operations Center erstellt werden, aktiviert. Eine Datenträgerkonsolidierung erfolgt, wenn der Schwellenwert für Konsolidierung für den Containerkopierspeicherpool unter 100 % liegt. Banddatenträger sind jedoch kein Kandidat für die Konsolidierung, bevor sie nicht zu 75 % gefüllt sind. Gehen Sie mit Vorsicht vor, wenn Sie die Konsolidierung mit Containerkopierspeicherpools verwenden, die über Datenträger an einem anderen Standort verfügen. Wenn ein Datenträger an einem anderen Standort für die Konsolidierung auswählbar wird, werden die Bereiche auf dem Datenträger vom Server an den Standort vor Ort zurückversetzt. Wenn vor Ort ein Katastrophenfall eintritt, kann der Server Bereiche von dem Datenträger an einem anderen Standort anfordern, wenn die zurückgeschriebene Datenbank auf Bereiche auf dem Datenträger an dem anderen Standort verweist. Um zu verhindern, dass Datenträger unmittelbar nach dem Löschen aller Bereiche erneut beschrieben werden, verwenden Sie den Parameter `REUSEDDELAY`, um einen Wert größer als 0 anzugeben. Der Schwellenwert für Konsolidierung wird für Containerkopierspeicherpools vor Ort vom Operations Center auf 60 % gesetzt.

Anweisungen zum Ändern des Schwellenwerts für Konsolidierung finden Sie in Schwellenwert für Datenträgerkonsolidierung für Containerkopierspeicherpools ändern.

3. Schützen Sie die Metadaten für Ihren Containerkopierspeicherpool.

Wenn der Zeitplan für den Schutz ausgeführt wird, werden Datenbereiche in Containerkopierspeicherpools ohne die zugehörigen Metadaten auf Banddatenträger kopiert. Diese Metadaten sind zum Zurückschreiben der Bandkopien erforderlich. Um die Metadaten zu schützen, müssen Sie die Serverdatenbank zusammen mit dem Datenträgerprotokoll, den Serveroptionen und den Einheitenkonfigurationsdateien separat sichern. Wenn Sie die Konsolidierung mit Containerkopierspeicherpools verwenden, die über Datenträger an einem anderen Standort verfügen, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind, um Schutz für die Wiederherstellung nach einem Katastrophenfall bereitstellen zu können:

- Datenbanksicherungsoperationen werden ausgeführt, nachdem Zeitpläne für den Schutz von Speicherpools und DRM-Versetzungszeitpläne beendet wurden.
- Alle Datenbanksicherungsdatenträger und DRM-Datenträger werden zusammen ausgelagert.

Anweisungen zum Sichern der Serverdatenbank und zugehöriger Dateien finden Sie in Zeitpläne für Serververwaltungsaktivitäten definieren.

4. Wahlweise können Sie den Zeitplan für den Schutz für einen Verzeichniscontainerspeicherpool, dem ein oder mehrere Containerkopierspeicherpools zugeordnet sind, ändern, indem Sie den Befehl `UPDATE SCHEDULE` verwenden. Der Zeitplan, der vom Operations Center erstellt wird, hat den Namen `CONTAINER_COPY`.

#### **Zugehörige Konzepte:**

Datenspeicher in Containerkopierspeicherpools

#### **Zugehörige Tasks:**

Bestimmen, ob Containerkopierspeicherpools für den Schutz vor Katastrophen verwendet werden können

#### **Zugehörige Verweise:**

`DEFINE LIBRARY` (Speicherarchiv definieren)

`PROTECT STGPOOL` (Daten schützen, die zu einem Speicherpool gehören)

`UPDATE SCHEDULE` (Verwaltungszeitplan aktualisieren)

`QUERY DRMSTATUS` (Disaster Recovery Manager-Systemparameter abfragen)

## **Banddatenträger ohne Konfiguration von DRM im Rotationsprinzip auslagern**

Wenn Ihre Speicherlösung Containerkopierspeicherpools umfasst, die durch Banddatenträger dargestellt werden, die Funktion 'Disaster Recovery Manager' (DRM) jedoch nicht konfiguriert wurde, können Sie eine manuelle Prozedur verwenden, um die Banddatenträger im Rotationsprinzip auszulagern. Indem Sie Kopien von Daten in ausgelagerten Banddatenträgern aufbewahren, können Sie die Daten in einem Katastrophenfall zurückschreiben.

### **Vorgehensweise**

1. Entnehmen Sie den Speicherdatenträger, der im Rotationsprinzip ausgelagert werden muss, mithilfe des Befehls `CHECKOUT LIBVOLUME`.
2. Aktualisieren Sie den Datenträger, um anzugeben, dass er ausgelagert wird, mithilfe des Befehls `UPDATE VOLUME` unter Angabe von `ACCESS=UNAVAILABLE`. Geben Sie wahlweise den Standort für die Auslagerung mithilfe des Parameters `LOCATION` an. Geben Sie beispielsweise `LOCATION=SITE1` an.

3. Konsolidieren Sie Speicherbereich, indem Sie eine der folgenden Aktionen ausführen:
  - Um Speicherbereich zu konsolidieren, ohne den Speicherpool zu schützen, führen Sie den Befehl PROTECT STGPOOL unter Angabe von `TYPE=LOCAL` und `RECLAIM=ONLY` aus.
  - Um Speicherbereich zu konsolidieren, während der Speicherpool geschützt wird, führen Sie den Befehl PROTECT STGPOOL ohne Angabe von `RECLAIM=ONLY` aus.
4. Überwachen Sie den Datenträger mithilfe des Befehls QUERY VOLUME. Wenn der Datenträger als nicht verfügbar und leer angezeigt wird, bringen Sie den Datenträger wieder vor Ort und stellen Sie ihn mithilfe des Befehls CHECKIN LIBVOLUME in das Speicherarchiv zurück.
5. Aktualisieren Sie den Datenträger mithilfe des Befehls UPDATE VOLUME unter Angabe von `ACCESS=READWRITE`.

**Zugehörige Verweise:**

CHECKOUT LIBVOLUME (Speicherdatenträger aus einem Speicherarchiv entnehmen)  
 PROTECT STGPOOL (Daten schützen, die zu einem Speicherpool gehören)  
 UPDATE VOLUME (Speicherpooldatenträger ändern)

## Schwellenwert für Datenträgerkonsolidierung für Containerkopienspeicherpools ändern

---

Standardmäßig ist die Konsolidierung von Banddatenträgern für Containerkopienspeicherpools aktiviert. Um sicherzustellen, dass Banddatenträger effizient verwendet werden, können Sie den Schwellenwert für Datenträgerkonsolidierung ändern.

### Vorgehensweise

---

1. Klicken Sie auf der Seite Übersicht im Operations Center auf Speicher > Speicherpools.
2. Wählen Sie den Speicherpool aus und klicken Sie auf Details und dann auf Merkmale.
3. Definieren Sie im Abschnitt Wiederherstellung den Prozentsatz der Konsolidierung und klicken Sie auf Sichern.  
 Tipp: Es ist auch möglich, den Schwellenwert für Konsolidierung zu ändern, indem Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters RECLAIM ausgeben. Ausführliche Informationen zum Parameter RECLAIM finden Sie in den Beschreibungen der Befehle zum Definieren und Aktualisieren von Containerkopienspeicherpools.  
 Einschränkung: Sie können den Befehl RECLAIM STGPOOL nicht zum Konsolidieren von Datenträgern in Containerkopienspeicherpools verwenden. Ausführliche Informationen zum Konsolidieren von Datenträgern in Containerkopienspeicherpools finden Sie in der Beschreibung des Parameters RECLAIM im Befehl PROTECT STGPOOL.

## Banddatenträger in Containerkopienspeicherpools konsolidieren

---

Sie können Banddatenträger in Containerkopienspeicherpools konsolidieren, ohne eine Schutzoperation auszuführen, wenn nicht ausreichend Zeit zur Verfügung steht, um sowohl Schutz- als auch Konsolidierungsoperationen zu ermöglichen.

### Informationen zu diesem Vorgang

---

Wenn Sie den Befehl PROTECT STGPOOL ausgeben und es sich bei dem Zielspeicherpool um einen Containerkopienspeicherpool handelt, werden standardmäßig sowohl Schutz- als auch Konsolidierungsoperationen ausgeführt. Das bevorzugte Verfahren ist sowohl die Ausführung von Schutz- als auch von Konsolidierungsoperationen zu ermöglichen. Aus Gründen der Zeitersparnis können Sie jedoch nur die Speicherpoolschutzoperation oder nur die Konsolidierung ausführen oder die Anzahl Banddatenträger, die konsolidiert werden, einschränken. Verwenden Sie diese Prozedur nur, wenn Banddatenträger schnell konsolidiert werden müssen oder wenn eine begrenzte Anzahl Banddatenträger konsolidiert werden muss.

### Vorgehensweise

---

Um Banddatenträger zu konsolidieren, ohne eine Speicherpoolschutzoperation auszuführen, führen Sie die folgenden Schritte aus:

1. Optional: Um den Umfang des Speicherbereichs, der konsolidiert wird, zu maximieren, starten Sie den Bestandsverfallsprozess, indem Sie den Befehl EXPIRE INVENTORY ausgeben.
2. Bestimmen Sie, ob die Konsolidierung bis zum Abschluss ausgeführt werden soll oder ob die Anzahl Banddatenträger, die konsolidiert werden, begrenzt werden soll.
3. Um die Konsolidierung bis zum Abschluss auszuführen, geben Sie den Befehl PROTECT STGPOOL unter Angabe der Parameter `TYPE=LOCAL` und `RECLAIM=ONLY` aus. Um beispielsweise Speicherbereich in einem lokalen Containerkopienspeicherpool zu konsolidieren, der als Zielschutzpool für SPOOL1 definiert ist, geben Sie den folgenden Befehl aus:

```
protect stgpool spool1 type=local reclaim=only
```

4. Um eine begrenzte Anzahl Banddatenträger zu konsolidieren, führen Sie die folgenden Schritte aus:

- a. Legen Sie einen Konsolidierungsgrenzwert für den Containerkopierspeicherpool fest, indem Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters RECLAIMLIMIT ausgeben. Mit diesem Parameter wird die Anzahl Datenträger in dem Containerkopierspeicherpool, die konsolidiert werden, begrenzt.
- b. Geben Sie den Befehl PROTECT STGPOOL unter Angabe des Parameters TYPE=LOCAL zusammen mit dem Parameter RECLAIM=YESLIMITED oder RECLAIM=ONLYLIMITED aus.  
Tipp: Wenn Sie RECLAIM=YESLIMITED angeben, werden sowohl Konsolidierungs- als auch Speicherpoolschutzoperationen ausgeführt, wenn der Befehl PROTECT STGPOOL ausgegeben wird. Wenn Sie RECLAIM=ONLYLIMITED angeben, wird nur die Konsolidierungsoperation ausgeführt. Wenn Sie einen dieser Werte angeben, wird die Konsolidierung nur so lange ausgeführt, bis der Konsolidierungsgrenzwert, der für den Containerkopierspeicherpool definiert ist, erreicht ist. Der Konsolidierungsgrenzwert wird mit dem Parameter RECLAIMLIMIT im Befehl DEFINE STGPOOL oder UPDATE STGPOOL definiert.

Um beispielsweise maximal fünf Banddatenträger in einem Containerkopierspeicherpool mit dem Namen CCPOOL1 zu konsolidieren, ohne eine Schutzoperation für den Quellenverzeichniscontainerspeicherpool mit dem Namen SPOOL1 auszuführen, geben Sie die folgenden Befehle aus:

```
update stgpool ccpool1 reclaimlimit=5
protect stgpool spool1 type=local reclaim=onlylimited
```

Um beispielsweise einen Speicherpool mit dem Namen SPOOL1 zu schützen und maximal 10 Banddatenträger in dem zugehörigen Containerkopierspeicherpool zu konsolidieren, geben Sie die folgenden Befehle aus:

```
update stgpool spool1 reclaimlimit=10
protect stgpool spool1 type=local reclaim=yeslimited
```

## Ergebnisse

---

Die Konsolidierungsverarbeitung für den Containerkopierspeicherpool ist abgeschlossen. Die Speicherpoolschutzoperation wurde nicht ausgeführt, sodass Daten im Verzeichniscontainerspeicherpool, die seit der letzten Schutzoperation aktualisiert wurden, nicht geschützt werden.

## Nächste Schritte

---

1. Schützen Sie die Daten im Verzeichniscontainerspeicherpool in dem Containerkopierspeicherpool, indem Sie den Befehl PROTECT STGPOOL unter Angabe des Parameters TYPE=LOCAL ausgeben. Der Schutzprozess wird mit dem Standardparameter RECLAIM=YES ausgeführt. Die Schutzoperation nimmt weniger Zeit in Anspruch, da die Konsolidierung bereits ausgeführt wurde. Um beispielsweise die Daten in einem Verzeichniscontainerspeicherpool mit dem Namen SPOOL1 zu schützen, geben Sie den folgenden Befehl aus:

```
protect stgpool spool1 type=local
```

Es ist auch möglich, die Daten in einem Verzeichniscontainerspeicherpool mit dem Namen SPOOL1 zu schützen, ohne die Konsolidierung auszuführen, indem Sie den folgenden Befehl ausgeben:

```
protect stgpool spool1 type=local reclaim=no
```

2. Sichern Sie die Serverdatenbank und führen Sie geplante Verwaltungsoperationen aus. Anweisungen finden Sie in Zeitpläne für Serververwaltungsaktivitäten definieren.

### Zugehörige Verweise:

PROTECT STGPOOL (Daten schützen, die zu einem Speicherpool gehören)  
DEFINE STGPOOL (Containerkopierspeicherpool definieren)  
UPDATE STGPOOL (Containerkopierspeicherpool aktualisieren)  
EXPIRE INVENTORY (Bestandsverfallsverarbeitung manuell starten)

## Bestimmen, ob Containerkopierspeicherpools für den Schutz vor Katastrophen verwendet werden können

---

Bestimmen, ob Containerkopierspeicherpools Ihre Anforderungen für den Schutz vor Katastrophen erfüllen

### Informationen zu diesem Vorgang

---

Sie können eine ausgelagerte Kopie Ihres Containerkopierspeicherpools für den Schutz für die Wiederherstellung nach einem Katastrophenfall oder zur Erfüllung gesetzlicher Bestimmungen und Geschäftsanforderungen für ausgelagerte Bandkopien erstellen. Bevor Sie sich für die Verwendung ausgelagerter Bandkopien zum Schutz vor Katastrophen entscheiden, müssen Sie sorgfältig abwägen, ob die Lösung Ihre Zielsetzung für Wiederherstellungszeit erfüllt.

Die Verwendung von Containerkopierspeicherpools für die Wiederherstellung nach einem Katastrophenfall ist geeignet, wenn das Datenvolumen in Ihrer Umgebung kleiner-gleich den folgenden Werten ist:

- 200 TB verwaltete Daten insgesamt
- 50 TB Back-End-Daten
- 37 TB Front-End-Daten

#### Gesamtvolumen der verwalteten Daten

Alle Daten, die in dem Verzeichniscontainerspeicherpool auf dem Server gespeichert sind. Dies umfasst aktive und inaktive Versionen der Daten. Die Anzahl Versionen wird durch Aufbewahrungsmaßnahmen bestimmt.

#### Back-End-Daten

Alle Daten, die in dem Containerkopierspeicherpool gespeichert sind.

#### Front-End-Daten

Die derzeit aktiven Daten, die in dem Containerkopierspeicherpool gespeichert sind. Dies sind die aktiven Daten, die zum Zurückschreiben von Daten auf Clientknoten verwendet werden. Bei einer Katastrophe sind alle Front-End-Daten oder ein Teil der Front-End-Daten zur Wiederaufnahme der Produktion erforderlich. Die Front-End-Daten sind ein Prozentsatz des Gesamtvolumens der verwalteten Daten; ihr Volumen ist abhängig von den aktiven Maßeinstellungen kleiner-gleich dem Gesamtvolumen der verwalteten Daten.

Um innerhalb von 48 Stunden nach einem Katastrophenfall eine Wiederherstellung ausführen zu können, muss die Systemumgebung am Wiederherstellungsstandort die Hardwaremindestvoraussetzungen für die Aktionen in der folgenden Tabelle erfüllen.

| Aktion  | Erforderlicher Zeitbedarf   | Mindestvoraussetzungen   |
|---|---|--|
| <p>Konfigurieren Sie einen neuen IBM Spectrum Protect-Server am Standort für die Wiederherstellung nach einem Katastrophenfall. Um den neuen Server zu konfigurieren, müssen Sie die folgenden Schritte ausführen:</p> <ol style="list-style-type: none"> <li>1. Stellen Sie Platten für den Server bereit.</li> <li>2. Schreiben Sie den Server aus der Sicherung zurück.</li> <li>3. Starten Sie den Server.</li> <li>4. Aktualisieren Sie die Speicher- und Einheitenkonfigurationen.</li> </ol> | <p>Zeitbedarf zum Wiederherstellen des Servers: 6 Stunden</p>   | <p>Verwenden Sie ein Solid-State-Laufwerk (SSD) für die Serverdatenbank, das die folgenden Voraussetzungen erfüllt:</p> <ul style="list-style-type: none"> <li>• Kombiniertes Schreib-/Lesedurchsatz von mindestens 100 MB pro Sekunde im Durchschnitt</li> <li>• Mindestens 12.862 Ein-/Ausgabeoperationen pro Sekunde (IOPS) im Durchschnitt</li> </ul>  |
| <p>Prüfen Sie den Verzeichniscontainerspeicherpool und reparieren Sie die Daten mithilfe von Bändern.<br/>Tipp: Wenn das System die Hardwaremindestvoraussetzungen erfüllt, können Sie bis zu 50 TB Back-End-Daten innerhalb von 48 Stunden reparieren.</p>   | <p>Zeitbedarf zum Prüfen des Speicherpools: 2 Stunden</p> <p>Zeitbedarf zum Reparieren des Speicherpools mithilfe einer Bandkopie: 28 Stunden</p> <p>Anmerkung: Der geschätzte Zeitbedarf gilt für den Fall, dass maximal 200 TB verwaltete Daten insgesamt im Speicherpool vorhanden sind.</p> | <p>Verwenden Sie Nearline-SAS-Laufwerke (NL-SAS-Laufwerke) wie in einer mittelgroßen Blueprint-Serverkonfiguration mit einer Mindestschreibleistung von 700 MB pro Sekunde auf Speicherpoolplatte.</p> <p>Verwenden Sie Bandtechnologie einer neuen Generation, wie beispielsweise LTO-7 oder besser, mit mindestens sechs Laufwerken, um gleichzeitig ablaufende Leseoperationen von Banddatenträgern zu ermöglichen.</p> |
| <p>Schreiben Sie Daten auf Clientknoten zurück.<br/>Tipp: Wenn das System die Hardwaremindestvoraussetzungen erfüllt, können Sie bis zu 37 TB Front-End-Daten innerhalb von 48 Stunden zurückschreiben.</p>   | <p>Zeitbedarf für Clientzurückschreibungsoperationen: 12 Stunden</p>  | <p>Verwenden Sie Nearline-SAS-Laufwerke (NL-SAS-Laufwerke) wie in einer mittelgroßen Blueprint-Serverkonfiguration mit mindestens 10 Zurückschreibungssitzungen und einer Mindestschreibleistung von 3102 GB pro Stunde.</p>   |

## Vorgehensweise

1. Schätzen Sie die Wiederherstellungszeit nach einem Katastrophenfall für Ihre Umgebung mithilfe der folgenden Tabelle. Bestimmen Sie, ob die Wiederherstellungszeit Ihre Anforderungen erfüllt.

Tabelle 1. Geschätzte Wiederherstellungszeit für unterschiedliche Gesamtvolumina verwalteter Daten

| Zielsetzung für Wiederherstellungszeit | Gesamtvolumen der verwalteten Daten (TB) | Anzahl Stunden zur Reparatur eines Verzeichniscontainerspeicherpools (erstes Byte zurückgeschrieben) | Stunden bis zur Zurückschreibung der Clientknoten (Wiederherstellung nach einem Katastrophenfall abgeschlossen) |
|--|--|--|---|
| Bis zu 1 Tag                           | 25                                       | 10   | 12  |
|  | 50                                       | 13   | 16  |
|  | 75                                       | 17   | 22  |
| Bis zu 2 Tage                          | 100                                      | 20   | 26  |
|  | 200                                      | 34   | 46  |
| Bis zu 4 Tage                          | 300                                      | 48   | 66  |
|  | 400                                      | 62   | 86  |
| Mehr als 4 Tage                        | 500                                      | 76   | 106   |

Anmerkungen:

- o Welche Geschwindigkeiten erzielt werden können, ist in hohem Maß von der Arbeitslast und der konfigurierten Umgebung abhängig.
  - o Der Prozentsatz an Front-End-Daten ist relativ zum Gesamtvolumen der verwalteten Daten. Eine Zunahme des Front-End-Datenvolumens hat eine Verlängerung der Wiederherstellungsgesamtzeit zur Folge. Eine Abnahme des Front-End-Datenvolumens hat eine Verkürzung der Wiederherstellungsgesamtzeit zur Folge.
2. Schätzen Sie die Wiederherstellungszeit für Ihre Umgebung mithilfe der folgenden Formel:
- o Schätzen Sie den Wert für **Stunden bis zur Reparatur eines Verzeichniscontainerspeicherpools (erstes Byte zurückgeschrieben)**:

Zeitbedarf bis zur Zurückschreibung des ersten Byte auf dem Client =  
6 Stunden + 14 Stunden pro 100 TB verwalteter Daten insgesamt

- o Schätzen Sie den Wert für **Stunden bis zur Zurückschreibung der Clientknoten (Wiederherstellung nach einem Katastrophenfall abgeschlossen)**:

Zeitbedarf bis zum Abschluss der Clientzurückschreibung =  
Zeitbedarf bis zur Zurückschreibung des ersten Byte auf dem Client + ((Gesamtvolumen der verwalteten Daten \* Front-End-Daten) / Zurückschreibungsgeschwindigkeit)

**Zurückschreibungsgeschwindigkeit:** Die Geschwindigkeit, mit der Clients Daten vom Server wieder auf ihren lokalen Computer oder ihre lokale Speichereinheit zurückschreiben können.

3. Führen Sie Testprozeduren für die Wiederherstellung nach einem Katastrophenfall aus, um sicherzustellen, dass Containerkopierspeicherpools zum Zurückschreiben Ihrer Umgebung innerhalb eines Zeitrahmens, der Ihre Anforderungen erfüllt, verwendet werden können.

#### Zugehörige Verweise:

Speicherpools nach einem Katastrophenfall reparieren

## Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren

Sie können deduplizierte Daten und nicht deduplizierte Daten in einem Cloud-Containerspeicherpool speichern und die Daten nach Bedarf zurückschreiben. Sie können Cloud-Containerspeicherpools für die Verwendung einer der folgenden Service-Provider und Protokolle konfigurieren: Amazon Web Services (AWS) mit Simple Storage Service (S3), IBM® Cloud Object Storage mit Swift oder S3 (und IBM SoftLayer), Microsoft Azure und OpenStack mit Swift unter Verwendung von Keystone Version 1 oder Version 2. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.

### Vorbereitende Schritte

Führen Sie die folgenden Schritte aus:

1. Rufen Sie die Konfigurationsinformationen für Ihren Cloud-Service-Provider ab:
  - o Amazon mit S3 (Off-Premises)
  - o Microsoft Azure
  - o IBM Cloud Object Storage mit S3 (Off-Premises, mit IBM SoftLayer)
  - o IBM Cloud Object Storage mit Swift (Off-Premises, mit IBM SoftLayer)
  - o IBM Cloud Object Storage mit S3 (On-Premises)

- o OpenStack mit Swift (On-Premises oder Off-Premises)
2. Geben Sie eine Einheitenklasse an, die für Datenbanksicherungsoperationen verwendet werden soll. Wenn Sie Verschlüsselung für Cloud-Containerspeicherpools verwenden, wird der Masterverschlüsselungsschlüssel des Servers zum Schützen des Cloudverschlüsselungsschlüssels in einer Datenbanksicherung verwendet.
    - a. Wählen Sie in der Menüleiste des Operations Center Server aus.
    - b. Wählen Sie eine Serverzeile aus und klicken Sie auf Sichern.
    - c. Wählen Sie eine Einheitenklasse aus, die für Datenbanksicherungsoperationen verwendet werden soll, und klicken Sie auf Sichern.
- Tipp: Sie können auch stattdessen den Befehl SET DBRECOVERY verwenden, um eine Einheitenklasse für die Datenbanksicherung anzugeben.

## Vorgehensweise

---

Um Daten in einem Cloud-Containerspeicherpool zu speichern, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen Cloud-Containerspeicherpool. Sie müssen Konfigurationsinformationen zur Identifikation des Cloud-Service angeben.
  - a. Klicken Sie in der Menüleiste des Operations Center auf Speicher > Speicherpools.
  - b. Klicken Sie auf der Seite Speicherpools auf + Speicherpool.
  - c. Führen Sie die Schritte im Assistenten Speicherpool hinzufügen aus. Wählen Sie On-Premises-Cloud oder Off-Premises-Cloud für den Typ des containerbasierten Speichers aus.
2. Aktualisieren Sie Ihre Verwaltungsklassen und Maßnahmengruppen für die Verwendung des neuen Speicherpools. Um eine Verwaltungsklasse für die Verwendung des neuen Speicherpools zu aktualisieren, führen Sie die folgenden Schritte aus:
  - a. Klicken Sie in der Menüleiste des Operations Center auf Services.
  - b. Wählen Sie auf der Seite Maßnahmen eine Maßnahmendomäne aus und klicken Sie auf Details.
  - c. Klicken Sie auf der Seite Details auf die Registerkarte Maßnahmengruppen.
  - d. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppen sind editierbar.
  - e. Optional: Um eine Maßnahmengruppe zu editieren, die nicht aktiv ist, klicken Sie auf die vorwärts und rückwärts gerichteten Pfeile, um die Maßnahmengruppe zu lokalisieren.
  - f. Aktualisieren Sie eine oder mehrere Verwaltungsklassen für die Verwendung des neuen Speicherpools, indem Sie das Feld Sicherungsziel der Tabelle editieren.
  - g. Klicken Sie auf Sichern.
3. Aktivieren Sie die geänderte Maßnahmengruppe, indem Sie die folgenden Schritte ausführen:
  - a. Klicken Sie auf Aktivieren. Da das Ändern der aktiven Maßnahmengruppe unter Umständen einen Datenverlust zur Folge haben kann, wird eine Zusammenfassung der Unterschiede zwischen der aktiven Maßnahmengruppe und der neuen Maßnahmengruppe angezeigt.
  - b. Studieren Sie die Unterschiede zwischen entsprechenden Verwaltungsklassen in den beiden Maßnahmengruppen und wägen Sie die Auswirkungen auf Clientdateien ab. Clientdateien, die an Verwaltungsklassen in der derzeit aktiven Maßnahmengruppe gebunden sind, werden nach der Aktivierung in der neuen Maßnahmengruppe an die Verwaltungsklassen mit denselben Namen gebunden.
  - c. Ermitteln Sie Verwaltungsklassen in der derzeit aktiven Maßnahmengruppe, die in der neuen Maßnahmengruppe keine Entsprechung haben, und wägen Sie die Auswirkungen auf Clientdateien ab. Clientdateien, die an diese Verwaltungsklassen gebunden sind, werden nach der Aktivierung von der Standardverwaltungsklasse in der neuen Maßnahmengruppe verwaltet.
  - d. Wenn die Änderungen, die durch die Maßnahmengruppe implementiert werden, akzeptabel sind, wählen Sie das Kontrollkästchen Ich weiß, dass diese Aktualisierungen zu einem Datenverlust führen können aus und klicken Sie auf Aktivieren.
4. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppen sind nicht mehr editierbar.
5. Um die Vorteile von lokalem Speicher nutzen zu können, erstellen Sie mit dem Befehl DEFINE STGPOOLDIRECTORY ein Speicherpoolverzeichnis für diesen Speicherpool. Weitere Informationen finden Sie in Leistung für Cloudobjektspeicher optimieren.

### Zugehörige Tasks:

Konfiguration von Cloud-Containerspeicherpools für AWS mit S3 vorbereiten (Off-Premises)  
 Konfiguration von Cloud-Containerspeicherpools für IBM Cloud Object Storage mit S3 vorbereiten (On-Premises)  
 Konfiguration von Cloud-Containerspeicherpools für IBM Cloud Object Storage mit S3 vorbereiten (Off-Premises)  
 Konfiguration von Cloud-Containerspeicherpools für IBM Cloud Object Storage mit Swift vorbereiten (Off-Premises)  
 Konfiguration von Cloud-Containerspeicherpools für OpenStack mit Swift vorbereiten  
 Daten für Cloud-Containerspeicherpools verschlüsseln  
 Leistung für Cloudobjektspeicher optimieren

### Zugehörige Verweise:

SET DBRECOVERY (Einheitenklasse für automatische Sicherungen definieren)

# Konfiguration von Cloud-Containerspeicherpools für AWS mit S3 vorbereiten (Off-Premises)

---

Bevor Sie Cloud-Containerspeicherpools für die Off-Premises-Verwendung von Amazon Web Services (AWS) mit dem Protokoll 'Simple Storage Service' (S3) konfigurieren können, müssen Sie Informationen von Amazon abrufen, die für den Konfigurationsprozess erforderlich sind.

## Informationen zu diesem Vorgang

---

AWS-Kontoberechtigungen unterscheiden sich von Amazon-Kontoberechtigungen. Verwenden Sie die Berechtigungen für Ihr AWS-Konto, wenn Sie Speicherpools im Operations Center oder mit dem Befehl DEFINE STGPOOL konfigurieren.

AWS verwendet *Buckets* zum Speichern von Daten. AWS-Buckets werden auf dieselbe Art und Weise wie Container in einem Cloud-Containerspeicherpool verwendet. IBM Spectrum Protect erstellt für eine Instanz von IBM Spectrum Protect automatisch ein Bucket in Amazon, das von allen Pools für diese Instanz gemeinsam genutzt wird.

Einschränkung: Es gelten die folgenden Einschränkungen:

- Sie dürfen ein AWS-Bucket nur mit IBM Spectrum Protect editieren und die Daten in dem Bucket nicht ändern oder die Konfigurationseinstellungen für das Bucket nicht editieren.
- Bei Off-Premises-Cloud-Containerspeicherpools, die AWS mit dem Amazon S3-Protokoll verwenden, werden Daten standardmäßig verschlüsselt. Der IBM Spectrum Protect-Server unterstützt jedoch nicht die Verschlüsselung der Daten unter Verwendung von AWS-Bucketmaßnahmen.

## Vorgehensweise

---

1. Melden Sie sich bei einem AWS-Konto an, indem Sie die Seite für Amazon S3 aufrufen und auf die Schaltfläche zum Erstellen eines AWS-Kontos klicken.
2. Rufen Sie Ihre AWS-Berechtigungen ab:
  - a. Rufen Sie die Seite für Amazon S3 auf und klicken Sie auf die Schaltfläche zum Anmelden an der Konsole.
  - b. Wählen Sie Ihren Namen und dann die Option für Sicherheitsberechtigungen aus.
  - c. Rufen Sie den Abschnitt für Zugriffsschlüssel auf und lokalisieren Sie die Felder für die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel. Notieren Sie die Werte, damit Sie diese beim Konfigurieren von Speicherpools verwenden können.
3. Wenn Sie planen, Speicherpools mithilfe des Assistenten 'Speicherpool hinzufügen' im Operations Center zu konfigurieren, verwenden Sie die folgenden Werte für die Parameter:
  - Cloudtyp: *Amazon - S3 API*
  - Zugriffsschlüssel-ID: *Zugriffsschlüssel-ID*
  - Geheimer Zugriffsschlüssel: *geheimer\_Zugriffsschlüssel*
  - Region: Wählen Sie auf der Basis der Seite Regionen und Endpunkte von AWS den Regionsendpunkt aus, der für Ihren Standort am besten geeignet ist. Wenn Sie *Other* auswählen, geben Sie eine Regionsendpunkt-URL im Feld URL an und schließen Sie das Protokoll, in der Regel `https://`, ein. Normalerweise können Sie für den Parameter Region die Region verwenden, die Ihrem physischen Standort am nächsten liegt. Da ein Amazon-Bucket nur in einer einzigen Region vorhanden ist, können Sie nur eine einzige Endpunkt-URL für eine Region angeben. Wenn eine GovCloud-Region erforderlich ist, geben Sie eine der auf der Seite AWS GovCloud (US) Endpoints aufgelisteten URLs an.  
Warnung: Stellen Sie sicher, dass nur die AWS-Endpunkt-URL für den Regionswert verwendet wird, wie beispielsweise `https://s3-us-west-1.amazonaws.com`. Verwenden Sie für diesen Wert nicht die statische Website-Hosting-URL.
  - Bucketname: Verwenden Sie den vom Server generierten Standardbucketnamen oder geben Sie einen neuen Bucketnamen an.
4. Um einen Cloud-Containerspeicherpool zu definieren, geben Sie den Befehl DEFINE STGPOOL mit den folgenden Werten aus:
  - CLOUDTYPE: *S3*
  - IDENTITY: *Zugriffsschlüssel-ID*
  - PASSWORD: *geheimer\_Zugriffsschlüssel*
  - CLOUDURL: Geben Sie auf der Basis der Seite Regionen und Endpunkte von AWS die Regionsendpunkt-URL an, die für Ihren Standort am besten geeignet ist.

Normalerweise können Sie für den Parameter CLOUDURL die Region verwenden, die Ihrem physischen Standort am nächsten liegt. Wenn eine GovCloud-Region erforderlich ist, geben Sie eine der auf der Seite AWS GovCloud (US) Endpoints aufgelisteten URLs an.

Warnung: Stellen Sie sicher, dass nur die AWS-Endpunkt-URL für den CLOUDURL-Wert verwendet wird, wie beispielsweise `https://s3-us-west-1.amazonaws.com`. Verwenden Sie für diesen Wert nicht die statische Website-Hosting-URL.

## Nächste Schritte

---

Konfigurieren Sie Cloud-Containerspeicherpools für AWS, indem Sie die Anweisungen in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren ausführen.

## Amazon S3-kompatible Einheit als Cloud-Containerspeicherpool konfigurieren

---

Sie können eine Speichereinheit konfigurieren, die mit dem Protokoll Amazon Simple Storage Service (S3) kompatibel ist, um die Einheit als IBM Spectrum Protect-Cloud-Containerspeicherpool verwenden zu können.

### Informationen zu diesem Vorgang

---

Amazon S3 verwendet *Buckets* zum Speichern von Daten. Sie müssen ein Bucket auf der S3-kompatiblen Speichereinheit für die Verwendung durch einen IBM Spectrum Protect-Server erstellen. Verwenden Sie nach dem Erstellen des Buckets die Berechtigungsnachweise des Kontos auf Ihrer Amazon S3-kompatiblen Cloudobjektspeichereinheit, wenn Sie Speicherpools mit dem Befehl DEFINE STGPOOL konfigurieren.

Einschränkung: Sie dürfen die Daten in dem Bucket nicht ändern oder die Konfigurationseinstellungen für das Bucket nicht editieren.

### Vorgehensweise

---

1. Erstellen Sie ein Bucket in der Cloudobjektspeichereinheit. Führen Sie die Anweisungen in der Einheitendokumentation aus.
2. Erstellen Sie ein Benutzerkonto in der Cloudobjektspeichereinheit. Das Konto wird von IBM Spectrum Protect für den Zugriff auf die Einheit mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels verwendet. Stellen Sie sicher, dass das Konto über Berechtigungen zum Speichern von Daten in dem in Schritt 1 erstellten Bucket und zum Löschen von Daten aus diesem Bucket verfügt. Notieren Sie die Werte für die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel, damit Sie diese beim Konfigurieren von Speicherpools verwenden können.
3. Geben Sie den URL-Wert an, der von IBM Spectrum Protect für den Zugriff auf die Cloudobjektspeichereinheit verwendet wird. Anweisungen finden Sie in der Dokumentation zu Ihrer Cloudobjektspeichereinheit.
4. Um einen Cloud-Containerspeicherpool zu definieren, geben Sie den Befehl DEFINE STGPOOL mit den folgenden Werten aus:
  - CLOUDTYPE: S3
  - IDENTITY: *Zugriffsschlüssel-ID*
  - PASSWORD: *geheimer\_Zugriffsschlüssel*
  - CLOUDURL: `http://IP-Adresse_des_Cloudobjektspeicherendpunkts` oder `https://IP-Adresse_des_Cloudobjektspeicherendpunkts`. Wenn Sie mehr als einen Endpunkt verwenden, listen Sie die IP-Adressen der Endpunkte wie in dem folgenden Beispiel gezeigt durch einen vertikalen Strich (|) ohne Leerzeichen voneinander getrennt auf:  
  
`CLOUDURL=URL1_für_Endpunkt|URL2_für_Endpunkt|URL3_für_Endpunkt`
  - BUCKETNAME: *Name\_des\_Buckets\_auf\_der\_Einheit*

Um die Leistung zu optimieren, verwenden Sie mehrere Endpunkte oder eine Einrichtung für den Lastausgleich.

## Nächste Schritte

---

Konfigurieren Sie Cloud-Containerspeicherpools auf ähnliche Weise wie einen Cloud-Containerspeicherpool für IBM Cloud Object Storage, indem Sie die Anweisungen in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren ausführen.

## Konfiguration von Cloud-Containerspeicherpools für Microsoft Azure vorbereiten (Off-Premises)

---

Bevor Sie Cloud-Containerspeicherpools für die Verwendung des Microsoft Azure-Cloud-Computing-Systems konfigurieren können, müssen Sie Informationen für den Konfigurationsprozess von Microsoft abrufen.

### Informationen zu diesem Vorgang

---

IBM Spectrum Protect unterstützt die folgenden Azure-Speicherebenen:

- *Speicherebene 'Heiß' (Hot)* für Daten, auf die häufig zugegriffen wird
- *Speicherebene 'Kalt' (Cool)* für Daten, auf die weniger häufig zugegriffen wird



Eine Speicherebene 'Kalt' (Cool) kann für die kosteneffiziente langfristige Speicherung verwendet werden. Das Zurückschreiben von Daten aus einer Speicherebene 'Kalt' (Cool) ist jedoch kostenintensiver als die Zurückschreibung aus einer Speicherebene 'Heiß' (Hot).

## Vorgehensweise

---

1. Melden Sie sich für ein Microsoft Azure-Konto an, indem Sie das Azure-Portal aufrufen und ein Konto erstellen.
2. Erstellen Sie ein Speicherkonto. In der Regel wählen Sie als Standort für das Speicherkonto den Standort aus, der Ihrem IBM Spectrum Protect-Server am nächsten liegt.
3. Rufen Sie Ihre Azure-Berechtigungsanzeige ab:
  - a. Rufen Sie das Azure-Portal auf und klicken Sie auf Speicherkonten.
  - b. Öffnen Sie das neue Speicherkonto, wechseln Sie zum Containerabschnitt im Bereich Blob-Dienst und notieren Sie den Wert für den Blob-Dienstendpunkt, damit Sie diesen beim Konfigurieren von Speicherpools verwenden können. Der Blob-Dienstendpunkt ähnelt den Werten in den folgenden Beispielen: `https://Name.blob.core.windows.net` und `http://Name.blob.core.windows.net`.
  - c. Erstellen Sie ein SAS-Token (SAS = Shared Access Signature), indem Sie die Registerkarte für Shared Access Signature öffnen und die Felder ausfüllen. Stellen Sie sicher, dass der Bereich Zulässige Dienste 'Blob' umfasst und dass der Bereich für zulässige Ressourcentypen 'Container' und 'Objekt' umfasst. Stellen Sie sicher, dass das SAS-Token über Berechtigungen zum Lesen, Schreiben, Löschen, Auflisten, Hinzufügen und Erstellen verfügt. Klicken Sie auf SAS generieren.
  - d. Notieren Sie den SAS-Tokenwert, damit Sie diesen beim Konfigurieren von Speicherpools verwenden können. Da IBM Spectrum Protect das Verfallsdatum des SAS-Tokens nicht überwacht, müssen Sie ein Datum auswählen, das Ihren Anforderungen am besten gerecht wird. Wenn das Token verfällt, geht der Zugriff des IBM Spectrum Protect-Servers auf das Speicherkonto verloren, bis Sie ein neues SAS-Token bereitstellen.  
Tipp: Wenn das SAS-Token seltener aktualisiert werden soll, legen Sie ein Verfallsdatum fest, das mehrere Jahre in der Zukunft liegt. Stellen Sie außerdem sicher, dass die Felder für das Startdatum und die Startzeit verifiziert werden.
4. Wenn Sie planen, Speicherpools mithilfe des Assistenten 'Speicherpool hinzufügen' im Operations Center zu konfigurieren, verwenden Sie die folgenden Werte für die Parameter:
  - o Cloudtyp: `Azure`
  - o SAS-Token: `Wert_für_SAS-Token`. Suchen Sie nach einer ähnlichen Zeichenfolge wie in dem folgenden Beispiel:  

```
?sv=2016-05-31&ss=b&srt=sco&sp=rwldlac&se=2017-04-05T18:26:12Z&st=2017-04-05T10:26:12Z&spr=https&sig=XUangS%2FcXXXXXXXXXXXXXXXXXXXXXXXXXXXXXELsuWp106Cmq7o%3D
```
  - o Blob-Dienstendpunkt: Geben Sie den Blob-Dienstendpunkt für Ihr Azure-Speicherkonto an, beispielsweise `https://Name.blob.core.windows.net` oder `http://Name.blob.core.windows.net`.
5. Wenn Sie planen, Speicherpools mithilfe des Befehls `DEFINE STGPOOL` zu konfigurieren, verwenden Sie die folgenden Werte für die Befehlsparameter:
  - o `CLOUDTYPE`: `Azure`
  - o `PASSWORD`: `Wert_für_SAS-Token`. Suchen Sie nach einer ähnlichen Zeichenfolge wie in dem folgenden Beispiel:  

```
?sv=2016-05-31&ss=b&srt=sco&sp=rwldlac&se=2017-04-05T18:26:12Z&st=2017-04-05T10:26:12Z&spr=https&sig=XUangS%2FcXXXXXXXXXXXXXXXXXXXXXXXXXXXXXELsuWp106Cmq7o%3D
```
  - o `CLOUDURL`: Geben Sie den Blob-Dienstendpunkt für Ihr Azure-Speicherkonto an, beispielsweise `https://Name.blob.core.windows.net` oder `http://Name.blob.core.windows.net`.

## Nächste Schritte

---

Konfigurieren Sie Cloud-Containerspeicherpools für Azure, indem Sie die Anweisungen in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren ausführen.

## Konfiguration von Cloud-Containerspeicherpools für IBM Cloud Object Storage mit Swift vorbereiten (Off-Premises)

---

Bevor Sie Cloud-Containerspeicherpools für die Off-Premises-Verwendung von IBM® Cloud Object Storage und IBM SoftLayer (IBM Bluemix) mit Swift konfigurieren können, müssen Sie Konfigurationsinformationen von der Seite 'Object Storage' in SoftLayer abrufen.

## Informationen zu diesem Vorgang

---

Verwenden Sie die Berechtigungsnachweise Ihres IBM SoftLayer-Kontos, wenn Sie die Speicherpools im Operations Center oder mit dem Befehl `DEFINE STGPOOL` konfigurieren.

## Vorgehensweise

---

1. Erstellen Sie ein SoftLayer-Konto, indem Sie die Anweisungen in der SoftLayer-Dokumentation ausführen.
2. Rufen Sie Ihre SoftLayer-Berechtigungsanzeige ab:
  - a. Rufen Sie die Seite 'Object Storage' in SoftLayer auf und melden Sie sich mit Ihren Kontoberechtigungsanzeigen an.
  - b. Wählen Sie das Konto und den Cluster für die Konfiguration aus.
  - c. Klicken Sie im Abschnitt Account auf View Credentials.
  - d. Lokalisieren Sie im Abschnitt Account Credentials die Felder Public Authentication Endpoint, Username und API Key. Notieren Sie die Werte in diesen Feldern, damit Sie diese beim Konfigurieren von Speicherpools verwenden können.
3. Wenn Sie planen, Speicherpools mithilfe des Assistenten 'Speicherpool hinzufügen' im Operations Center zu konfigurieren, verwenden Sie die folgenden Werte für die Parameter:
  - o Cloudtyp: IBM Cloud Object Storage - Swift API (SoftLayer)
  - o Benutzername: *Benutzername*
  - o Kennwort: *API-Schlüssel*
  - o URL: *öffentlicher\_Authentifizierungsendpunkt*
4. Wenn Sie planen, Speicherpools mithilfe des Befehls DEFINE STGPOOL zu konfigurieren, verwenden Sie die folgenden Werte für die Befehlsparameter:
  - o CLOUDTYPE: SOFTLAYER
  - o IDENTITY: *Benutzername*
  - o PASSWORD: *API-Schlüssel*
  - o CLOUDURL: *öffentlicher\_Authentifizierungsendpunkt*

## Nächste Schritte

---

Konfigurieren Sie Cloud-Containerspeicherpools für IBM SoftLayer, indem Sie die Anweisungen in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren ausführen.

## Konfiguration von Cloud-Containerspeicherpools für IBM Cloud Object Storage mit S3 vorbereiten (Off-Premises)

---

Sie können Cloudspeicherpools für die Off-Premises-Verwendung von IBM® Cloud Object Storage mit dem Protokoll 'Simple Storage Service' (S3) konfigurieren.

## Informationen zu diesem Vorgang

---

Die Off-Premises-Implementierung von IBM Cloud Object Storage wird über IBM SoftLayer oder IBM Bluemix verwaltet. Bei dieser Konfiguration kann nur der Eigner des SoftLayer- oder Bluemix-Kontos Buckets und Administratoren erstellen.

Verwenden Sie die Berechtigungsanzeige Ihres IBM SoftLayer- oder IBM Bluemix-Kontos, wenn Sie die Speicherpools im Operations Center oder mit dem Befehl DEFINE STGPOOL konfigurieren. Weitere Informationen finden Sie auf der Seite 'Objektspeicher' in SoftLayer. Um diese Konfiguration zu verwenden, wählen Sie Cloud Object Storage - S3 API auf der Seite 'Order Object Storage' in SoftLayer aus.

## Vorgehensweise

---

1. Melden Sie sich beim SoftLayer-Kundenportal an.
2. Klicken Sie auf das Menü Storage und wählen Sie Object Storage aus.
3. Wählen Sie auf der Seite 'Object Storage' ein S3-Konto aus.
4. Klicken Sie auf der Seite 'Cloud Object Storage' auf Manage Buckets und anschließend auf das Symbol +, um das Bucket zu erstellen, das mit dem neuen Cloud-Containerspeicherpool verwendet werden soll.
5. Klicken Sie auf Show Credentials, um Administratorberechtigungsanzeige für Ihr neues Bucket zu erstellen.
6. Klicken Sie auf Add Credential.
7. Lokalisieren Sie die Zugriffsschlüssel-ID (Access Key ID), den geheimen Zugriffsschlüssel (Secret Access Key) und den öffentlichen Authentifizierungsendpunkt (Public Authentication Endpoint). Notieren Sie die Werte in diesen Feldern, damit Sie diese beim Konfigurieren von Speicherpools verwenden können. Innerhalb des SoftLayer-Netzes können Sie einen privaten Authentifizierungsendpunkt verwenden.
8. Um Speicherpools mithilfe des Assistenten 'Speicherpool hinzufügen' im Operations Center zu konfigurieren, wählen Sie Off-Premises-Cloud aus. Verwenden Sie für die Parameter die folgenden Werte:
  - o Cloudtyp: IBM Cloud Object Storage - S3 API (SoftLayer)
  - o Zugriffsschlüssel-ID: *Zugriffsschlüssel-ID*
  - o Geheimer Zugriffsschlüssel: *geheimer\_Zugriffsschlüssel*
  - o Bucketname: *Bucketname* (aus Schritt 4)
  - o URL: *us-geo-Authentifizierungsendpunkt*Anmerkung: Bei dieser Konfiguration ist nur ein einziger Cloud-Provider-Endpunkt erforderlich. Wenn sich alle Ihre Server innerhalb des SoftLayer-Netzes befinden, können Sie einen privaten Authentifizierungsendpunkt verwenden.

9. Wenn Sie Speicherpools mithilfe des Befehls DEFINE STGPOOL konfigurieren, verwenden Sie die folgenden Werte für die Befehlsparameter:
- o CLOUDTYPE: S3
  - o IDENTITY: *Zugriffsschlüssel-ID*
  - o BUCKETNAME: *Bucketname* (aus Schritt 4)
  - o PASSWORD: *geheimer\_Zugriffsschlüssel*
  - o CLOUDURL: *us-geo-Authentifizierungsendpunkt*
- Anmerkung: Bei dieser Konfiguration ist nur ein einziger Cloud-Provider-Endpunkt erforderlich. Wenn sich alle Ihre Server innerhalb des SoftLayer-Netztes befinden, können Sie einen privaten Authentifizierungsendpunkt verwenden.

## Nächste Schritte

---

Konfigurieren Sie Cloud-Containerspeicherpools für IBM SoftLayer Cloud Object Storage, indem Sie die Anweisungen in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren ausführen.

## Konfiguration von Cloud-Containerspeicherpools für IBM Cloud Object Storage mit S3 vorbereiten (On-Premises)

---

Bevor Sie Cloud-Containerspeicherpools für die On-Premises-Verwendung von IBM® Cloud Object Storage mit S3 konfigurieren können, müssen Sie eine IBM Cloud Object Storage-Vaultvorlage und ein IBM Cloud Object Storage-Benutzerkonto definieren und dann Konfigurationsinformationen abrufen.

## Informationen zu diesem Vorgang

---

Einschränkung:

Um IBM Cloud Object Storage vor Ort mit S3 verwenden zu können, müssen Sie sicherstellen, dass Ihre Version von IBM Cloud Object Storage mit Ihrer Version von IBM Spectrum Protect kompatibel ist.

Ab IBM Spectrum Protect Version 8.1.3 ist IBM Cloud Object Storage Version 3.7.2.31 oder höher erforderlich.

IBM Cloud Object Storage-Vaults werden auf dieselbe Art und Weise wie Container in einem Cloud-Containerspeicherpool verwendet. Definieren Sie eine Vaultvorlage, um Vaults schnell mit Ihren bevorzugten Einstellungen erstellen zu können.

Verwenden Sie nach dem Erstellen einer Vaultvorlage die Berechtigungsnachweise Ihres IBM Cloud Object Storage-Benutzerkontos, um die Speicherpools im Operations Center oder mit dem Befehl DEFINE STGPOOL zu konfigurieren. Der Server verwendet das Protokoll 'Simple Storage Service' (S3) für die Kommunikation mit IBM Cloud Object Storage.

Tipp: Sie können die ersten vier Schritte in der Prozedur überspringen, wenn eine vorhandene Vault konfiguriert werden soll, indem Sie den Parameter BUCKETNAME im Befehl DEFINE STGPOOL oder UPDATE STGPOOL verwenden.

## Vorgehensweise

---

1. Erstellen Sie eine Vaultvorlage:
  - a. Melden Sie sich bei IBM Cloud Object Storage an und klicken Sie auf die Registerkarte Configure.
  - b. Erweitern Sie im Navigationsfenster dsNet die Option Storage Pools.
  - c. Wählen Sie den IBM Cloud Object Storage-Speicherpool aus, für den die Vaultvorlage erstellt werden soll, und klicken Sie auf den Link Storage Pool im Abschnitt General.
  - d. Klicken Sie im Abschnitt Vault Templates auf Create Vault Template.
  - e. Wählen Sie die Einstellungen für die Standardvaultvorlage aus. Unter Umständen können Sie die Leistung optimieren, indem Sie die Option Enable SecureSlice Technology oder Name Index Enabled nicht auswählen und die Option Recovery Listing Enabled auswählen.
  - f. Wählen Sie im Abschnitt Deployment den oder die Zugriffspools aus, die für die Vorlage verwendet werden sollen, und klicken Sie auf Save.
2. Legen Sie die Vaultvorlage als Standardvaultvorlage für Ihr IBM Cloud Object Storage-dsNet fest:
  - a. Klicken Sie auf die Registerkarte Configure.
  - b. Klicken Sie im Abschnitt Default Vault Template Configuration auf Configure.
  - c. Wählen Sie eine Vaultvorlage aus, die als Standardvaultvorlage verwendet werden soll, und klicken Sie auf Update, um diese Vorlage als Standardvorlage festzulegen.
3. Wenn Sie zum ersten Mal eine Vaultvorlage konfigurieren, aktivieren Sie die Rolle für die Vaultbereitstellung, damit Sie neue Vaults erstellen können:
  - a. Klicken Sie auf die Registerkarte Administration.
  - b. Klicken Sie im Abschnitt Provisioning API Configuration auf Configure.

- c. Wählen Sie Create Only oder Create and Delete aus, damit Benutzer neue Vaults mithilfe der Bereitstellungs-API (Provisioning API) erstellen können.
  - d. Klicken Sie auf Update, um die Einstellungen zu speichern.
4. Verwenden Sie ein IBM Cloud Object Storage-Konto mit Administratorberechtigung, um ein Benutzerkonto für die IBM Cloud Object Storage-Instanz in Ihrer Umgebung zu erstellen. Stellen Sie sicher, dass das neue Benutzerkonto über die Rolle Vault Provisioner verfügt.
5. Klicken Sie auf die Registerkarte Security und wählen Sie das neue Benutzerkonto aus.
6. Generieren Sie einen Zugriffsschlüssel für den neuen Benutzer:
  - a. Klicken Sie im Abschnitt Access Key Authentication auf Change Keys.
  - b. Klicken Sie auf der Seite Edit Access Key auf Generate New Access Key.
  - c. Klicken Sie auf Back.
7. Lokalisieren Sie im Abschnitt Access Key Authentication die Werte für Access Key ID und Secret Access Key. Notieren Sie die Werte, damit Sie diese beim Konfigurieren von Speicherpools verwenden können.
8. Lokalisieren Sie den Wert für die URL:
  - a. Klicken Sie auf die Registerkarte Configure.
  - b. Erweitern Sie im Navigationsfenster dsNet die Abschnitte Devices und Accesser.
  - c. Wählen Sie den IBM Cloud Object Storage-Accesser aus. Stellen Sie sicher, dass der Accesser zu einem Zugriffspool gehört, für den die Standardvaultvorlage implementiert ist.
  - d. Notieren Sie den im Abschnitt Device Configuration für den Accesser angegebenen Wert für IP Address, damit Sie diesen beim Konfigurieren von Speicherpools verwenden können. Geben Sie `http://` vor dem Wert für die IP-Adresse an, um Zertifikatssicherheitsfehler zu verhindern.
9. Wenn Sie Speicherpools mithilfe des Assistenten 'Speicherpool hinzufügen' im Operations Center konfigurieren, verwenden Sie die folgenden Werte für die Parameter:
  - Cloudtyp: `IBM Cloud Object Storage - S3 API`
  - Zugriffsschlüssel-ID: `Zugriffsschlüssel-ID`
  - Geheimer Zugriffsschlüssel: `geheimer_Zugriffsschlüssel`
  - Bucketname: Verwenden Sie den vom Server generierten Standardbucketnamen oder geben Sie einen neuen Bucketnamen an.
  - URL: `http://IP-Adresse_des_Cloud_Object_Storage-Accessers`  
Wichtig: Wenn mehr als ein Accesser verwendet wird, geben Sie die IP-Adresse eines Accessers ein und drücken Sie dann die Eingabetaste, um weitere IP-Adressen hinzuzufügen. Verwenden Sie zur Erzielung der optimalen Leistung mehrere Accesser oder eine Einrichtung für den Lastausgleich.
10. Wenn Sie Speicherpools mithilfe des Befehls DEFINE STGPOOL konfigurieren, verwenden Sie die folgenden Werte für die Befehlsparameter:
  - CLOUDTYPE: `S3`
  - IDENTITY: `Zugriffsschlüssel-ID`
  - PASSWORD: `geheimer_Zugriffsschlüssel`
  - CLOUDURL: `http://IP-Adresse_des_Cloud_Object_Storage-Accessers`  
Wichtig: Wenn Sie mehr als einen Accesser verwenden, listen Sie die IP-Adressen der Accesser durch einen vertikalen Strich (|) ohne Leerzeichen voneinander getrennt auf. Beispiel: `CLOUDURL=<Accesser-URL1>|<Accesser-URL2>|<Accesser-URL3>`. Verwenden Sie zur Erzielung der optimalen Leistung mehrere Accesser oder eine Einrichtung für den Lastausgleich.

## Nächste Schritte

---

Konfigurieren Sie Cloud-Containerspeicherpools für IBM Cloud Object Storage, indem Sie die Anweisungen in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren ausführen.

## Konfiguration von Cloud-Containerspeicherpools für OpenStack mit Swift vorbereiten

---

Bevor Sie Cloud-Containerspeicherpools für die On-Premises- oder Off-Premises-Verwendung von OpenStack mit Swift konfigurieren können, müssen Sie Konfigurationsinformationen vom OpenStack Swift-Computer abrufen.

### Informationen zu diesem Vorgang

---

Einschränkung: Sie müssen Version 1 oder 2 der Anwendungsprogrammierschnittstelle (API) von OpenStack Swift Release Series Juno (Serviceprojekt Keystone) verwenden.

Verwenden Sie die Berechtigungsnachweise Ihres OpenStack Swift-Kontos, wenn Sie die Speicherpools mit dem Operations Center oder dem Befehl DEFINE STGPOOL konfigurieren.

## Vorgehensweise

---

1. Erstellen Sie ein OpenStack Swift-Konto, indem Sie die Anweisungen in der OpenStack Swift-Dokumentation ausführen.
2. Rufen Sie Ihre OpenStack Swift-Berechtigungsanzeige ab:
  - a. Geben Sie auf dem OpenStack Swift-Computer den folgenden Befehl ein:

```
swift auth -v
```
  - b. Lokalisieren Sie in der Ausgabe die Werte für `OS_AUTH_URL`, `OS_TENANT_NAME`, `OS_USERNAME` und `OS_PASSWORD`.  
Notieren Sie die Werte, damit Sie diese beim Konfigurieren von Speicherpools verwenden können.
3. Wenn Sie planen, Speicherpools mithilfe des Assistenten 'Speicherpool hinzufügen' im Operations Center zu konfigurieren, verwenden Sie die folgenden Werte für die Parameter:
  - o Cloudtyp: `OpenStack Swift`
  - o Benutzername: `OS-Tenantname:OS-Benutzername`
  - o Kennwort: `OS-Kennwort`
  - o URL: `OS-Authentifizierungs-URL`
4. Wenn Sie planen, Speicherpools mithilfe des Befehls `DEFINE STGPOOL` zu konfigurieren, verwenden Sie die folgenden Werte für die Befehlsparameter:
  - o `CLOUDTYPE`: `SWIFT` oder `V1SWIFT`
  - o `IDENTITY`: `OS-Tenantname:OS-Benutzername`
  - o `PASSWORD`: `OS-Kennwort`
  - o `CLOUDURL`: `OS-Authentifizierungs-URL`
5. Wenn Sie planen, einen bestimmten Tenant- oder Benutzernamen zu verwenden, notieren Sie die Werte in folgendem Format:  
`Tenantname:Benutzername`.
6. Um einen Datenverlust zu verhindern, konfigurieren OpenStack Swift zum Erstellen von Replikaten der Daten, die in den OpenStack Swift-Objektspeicher geschrieben werden. Weitere Informationen enthält die OpenStack Swift-Dokumentation.

---

## Nächste Schritte

Konfigurieren Sie Cloud-Containerspeicherpools für OpenStack Swift, indem Sie die Anweisungen in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren ausführen.

---

## Daten für Cloud-Containerspeicherpools verschlüsseln

Daten, die in Off-Premises-Cloud-Container-Pools gespeichert werden, werden standardmäßig verschlüsselt. Daten in On-Premises-Cloud-Containerspeicherpools können wahlweise verschlüsselt werden.

---

## Informationen zu diesem Vorgang

Informationen zum Verschlüsseln von Daten in Cloud-Containerspeicherpools und zu Leistungsaspekten bei der Verschlüsselung von Daten, finden Sie in der Technote 1963635.

---

## Speicherregel für Cloud-Tiering definieren

Sie können eine Speicherregel für die Implementierung von Cloud-Tiering definieren, mit dem Daten aus einem Verzeichniscontainerspeicherpool auf Platte in einen Cloud-Containerspeicherpool versetzt werden. Mithilfe der Speicherregel wird das Cloud-Tiering aus Verzeichniscontainerspeicherpools in Cloud-Containerspeicherpools geplant.

---

## Informationen zu diesem Vorgang

Sie können Speicherregeln definieren, um die folgenden Anforderungen anzugeben:

- Den Zeitraum, den Daten in Containerspeicherpools auf Platte verbleiben, bevor sie in Cloudspeicher versetzt werden.
- Die Angabe, ob eine Speicherregel aktiv oder inaktiv ist. Speicherregeln werden täglich zu einem in der Speicherregel definierten Zeitpunkt ausgeführt.

---

## Vorgehensweise

1. Klicken Sie in der Menüleiste des Operations Center auf Speicher > Tiering-Regeln.
2. Klicken Sie auf der Seite Speicherregeln für Tiering auf Regel erstellen.
3. Füllen Sie auf der Seite Regel erstellen die Felder aus und klicken Sie auf Erstellen.

---

## Ergebnisse

Wenn die Speicherregel aktiv ist, bestimmt der Server, ob die Quellenverzeichniscontainerpools Daten enthalten, die alt genug für die Versetzung sind. Der Server versetzt auswählbare Daten in die Ziel-Cloud-Containerspeicherpools.

## Leistung für Cloudobjektspeicher optimieren

---

Sie können IBM Spectrum Protect so konfigurieren, dass Daten während der Datenaufnahme vorübergehend in einem oder mehreren lokalen Speicherpoolverzeichnissen gespeichert werden. Die Daten werden dann aus dem lokalen Speicher in die Cloud übertragen. Auf diese Art und Weise können Sie die Datensicherungs- und -archivierungsleistung verbessern.

### Vorbereitende Schritte

---

Um die Sicherungs- und Archivierungsleistung zu optimieren, müssen Sie sicherstellen, dass IBM Spectrum Protect Version 8.1 installiert ist.

### Informationen zu diesem Vorgang

---

Nachdem Sie ein Speicherpoolverzeichnis definiert haben, verwendet der IBM Spectrum Protect-Server dieses Verzeichnis als temporären Speicherplatz für die Daten, die Sie in den Cloudobjektspeicher übertragen. Der Server verwendet einen automatisierten Hintergrundprozess, um die Daten aus dem lokalen Speicher im Verzeichnis in den Cloudobjektspeicher zu übertragen. Sie müssen keine zusätzlichen Schritte ausführen, um diesen Übertragungsprozess zu starten oder zu verwalten. Nachdem der Server die Daten erfolgreich aus dem lokalen Speicher in den Cloudobjektspeicher übertragen hat, löscht der Server die Daten aus dem Verzeichnis und gibt Speicherbereich für weitere ankommende Daten frei.

Wenn Speicherpoolverzeichnisse keinen freien Speicherbereich mehr enthalten, werden Sicherungsoperationen vorzeitig gestoppt. Um diese Situation zu vermeiden, können Sie weitere Speicherpoolverzeichnisse zuordnen. Sie können auch warten, bis die Daten nach der Übertragung in die Cloud automatisch aus den lokalen Verzeichnissen entfernt werden. Die erforderliche Anzahl Speicherpoolverzeichnisse, die Sie definieren müssen, ist von Ihrer Plattenkonfiguration auf dem Server abhängig. Wenn die Erstsicherung erfolgt, verteilt der Server die Daten über alle definierten Verzeichnisse.

Der Umfang des Speicherbereichs, der für lokalen Speicher benötigt wird, basiert auf dem erwarteten Datenvolumen nach der Datenduplizierung und Komprimierung, das täglich gesichert werden muss. Wenn Sie über eine stabile Netzverbindung zum Cloudobjektspeicher verfügen, entspricht der erforderliche Speicherbedarf in etwa dem für eine tägliche Sicherung erforderlichen Speicherbereich.

Zusätzliche Planungsinformationen finden Sie in dem Abschnitt für Ihr Betriebssystem:

- AIX: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools
- Linux: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools
- Windows: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools




### Vorgehensweise

---

1. Erstellen Sie einen Cloud-Containerspeicherpool mithilfe des Assistenten 'Speicherpool hinzufügen' im Operations Center. Es ist auch möglich, den Pool mithilfe des Befehls `DEFINE STGPOOL` zu erstellen.
2. Definieren Sie ein oder mehrere Speicherpoolverzeichnisse mithilfe des Befehls `DEFINE STGPOOLDIRECTORY`. Stellen Sie sicher, dass jedes Speicherpoolverzeichnis sein eigenes Dateisystem hat. Verwenden Sie auf Linux-Systemen das `xfs-` oder `ext4-` Dateisystem statt des `ext3-` Dateisystems, da das Löschen großer Dateien bei `ext3` länger dauert. Stellen Sie sicher, dass die neuen Speicherpoolverzeichnisse weder das Stammdateisystem noch dieselben Dateisysteme gemeinsam nutzen, die von anderen IBM Spectrum Protect-Ressourcen, wie beispielsweise der Datenbank oder den Protokollen, verwendet werden.

#### Zugehörige Verweise:

`DEFINE STGPOOLDIRECTORY` (Speicherpoolverzeichnis definieren)

## Speicherbereich in Containerspeicherpools verwalten

---

Nachdem Sie IBM Spectrum Protect konfiguriert und Speicherbereich hinzugefügt haben, müssen Sie Ihre Daten und Ihren Speicherbereich im Speicherpool effektiv verwalten, um die ordnungsgemäße Funktion zu gewährleisten. Maximieren Sie Ihren Speicherbereich und die Serverleistung mithilfe von Containerspeicherpools.

### Informationen zu diesem Vorgang

---

Containerspeicherpools sind primäre Speicherpools, die für Inline-Datenduplizierung, Inline-Komprimierung und Cloudspeicher verwendet werden.

Einschränkung: Folgende Funktionen können bei Containerspeicherpools nicht verwendet werden:

- Umlagerung

- Konsolidierung
- Zusammenfassung
- Kollokation
- Export
- Import
- Gleichzeitiges Schreiben
- Speicherpoolsicherung
- Virtuelle Datenträger

## Vorgehensweise

- Erstellen Sie einen Verzeichniscontainerspeicherpool, indem Sie die folgenden Schritte ausführen:
  - Öffnen Sie das Operations Center.
  - Klicken Sie in der Menüleiste des Operations Center auf Speicher > Speicherpools.
  - Klicken Sie auf +Speicherpool.
  - Führen Sie die Schritte im Assistenten Speicherpool hinzufügen aus:
    - Um die Inline-Dateneduplizierung verwenden zu können, wählen Sie einen Speicherpool Verzeichnis unter dem containerbasierten Speicher aus.
    - Wenn Sie Verzeichnisse für den Verzeichniscontainerspeicherpool konfigurieren, geben Sie die Verzeichnispfade an, die während der Systemkonfiguration für Speicher erstellt wurden.
  - Klicken Sie nach dem Konfigurieren des neuen Verzeichniscontainerspeicherpools auf Schließen & Maßnahmen anzeigen, um eine Verwaltungsklasse zu aktualisieren und mit der Verwendung des Speicherpools zu beginnen.
- Um eine optimale Leistung bei Containerspeicherpools zu erzielen, führen Sie die folgenden Tasks aus:

| Task                    | Prozedur  | Weitere Informationen   |
|-------------------------|---|---|
| Speicherpool schützen   | <p>Wenn Sie im Operations Center einen Verzeichniscontainerspeicherpool erstellen, können Sie Speicherpoolschutz in dem Zeitplan konfigurieren, den Sie dem Speicherpool zuordnen.</p> <p>Sie können auch stattdessen den Befehl PROTECT STGPOOL auf dem Quellenserver verwenden, um Datenbereiche in einem Verzeichniscontainerspeicherpool zu sichern.</p> <p>Indem ein Speicherpool geschützt wird, werden keine Ressourcen verwendet, die vorhandene Daten und Metadaten replizieren, wodurch die Serverleistung verbessert wird.</p> | <ul style="list-style-type: none"> <li>○ Daten in Verzeichniscontainerspeicherpools schützen</li> <li>○ PROTECT STGPOOL (Daten schützen, die zu einem Speicherpool gehören)</li> </ul>                                    |
| Speicherpool reparieren | <p>Wenn ein Speicherpool geschützt ist, können Sie beschädigte Datenbereiche mit dem Befehl REPAIR STGPOOL reparieren. Verwenden Sie den Befehl REPAIR STGPOOL, um einen Verzeichniscontainerspeicherpool zu reparieren.</p> <p>Einschränkung: Wenn Sie Clientknoten replizieren, den Verzeichniscontainerspeicherpool aber nicht schützen, können Sie den Speicherpool nicht reparieren.</p>   | <ul style="list-style-type: none"> <li>○ Speicherpools reparieren</li> <li>○ REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)</li> </ul>  |
| Container löschen       | <p>Container werden im Bestand gelöscht, wenn Dateidaten entfernt werden oder verfallen.</p> <p>Steuern Sie mithilfe des Befehls DEFINE STGPOOL unter Angabe des Parameters REUSEDELAY, wie lange deduplizierte Speicherbereiche einem Verzeichniscontainerspeicherpool</p>   | <ul style="list-style-type: none"> <li>○ DEFINE STGPOOL (Verzeichniscontainerspeicherpool definieren)</li> <li>○ AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)</li> </ul> |

|  |  |   |
|--|--|---|
|  | zugeordnet bleiben, nachdem sie nicht mehr referenziert werden.<br><br>Wenn ein Container beschädigt ist, verwenden Sie den Befehl <code>AUDIT CONTAINER</code> , um Daten wiederherzustellen oder zu entfernen.   |   |
| Einen primären Speicherpool, der eine Einheitenklasse FILE, eine Bänderklassenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet, konvertieren | Sie können einen vorhandenen Speicherpool in einen Verzeichniscontainerspeicherpool konvertieren, indem Sie die Schritte in Primären Speicherpool in einen Containerspeicherpool konvertieren ausführen.<br>Einschränkung: Die folgenden Speicherpooltypen können nicht konvertiert werden: <ul style="list-style-type: none"> <li>○ Primäre Speicherpools, die Einheitenklassen für Einheiten mit wahlfreiem Zugriff (DISK) verwenden</li> <li>○ Kopierspeicherpools</li> <li>○ Speicherpools für aktive Daten</li> </ul> | <ul style="list-style-type: none"> <li>○ <code>CONVERT STGPOOL</code> (Speicherpool in einen Containerspeicherpool konvertieren)</li> </ul> |
| Containerspeicherpoolbelegung überwachen   | Überwachen Sie die Speicherlösung, um vorhandene und potenzielle Probleme zu ermitteln. Weitere Informationen finden Sie in Speicherlösungen überwachen.   |   |

- Primären Speicherpool in einen Containerspeicherpool konvertieren  
Konvertieren Sie einen primären Speicherpool, der eine Einheitenklasse FILE, eine Bänderklassenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet, in einen Containerspeicherpool. Daten, die in einem Containerspeicherpool gespeichert sind, können sowohl die Inline-Datendeduplizierung als auch die Inline-Komprimierung verwenden.
- Daten in einem Quellenspeicherpool bereinigen  
Um einen Speicherpool in einen Verzeichniscontainerspeicherpool zu konvertieren, müssen Sie gegebenenfalls beschädigte Daten oder Dateien bereinigen, die sich im Quellenspeicherpool befinden.

## Primären Speicherpool in einen Containerspeicherpool konvertieren

Konvertieren Sie einen primären Speicherpool, der eine Einheitenklasse FILE, eine Bänderklassenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet, in einen Containerspeicherpool. Daten, die in einem Containerspeicherpool gespeichert sind, können sowohl die Inline-Datendeduplizierung als auch die Inline-Komprimierung verwenden.

### Vorbereitende Schritte

Um sicherzustellen, dass Datenträger in einem Quellenspeicherpool und zugehörigen Kopierspeicherpools während eines Konvertierungsprozesses nicht wiederverwendet werden, geben Sie für den Parameter `REUSEDELAY` im Befehl `UPDATE STGPOOL` einen Wert an. Geben Sie für den Parameter `REUSEDELAY` einen Wert an, der größer als der Wert für die Konvertierungsdauer ist. Möglicherweise müssen Sie die Wiederverwendung von Datenträgern aus den folgenden Gründen verzögern:

- Die Daten werden während der Speicherpoolkonvertierung versehentlich gelöscht.
- Es ist Quellenspeicherpoolfunktionalität erforderlich, die in Containerspeicherpools nicht verfügbar ist.

Tipp: Wenn Sie den Parameter `REUSEDELAY` angeben, während eine Konvertierungsoperation in Bearbeitung ist, ist ein Teil des Speicherbereichs im Quellenspeicherpool erst wieder verfügbar, wenn die durch den Wert für den Parameter angegebene Zeit abläuft. Erstellen Sie einen Containerspeicherpool, in den die Daten versetzt werden sollen, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie auf der Seite Speicherpools im Operations Center auf + Speicherpool.
2. Führen Sie die Schritte im Assistenten 'Speicherpool hinzufügen' aus. Wählen Sie den Typ des erforderlichen containerbasierten Speichers aus.

### Informationen zu diesem Vorgang



Wenn Sie einen Speicherpool in einen Containerspeicherpool konvertieren, ist keine Datenträgerkonsolidierung erforderlich. Das Entfallen von Datenträgerkonsolidierungsoperationen kann dazu beitragen, die Serverleistung zu verbessern und den Umfang der erforderlichen Speicherhardware zu reduzieren.

Beim Konvertieren von Dateien werden alle in Kopienpools oder Pools für aktive Daten gespeicherten Kopien gelöscht. Einschränkungen:

- Wenn der Quellenpool in einer aktiven Maßnahmengruppe als Sicherungs-, Archivierungs- oder Umlagerungsziel mit anstehenden Änderungen angegeben ist, müssen Sie diese Änderungen aktivieren, bevor Sie den Pool konvertieren können.
- Um sicherzustellen, dass das Ziel einen Speicherpool angibt, der nicht konvertiert wurde bzw. gerade konvertiert wird, müssen Sie alle Maßnahmen aktualisieren, die den Quellenspeicherpool referenzieren.
- Wenn der Quellenspeicherpool als nächster Speicherpool angegeben ist, müssen Sie den Parameter NEXTSTGPOOL im Befehl UPDATE STGPOOL aktualisieren, um einen Speicherpool mit wahlfreiem oder sequenziellem Zugriff anzugeben, der nicht gerade konvertiert wird.
- Die folgenden Datentypen sind für die Konvertierung nicht auswählbar: Sicherungen von Inhaltsverzeichnissen (TOC-Sicherungen), virtuelle Datenträger und Network Data Management Protocol-Daten (NDMP-Daten). Bevor Sie den Konvertierungsprozess starten, müssen Sie diese Datentypen manuell aus dem Speicherpool löschen und die Datentypen in einen anderen primären Speicherpool versetzen oder die Datentypen müssen auf der Basis von Maßnahmeneinstellungen verfallen können.
- Wenn Sie einen Speicherpool mit einer Einheitenklasse FILE in einen Verzeichniscontainerpool konvertieren, sollte der Zielspeicherpool ungefähr 30 % größer als der Quellenspeicherpool sein. Zusätzlicher Speicherbereich ist in der Regel nicht erforderlich, wenn Sie andere Speicherpooltypen konvertieren.

Weitere Informationen zu Best Practices für die Speicherpoolkonvertierung finden Sie in Best practices for IBM Spectrum Protect storage pool conversion.

- Wenn der Quellenspeicherpool zum Speichern von TOC-Sicherungen verwendet wird, stellen Sie sicher, dass ein weiterer primärer Speicherpool zum Speichern neuer TOC-Sicherungen verfügbar ist. Vorhandene TOC-Sicherungen werden im Rahmen der Konvertierung nicht versetzt.

Der TOC-Pool muss das Datenformat NATIVE oder NONBLOCK und eine andere Einheitenklasse als Centera haben. Verwenden Sie die Einheitenklasse DISK oder FILE, um Mountverzögerungen zu verhindern.

## Vorgehensweise

---

1. Wählen Sie auf der Seite Speicherpools im Operations Center einen Speicherpool aus, der eine Einheitenklasse FILE, eine Bändeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet.
2. Klicken Sie auf Weitere > Konvertieren und führen Sie die Schritte im Assistenten 'Speicherpool konvertieren' aus.  
Tipp: Planen Sie für die Konvertierung eines Speicherpools, der eine Einheitenklasse FILE verwendet, mindestens 2 Stunden ein und für die Konvertierung eines Speicherpools, der ein VTL verwendet, mindestens 4 Stunden.

## Nächste Schritte

---

Wenn der Konvertierungsprozess abgeschlossen ist, kann der Quellenspeicherpool unter Umständen beschädigte Daten oder Daten enthalten, die mit Containerspeicherpools inkompatibel sind. Bereinigen Sie den Quellenspeicherpool, indem Sie die Schritte in Objekte in einem Quellenspeicherpool bereinigen ausführen.

### Zugehörige Tasks:

Datenbank zurückschreiben

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Daten in einem Quellenspeicherpool bereinigen

---

Um einen Speicherpool in einen Verzeichniscontainerspeicherpool zu konvertieren, müssen Sie gegebenenfalls beschädigte Daten oder Dateien bereinigen, die sich im Quellenspeicherpool befinden.

## Vorgehensweise

---

Verwenden Sie die folgenden Optionen, um beschädigte Daten wiederherzustellen oder zu reparieren.

- Stellen Sie eine unbeschädigte Version der Daten aus einem Kopien Speicherpool oder Speicherpool für aktive Daten wieder her, indem Sie den Befehl RESTORE STGPOOL ausgeben.
- Stellen Sie eine unbeschädigte Version der Daten von einem Zielreplikationsserver wieder her, indem Sie den Befehl REPLICATE NODE unter Angabe des Parameters RECOVERDAMAGED=YES ausgeben.

- Entfernen Sie Daten, die nicht repariert werden können, nach der Speicherpoolkonvertierung, indem Sie den Befehl REMOVE DAMAGED ausgeben.  
Mit dem Befehl REMOVE DAMAGED werden möglicherweise keine Datenträger entfernt, die im Quellenspeicherpool als dauerhaft beschädigt markiert sind. Um diese Datenträger zu entfernen, führen Sie die folgenden Schritte aus:
  - a. Geben Sie den Befehl DELETE VOLUME unter Angabe des Parameters DISCARDDATA=YES aus.
  - b. Geben Sie den Befehl CONVERT STGPOOL aus, um den Speicherpool erneut zu konvertieren.
  - c. Wenn während der Speicherpoolkonvertierung beschädigte Daten erkannt werden, geben Sie den Befehl REMOVE DAMAGED erneut aus.
- Führen Sie die in der Technote 1666371 beschriebenen Analysetasks aus.

## Nächste Schritte

---

Nachdem Sie die beschädigten Daten wiederhergestellt oder repariert haben, wiederholen Sie die Konvertierung, indem Sie den Befehl CONVERT STGPOOL ausgeben.

Um Informationen zu beschädigten Dateien anzuzeigen, die im Quellenspeicherpool verblieben sind, geben Sie den Befehl QUERY CLEANUP aus.

Tipp: Wenn für einen Speicherpool, der keine Daten enthält, ein Bereinigungsstatus angezeigt wird, können Sie den Speicherpool mit dem Befehl DELETE STGPOOL löschen.

### Zugehörige Verweise:

DELETE VOLUME (Speicherpooldatenträger löschen)

QUERY CLEANUP (In einem Quellenspeicherpool erforderliche Bereinigung abfragen)

REMOVE DAMAGED (Beschädigte Daten aus einem Quellenspeicherpool entfernen)

REPLICATE NODE (Daten in Dateibereichen replizieren, die zu einem Clientknoten gehören)

RESTORE STGPOOL (Speicherpooldaten aus einem Kopienpool oder einem Pool für aktive Daten zurückschreiben)

## Speicherpoolcontainer prüfen

---

Mit der Prüfung eines Speicherpoolcontainers wird auf Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Speicherpool geprüft.

## Informationen zu diesem Vorgang

---

Sie prüfen einen Speicherpoolcontainer in den folgenden Situationen:

- Sie geben den Befehl QUERY DAMAGED aus und es wird ein Problem erkannt.
- Der Server zeigt Nachrichten zu beschädigten Datenbereichen an.
- Ihre Hardware meldet ein Problem und es werden Fehlernachrichten angezeigt, die sich auf den Speicherpoolcontainer beziehen.

## Vorgehensweise

---

1. Um einen Speicherpoolcontainer zu prüfen, geben Sie den Befehl AUDIT CONTAINER aus. Geben Sie beispielsweise den folgenden Befehl aus, um den Container 000000000000076c.dcf zu prüfen:

```
audit container c:\tsm-storage\07\000000000000076c.dcf
```

2. Überprüfen Sie die Ausgabe der Nachricht ANR4891I auf Informationen zu allen beschädigten Datenbereichen.

## Nächste Schritte

---

Wenn Sie Probleme mit dem Speicherpoolcontainer erkennen, können Sie Daten auf der Basis Ihrer Konfiguration zurückschreiben. Sie können den Inhalt des Speicherpools mit dem Befehl REPAIR STGPOOL reparieren.

Einschränkung: Sie können den Inhalt des Speicherpools nur reparieren, wenn der Speicherpool mit dem Befehl PROTECT STGPOOL geschützt wurde.

### Zugehörige Verweise:

➤ AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)

➤ QUERY DAMAGED (Beschädigte Daten in einem Verzeichniscontainer- oder Cloud-Containerspeicherpool abfragen)

## Speichersystemvoraussetzungen und Reduzierung des Risikos fehlerhafter Daten

---

Für den IBM Spectrum Protect-Server können viele Typen von Speicher verwendet werden. Wenn Sie Plattenblockspeicher, Solid-State-Laufwerke (SSDs) oder an das Netz angeschlossene Dateisysteme als Serverspeicher verwenden, müssen Sie sicherstellen, dass der Speicher die Voraussetzungen erfüllt.

Die folgenden Voraussetzungen gelten für Speicher für die Serverdatenbank, die aktive Protokolldatei und das Archivprotokoll sowie für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden, und für Verzeichniscontainerspeicherpools.

Speicher kann mit jeder Methode, die für das Betriebssystem gültig ist, an das Serversystem angeschlossen werden. Beispielsweise kann der Speicher direkt angeschlossen werden oder unter Verwendung der Fibre Channel- oder iSCSI-Technologie.

Da viele Speichersysteme die Voraussetzungen für Serverspeicher erfüllen können, ist eine Liste derartiger Einheiten nicht verfügbar. Wenden Sie sich an den Hersteller, wenn Sie nicht wissen, ob ein System die IBM Spectrum Protect-Voraussetzungen erfüllt.

Ausführliche Informationen zu Dateisystemvoraussetzungen enthält die Technote 1902417. Ausführliche Informationen zu NFS-Voraussetzungen enthält die Technote 1470193.

Speicher- und Dateisysteme müssen Schreib- und Festschreibergebnisse synchron und korrekt an den IBM Spectrum Protect-Server zurückmelden. Nicht zurückgemeldete oder asynchron zurückgemeldete Schreibfehler, die zur Folge haben, dass Daten nicht permanent im Speichersystem festgeschrieben werden, können fehlerhafte Daten zur Folge haben. Fehlerhafte Daten können betriebsbezogene Fehler verursachen, einschließlich des Fehlschlagens, den Server starten zu können, und erfordern in der Regel eine Datenwiederherstellung.

Die folgenden Informationen enthalten Tipps, wie das Risiko fehlerhafter Daten verringert werden kann:

#### Schreibcache

Plattensysteme verwenden Schreibcache zur Verbesserung der Systemleistung. Um das Risiko fehlerhafter Daten zu verringern, muss das Speichersystem die Daten im Schreibcache zuverlässig in permanentem Speicher festschreiben.

Der Schreibcache verfügt normalerweise über eine Batterie, um den Verlust von Daten im Cache während eines kurzen Stromausfalls zu verhindern. Bei kritischen Systemen sollten Sie die Bereitstellung einer Notstromversorgung in Erwägung ziehen, um den Cache bei längeren Stromausfällen zu schützen.

#### Direkte E/A

Die direkte E/A erfüllt die Anforderungen des Servers in Bezug auf das synchrone und korrekte Zurückmelden bei Schreib- und Festschreibungsoperationen für Daten.

Achtung: Sie dürfen die direkte E/A nicht in Situationen inaktivieren, in denen das Schreibcaching einen Datenverlust zur Folge haben könnte. Das Inaktivieren der direkten E/A kann die Wahrscheinlichkeit eines Datenverlusts stark erhöhen, da zusätzlich zum Plattensystem mehr Daten vom Dateisystem zwischengespeichert werden.

#### Speicherreplikation

Umgebungen, die IBM Spectrum Protect-Speicher replizieren, müssen Funktionen wie die Beibehaltung der Schreibreihenfolge zwischen der Quelle (dem lokalen Server) und dem Ziel (dem fernen Server) verwenden. Die Datenbank, die aktive Protokolldatei, die Archivprotokolle und die Speicherpools müssen zu einer Konsistenzgruppe gehören. Eine Konsistenzgruppe verwaltet Beziehungen zwischen Datenträgern, um die Schreibreihenfolge beizubehalten, damit eine Wiederherstellung der Datenträger möglich ist. Jede Ein-/Ausgabe für die Mitglieder der Zielkonsistenzgruppe muss in derselben Reihenfolge wie die der Quelle geschrieben werden und dieselben Volatilitätsmerkmale haben.

Um die Synchronisation zwischen IBM Spectrum Protect-Servern am lokalen und fernen Standort zu gewährleisten, dürfen Sie einen Server am fernen Standort nur in einer Übernahmesituation starten. Überwachen Sie die Synchronisation der Daten am lokalen und fernen Standort. Wenn die Synchronisation verloren geht, müssen Sie den Server am fernen Standort mithilfe von IBM Spectrum Protect-Zurückschreibungsbefehlen für die Datenbank und Speicherpools zurückschreiben.

## Tipps zur Speicherkonfiguration

---

Tipps zur Speicherkonfiguration zur Optimierung der Systemleistung liefern die folgenden Themen in der Produktdokumentation der Version 7.1.1. Die Informationen in den Prüflisten können auf höhere Releases angewendet werden.

- Prüfliste für Platten für die Serverdatenbank
- Prüfliste für Platten für das Serverwiederherstellungsprotokoll
- Prüfliste für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden

## Speicherlösungen überwachen

---

Nach der Implementierung einer IBM Spectrum Protect-Lösung müssen Sie die Lösung überwachen, um sicherzustellen, dass sie ordnungsgemäß funktioniert. Indem die Lösung täglich und regelmäßig überwacht wird, können Sie bestehende und potenzielle Probleme erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden.

## Informationen zu diesem Vorgang

---

Die bevorzugte Art und Weise zur Überwachung einer Lösung erfolgt über die Verwendung des Operations Center, das den Gesamtstatus und den detaillierten Systemstatus in einer grafischen Benutzerschnittstelle bereitstellt. Darüber hinaus können Sie das Operations Center zum Generieren von E-Mail-Berichten mit einer Zusammenfassung des Systemstatus konfigurieren.

## Vorgehensweise

1. Führen Sie tägliche Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für tägliche Überwachungstasks.
2. Führen Sie regelmäßige Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für regelmäßige Überwachungstasks.
3. Um zu überprüfen, ob Ihr System Lizenzierungsvoraussetzungen erfüllt, führen Sie die Anweisungen in Lizenz Einhaltung überprüfen aus.
4. Optional: Konfigurieren Sie E-Mail-Berichte des Systemstatus. Anweisungen finden Sie in Systemstatus mithilfe von E-Mail-Berichten verfolgen.
5. Optional: In einigen Fällen möchten Sie vielleicht erweiterte Überwachungstools verwenden, um bestimmte Überwachungs- oder Fehlerbehebungstasks auszuführen. Informationen zum Auswählen und Konfigurieren erweiterter Überwachungstools finden Sie in Überwachungstools auswählen, konfigurieren und verwenden.

## Nächste Schritte

Installieren Sie zur Unterstützung bei der Diagnose von Problemen bei Clients für Sichern/Archivieren die IBM Spectrum Protect-Clientverwaltungsservices auf den Systemen des Clients für Sichern/Archivieren, die diese unterstützen. Wenn der Clientverwaltungsservice auf einem System installiert ist, können Sie im Operations Center auf Diagnose klicken, um Hilfe bei der Diagnose von Problemen beim Client für Sichern/Archivieren anzufordern. Um den Clientverwaltungsservice zu installieren, führen Sie die Anweisungen in Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen aus.

### Zugehörige Konzepte:

Leistung

### Zugehörige Tasks:

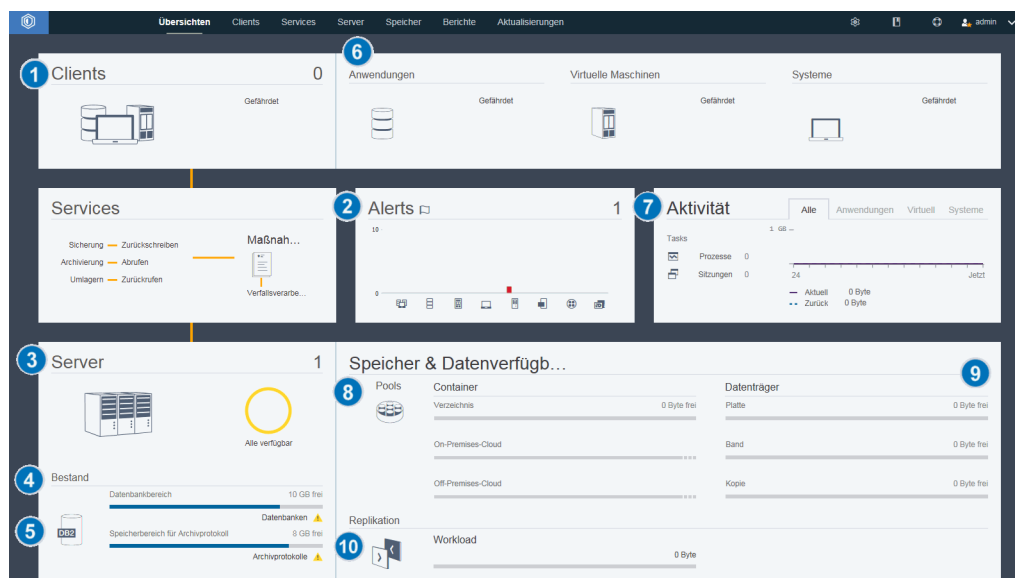
Fehlerbehebung


## Prüfliste für tägliche Überwachungstasks

Überprüfen Sie die Prüfliste, um sicherzustellen, dass wichtige tägliche Überwachungstasks ausgeführt werden.

Führen Sie die täglichen Überwachungstasks über die Seite Übersicht im Operations Center aus. Sie können auf die Seite Übersicht zugreifen, indem Sie das Operations Center öffnen und auf Übersichten klicken.

Die folgende Abbildung zeigt die Position zur Ausführung der jeweiligen Task.









Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen  und klicken Sie auf Command Builder.

In der folgenden Tabelle sind die täglichen Überwachungstasks sowie Anweisungen zur Ausführung jeder Task aufgeführt.

Tabelle 1. Tägliche Überwachungstasks



| Task   | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen  |
|--|--|---|
| <p><b>1</b> Bestimmen Sie, ob Clients vorhanden sind, bei denen die Gefahr besteht, dass sie aufgrund fehlgeschlagener oder versäumter Sicherungsoperationen ungeschützt sind.</p> | <p>Um zu überprüfen, ob Clients gefährdet sind, suchen Sie nach einem Hinweis Gefährdet. Um Details anzuzeigen, klicken Sie auf den Bereich 'Clients'.</p> <p>Achtung: Wenn der Prozentsatz für Gefährdet sehr viel höher als üblicherweise ist, kann dies eine Ransomware-Attacke anzeigen. Eine Ransomware-Attacke kann das Fehlschlagen von Sicherungsoperationen zur Folge haben und somit Clients in den Status 'Gefährdet' versetzen. Wenn beispielsweise der Prozentsatz gefährdeter Clients normalerweise zwischen 5 % und 10 % liegt, sich aber auf 40 % oder 50 % erhöht, ermitteln Sie die Ursache.</p> <p>Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie die Clientfehler- und -planungsprotokolle anzeigen, indem Sie die folgenden Schritte ausführen:</p> <ol style="list-style-type: none"> <li>1. Wählen Sie in der Tabelle 'Clients' den Client aus und klicken Sie auf Details.</li> <li>2. Um ein Problem zu diagnostizieren, klicken Sie auf Diagnose.</li> </ol> | <p>Greifen Sie bei Clients, für die der Clientverwaltungsservice nicht installiert ist, auf das Clientsystem zu, um die Clientfehlerprotokolle zu überprüfen.</p>   |
| <p><b>2</b> Bestimmen Sie, ob clientbezogene oder serverbezogene Fehler einen Bedieneingriff erfordern.</p>  | <p>Um die Bewertung jedes zurückgemeldeten Alerts zu bestimmen, bewegen Sie den Mauszeiger im Bereich 'Alerts' über die Spalten.</p>   | <p>Um weitere Informationen zu Alerts anzuzeigen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf den Bereich 'Alerts'.</li> <li>2. Wählen Sie in der Tabelle 'Alerts' einen Alert aus.</li> <li>3. Überprüfen Sie die Nachrichten im Fenster 'Aktivitätenprotokoll'. Im Fenster werden zugehörige Nachrichten angezeigt, die vor und nach dem Auftreten des ausgewählten Alerts ausgegeben wurden.</li> </ol> |
| <p><b>3</b> Bestimmen Sie, ob die vom Operations Center verwalteten Server verfügbar sind, um Datenschutzservices für Clients bereitzustellen.</p>                                 | <ol style="list-style-type: none"> <li>1. Um zu überprüfen, ob Server gefährdet sind, suchen Sie im Bereich 'Server' nach einem Hinweis Nicht verfügbar.</li> <li>2. Um zusätzliche Informationen anzuzeigen, klicken Sie auf den Bereich 'Server'.</li> <li>3. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details.</li> </ol>  | <p> Tipp: Wenn Sie ein Problem erkennen, das sich auf die Servermerkmale bezieht, aktualisieren Sie die Servermerkmale:</p> <ol style="list-style-type: none"> <li>1. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details.</li> <li>2. Um die Servermerkmale zu aktualisieren, klicken Sie auf Merkmale.</li> </ol>   |



| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|---|--|--|
| <p><b>4</b> Bestimmen Sie, ob für den Serverbestand, der aus der Serverdatenbank, der aktiven Protokolldatei und dem Archivprotokoll besteht, genügend Speicherbereich verfügbar ist.</p> | <ol style="list-style-type: none"> <li>1. Klicken Sie auf den Bereich 'Server'.</li> <li>2. Zeigen Sie in der Spalte 'Status' der Tabelle den Status des Servers an und beheben Sie alle Probleme: <ul style="list-style-type: none"> <li>o Normal  Für die Serverdatenbank, die aktive Protokolldatei und das Archivprotokoll ist genügend Speicherbereich verfügbar.</li> <li>o Kritisch  Für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll ist nicht genügend Speicherbereich verfügbar. Sie müssen unverzüglich Speicherbereich hinzufügen; andernfalls werden die vom Server bereitgestellten Datenschutzservices unterbrochen.</li> <li>o Warnung  Der Speicherbereich für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll wird knapp. Wenn diese Bedingung bestehen bleibt, müssen Sie Speicherbereich hinzufügen.</li> <li>o Nicht verfügbar  Der Status kann nicht abgerufen werden. Stellen Sie sicher, dass der Server aktiv ist und keine Netzprobleme vorliegen. Dieser Status wird auch angezeigt, wenn die Überwachungsadministrator-ID gesperrt ist oder aus anderen Gründen auf dem Server nicht verfügbar ist. Diese ID hat den Namen IBM-OC-Name_des_Hub-Servers.</li> <li>o Nicht überwacht  Nicht überwachte Server sind für den Hub-Server definiert, aber nicht für die Verwaltung durch das Operations Center konfiguriert. Um einen nicht überwachten Server zu konfigurieren, wählen Sie den Server aus und klicken Sie auf Peripherieserver überwachen.</li> </ul> </li> </ol> | <p>Sie können auch auf der Seite Alerts nach zugehörigen Alerts suchen. Weitere Anweisungen zur Fehlerbehebung finden Sie in Serverprobleme beheben.</p> |


| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen  |
|---|--|---|
| <p><b>5</b> Überprüfen Sie Operationen zur Sicherung der Serverdatenbank.</p>   | <p>Um zu bestimmen, ob ein Server kürzlich gesichert wurde, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf den Bereich 'Server'.</li> <li>2. Überprüfen Sie in der Tabelle 'Server' die Spalte 'Letzte Datenbanksicherung'.</li> </ol>   | <p>Um detaillierte Informationen zu Sicherungsoperationen abzurufen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Wählen Sie in der Tabelle 'Server' eine Zeile aus und klicken Sie auf Details.</li> <li>2. Bewegen Sie im Bereich 'Datenbanksicherung' den Mauszeiger über die Häkchen, um Informationen zu Sicherungsoperation zu überprüfen.</li> </ol> <p>Wenn eine Datenbank nicht kürzlich (beispielsweise innerhalb der letzten 24 Stunden) gesichert wurde, können Sie eine Sicherungsoperation starten:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Server'.</li> <li>2. Wählen Sie in der Tabelle einen Server aus und klicken Sie auf Sichern.</li> </ol> <p>Um zu bestimmen, ob die Serverdatenbank für automatische Sicherungsoperationen konfiguriert ist, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>2. Geben Sie den Befehl QUERY DB aus: <pre>query db f=d</pre> </li> <li>3. Überprüfen Sie in der Ausgabe das Feld <code>Einheitenklassenname</code> für Gesamtsicherungen. Wenn eine Einheitenklasse angegeben ist, ist der Server für automatische Datenbanksicherungen konfiguriert.</li> </ol> |
| <p><b>6</b> Überwachen Sie andere Serververwaltungstasks. Serververwaltungstasks können die Ausführung von Zeitplänen für Verwaltungsbefehle, Verwaltungsscripts und zugehörigen Befehlen umfassen.</p> | <p>Um nach Informationen zu Prozessen zu suchen, die aufgrund von Serverproblemen fehlgeschlagen sind, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf Server &gt; Verwaltung.</li> <li>2. Um das zwei Wochen umfassende Verlaufsprotokoll eines Prozesses abzurufen, zeigen Sie Spalte 'History' an.</li> <li>3. Um weitere Informationen zu einem geplanten Prozess abzurufen, bewegen Sie den Mauszeiger über das Kontrollkästchen, das dem Prozess zugeordnet ist.</li> </ol> | <p>Weitere Informationen zum Überwachen von Prozessen und Beheben von Problemen, finden Sie in der Onlinehilfe des Operations Center.</p>   |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|---|--|--|
| <p><b>7</b> Überprüfen Sie, ob das Datenvolumen, das kürzlich an Server bzw. von Servern gesendet wurde, innerhalb des erwarteten Bereichs liegt.</p> | <ul style="list-style-type: none"> <li>• Um eine Übersicht über die Aktivität der letzten 24 Stunden abzurufen, zeigen Sie den Bereich 'Aktivität' an.</li> <li>• Um die Aktivität der letzten 24 Stunden mit der Aktivität der vorherigen 24 Stunden zu vergleichen, studieren Sie die Zahlen in den Bereichen 'Aktuell' und 'Vorherig'.</li> </ul> | <ul style="list-style-type: none"> <li>• Wenn mehr Daten als erwartet an den Server gesendet wurden, bestimmen Sie die Clients, die mehr Daten sichern und ermitteln Sie die Ursache. Möglicherweise funktioniert die clientseitige Datendeduplizierung nicht ordnungsgemäß.<br/>Achtung: Wenn das Volumen gesicherter Daten deutlich umfangreicher als üblicherweise ist, kann dies eine Ransomware-Attacke anzeigen. Wenn Daten durch Ransomware verschlüsselt werden, werden die Daten vom System als geändert wahrgenommen und die geänderten Daten werden gesichert. Demzufolge wird das Volumen gesicherter Daten umfangreicher. Um die betroffenen Clients zu bestimmen, klicken Sie auf die Registerkarten Anwendungen, Virtuell oder Systeme.</li> <li>• Wenn weniger Daten als erwartet an den Server gesendet wurden, überprüfen Sie, ob Clientsicherungsoperationen gemäß Zeitplan ausgeführt werden.</li> </ul> |



| Task   | Basisprozeduren   | Erweiterte Prozeduren und Fehlerbehebungsinformationen  |
|--|---|---|
| <p><b>8</b> Stellen Sie sicher, dass Speicherpools zum Sichern von Clientdaten verfügbar sind.</p> | <p>1. Wenn im Bereich 'Speicher &amp; Datenverfügbarkeit' Probleme angezeigt werden, klicken Sie auf Pools, um die Details anzuzeigen:</p> <ul style="list-style-type: none"> <li>○ Wenn der Status Kritisch  angezeigt wird, ist in dem Speicherpool nicht genügend Speicherbereich verfügbar oder der Speicherpool hat den Zugriffsstatus UNAVAILABLE (Nicht verfügbar).<br/>Achtung: Wenn der Status kritisch ist, ermitteln Sie die Ursache: <ul style="list-style-type: none"> <li>■ Wenn die Dateneduplizierungsrate für einen Speicherpool deutlich fällt, kann dies eine Ransomware-Attacke anzeigen. Während einer Ransomware-Attacke werden Daten verschlüsselt und können nicht dedupliziert werden. Um die Dateneduplizierungsrate zu verifizieren, überprüfen Sie in der Tabelle 'Speicherpools' den Wert in der Spalte 'Einsparungen in %'.</li> <li>■ Wenn ein Speicherpool wider Erwarten zu 100 % ausgelastet ist, kann dies eine Ransomware-Attacke anzeigen. Um die Auslastung zu verifizieren, überprüfen Sie den Wert in der Spalte 'Verwendete Kapazität'.<br/>Bewegen Sie den Mauszeiger über die Werte, um den Prozentsatz für den verwendeten Speicherbereich und den Prozentsatz für den freien Speicherbereich anzuzeigen.</li> </ul> </li> <li>○ Wenn der Status Warnung  angezeigt wird, wird der Speicherbereich für den Speicherpool knapp oder der Speicherpool hat den Zugriffsstatus READONLY (Lesezugriff).</li> </ul> <p>2. Um den verwendeten Speicherbereich, den freien Speicherbereich und den Gesamtspeicherbereich für Ihren ausgewählten Speicherpool anzuzeigen, bewegen Sie den Mauszeiger über die Einträge in der Spalte 'Verwendete Kapazität'.</p> | <p>Um die Speicherpoolkapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie eine Zeile in der Tabelle 'Speicherpools' aus und klicken Sie auf Details.</p> |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|---|--|--|
| <p>9 Stellen Sie sicher, dass Speichereinheiten für Sicherungsoperationen verfügbar sind.</p> | <p>Überprüfen Sie im Bereich 'Speicher &amp; Datenverfügbarkeit' im Abschnitt 'Datenträger' unterhalb der Balken für die Kapazität den Status, der neben Einheiten angegeben ist. Wenn der Status Kritisch  oder Warnung  für eine Einheit angezeigt wird, müssen Sie das Problem untersuchen. Um Details anzuzeigen, klicken Sie auf Einheiten.</p> | <p>Platteneinheiten können aus den folgenden Gründen den Status 'Kritisch' oder 'Warnung' haben:</p> <ul style="list-style-type: none"> <li>• Für Einheitenklassen DISK können Datenträger offline sein oder den Zugriffsstatus READONLY (Lesezugriff) haben. In der Spalte 'Plattenspeicher' der Tabelle 'Platteneinheiten' wird der Status der Datenträger angezeigt.</li> <li>• Für nicht gemeinsam genutzte Einheitenklassen FILE können Verzeichnisse offline sein. Außerdem ist unter Umständen nicht genügend freier Speicherbereich für die Zuordnung von Arbeitsdatenträgern verfügbar. In der Spalte 'Plattenspeicher' der Tabelle 'Platteneinheiten' wird der Status der Verzeichnisse angezeigt.</li> <li>• Für gemeinsam genutzte Einheitenklassen FILE sind Laufwerke unter Umständen nicht verfügbar. Ein Laufwerk ist nicht verfügbar, wenn es offline ist, während der Antwort an den Server gestoppt wurde oder sein Pfad offline ist. In anderen Spalten der Tabelle 'Platteneinheiten' wird der Status der Laufwerke und Pfade angezeigt.</li> </ul> <p>Bandeinheiten können den Status 'Kritisch' haben, wenn Laufwerke nicht verfügbar sind. Ein Laufwerk ist nicht verfügbar, wenn es offline ist, während der Antwort an den Server gestoppt wurde oder sein Pfad offline ist. Eine Bandeinheit kann auch den Status 'Kritisch' haben, wenn das Speicherarchiv offline ist. In anderen Spalten der Tabelle 'Bandeinheiten' wird der Status der automatischen Einheiten im Speicherarchiv, der Laufwerke und der Pfade angezeigt.</p> <p>Stellen Sie für Bandsicherungsoperationen sicher, dass genügend Arbeitsbänder verfügbar sind. Wenn Sie sich nicht sicher sind, ob die Anzahl verfügbarer Arbeitsbänder ausreichend ist, öffnen Sie das Notizbuch 'Details', um die Bandnutzung sowie eine Schätzung der Verfügbarkeit von Arbeitsbändern anzuzeigen. Um das Notizbuch 'Details' zu öffnen, wählen Sie in der Tabelle ein Speicherarchiv aus und klicken Sie auf 'Details'.</p> |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebungsinformationen   |
|---|--|--|
| <p><b>10</b> Überwachen Sie Knotenreplikationsprozesse.</p> | <ol style="list-style-type: none"> <li>Um den Gesamtstatus der Knotenreplikationsprozesse abzurufen, zeigen Sie den Bereich 'Replikation' auf der Seite Übersicht im Operations Center an.</li> <li>Um Informationen zu jedem replizierten Serverpaar anzuzeigen, klicken Sie auf den Bereich 'Replikation'.<br/>Achtung: Wenn Sie eine nicht erwartete Erhöhung der Anzahl Replikationsfehler beobachten, kann dies eine Ransomware-Attacke anzeigen. Ermitteln Sie die Fehlerursache.</li> <li>Um das Datenvolumen, das im Laufe der letzten zwei Wochen repliziert wurde, und die Geschwindigkeit der Replikation anzuzeigen, wählen Sie ein Serverpaar aus und klicken Sie auf Details.</li> <li>Um Replikationsinformationen für einen Client anzuzeigen, klicken Sie auf der Seite Übersicht im Operations Center auf Clients. Studieren Sie die Informationen in der Spalte 'Replikationsworkload'.<br/>Achtung: Wenn Sie eine drastische, nicht erwartete Erhöhung der Replikationslast beobachten, kann dies eine Ransomware-Attacke anzeigen. Ermitteln Sie die Ursache für die erhöhte Last.</li> </ol> | <p>Zeigen Sie für die erweiterte Überwachung mithilfe von Befehlen Informationen zu aktiven und beendeten Knotenreplikationsprozessen an:</p> <ol style="list-style-type: none"> <li>Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>Geben Sie den Befehl QUERY REPLICATION aus. Anweisungen finden Sie in QUERY REPLICATION (Knotenreplikationsprozesse abfragen). Wenn die Replikationsoperation erfolgreich ausgeführt wurde, stimmt der Wert für Gesamtzahl der zu replizierenden Dateien mit dem Wert für Gesamtzahl der replizierten Dateien überein.</li> </ol> <p>Um Nachrichten anzuzeigen, die sich auf einen Knotenreplikationsprozess auf einem Quellen- oder Zielreplikationsserver beziehen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>Klicken Sie auf der Seite Übersicht im Operations Center auf Server.</li> <li>Wählen Sie den Quellen- oder Zielreplikationsserver aus und klicken Sie auf Details: <ul style="list-style-type: none"> <li>Um aktive Tasks anzuzeigen, klicken Sie auf Aktive Tasks, wählen die Task aus und überprüfen, ob der Status Aktiv angezeigt wird. Ausführliche Informationen enthalten die zugehörigen Aktivitätenprotokolle.</li> <li>Um abgeschlossene Tasks anzuzeigen, klicken Sie auf Abgeschlossene Tasks, wählen die Task aus und überprüfen, ob der Status Abgeschlossen angezeigt wird. Ausführliche Informationen enthalten die zugehörigen Aktivitätenprotokolle.</li> </ul> </li> </ol> |

## Prüfliste für regelmäßige Überwachungstasks

Um sicherzustellen, dass Operationen ordnungsgemäß ausgeführt werden, führen Sie die Tasks in der Prüfliste für regelmäßige Überwachungstasks aus. Planen Sie regelmäßige Tasks häufig genug, sodass Sie potenzielle Probleme erkennen können, bevor diese wirklich problematisch werden.










Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen  und klicken Sie auf Command Builder.

Tabelle 1. Regelmäßige Überwachungstasks

| Task | Basisprozeduren | Erweiterte Prozeduren und Fehlerbehebung |
|------|-----------------|--|
|------|-----------------|--|

| Task                               | Basisprozeduren   | Erweiterte Prozeduren und Fehlerbehebung  |
|------------------------------------|---|---|
| Überwachen Sie die Systemleistung. | <p>Bestimmen Sie den für Clientsicherungsoperationen erforderlichen Zeitraum:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients. Suchen Sie den Server, der dem Client zugeordnet ist.</li> <li>2. Klicken Sie auf Server. Wählen Sie den Server aus und klicken Sie auf Details.</li> <li>3. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die in den letzten 24 Stunden abgeschlossen wurden, klicken Sie auf Abgeschlossene Tasks.</li> <li>4. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die vor mehr als 24 Stunden abgeschlossen wurden, verwenden Sie den Befehl QUERY ACTLOG. Führen Sie die Anweisungen in QUERY ACTLOG (Aktivitätenprotokoll abfragen) aus.</li> <li>5. Wenn die Dauer von Clientsicherungsoperationen zunimmt, ohne dass ein offensichtlicher Grund erkennbar ist, überprüfen Sie Ursache.</li> </ol> <p>Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie Leistungsprobleme für den Client für Sichern/Archivieren diagnostizieren, indem Sie die folgenden Schritte ausführen:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients.</li> <li>2. Wählen Sie einen Client für Sichern/Archivieren aus und klicken Sie auf Details.</li> <li>3. Um Clientprotokolle abzurufen, klicken Sie auf Diagnose.</li> </ol> | <p>Informationen zur Verkürzung der Zeit, die der Client zum Sichern von Daten auf dem Server benötigt, finden Sie in Häufig auftretende Clientleistungsprobleme lösen.</p> <p>Suchen Sie nach Leistungsengpässen. Anweisungen finden Sie in Leistungsengpässe identifizieren.</p> <p>Informationen zur Identifikation und Behebung anderer Leistungsprobleme finden Sie in Leistung.</p> |


| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung   |
|---|--|--|
| <p>Bestimmen Sie die Platteneinsparungen, die durch die Datendeduplizierung bereitgestellt werden.</p>                                  | <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf Pools.</li> <li>2. Wählen Sie einen Pool aus und klicken Sie auf Kurzübersicht.</li> <li>3. Zeigen Sie im Bereich 'Datendeduplizierung' die Zeile 'Eingesparter Speicherbereich' an.</li> </ol>   | <p>Um für die erweiterte Überwachung detaillierte Statistikdaten zu dem Datendeduplizierungsprozess für einen bestimmten Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool abzurufen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>2. Fordern Sie einen Statistikbericht an, indem Sie den Befehl GENERATE DEDUPSTATS ausgeben. Führen Sie die Anweisungen in GENERATE DEDUPSTATS (Datendeduplizierungsstatistikdaten für einen Verzeichniscontainerspeicherpool generieren) aus.</li> <li>3. Zeigen Sie den Statistikbericht an, indem Sie den Befehl QUERY DEDUPSTATS ausgeben. Führen Sie die Anweisungen in QUERY DEDUPSTATS (Datendeduplizierungsstatistikdaten abfragen) aus.</li> </ol> |
| <p>Stellen Sie sicher, dass aktuelle Sicherungsdateien für Einheitenkonfigurations- und Datenträgerprotokolldaten gesichert werden.</p> | <p>Greifen Sie auf Ihre Speicherpositionen zu, um sicherzustellen, dass die Dateien verfügbar sind. Die bevorzugte Methode ist die Sicherung der Dateien an zwei Positionen.</p> <p>Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>2. Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, geben Sie die folgenden Befehle aus: <pre>query option volhistory query option devconfig</pre> </li> <li>3. Überprüfen Sie in der Ausgabe die Spalte 'Optionseinstellung', um die Dateipositionen zu finden.</li> </ol> <p>Wenn ein Katastrophenfall eintritt, sind sowohl die Protokolldatei für Datenträger als auch die Einheitenkonfigurationsdatei für die Zurückschreibung der Serverdatenbank erforderlich.</p> |  |

| Task   | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung |
|--|--|--|
| <p>Bestimmen Sie, ob für das Instanzverzeichnisdateisystem genügend Speicherbereich verfügbar ist.</p> | <p>Stellen Sie sicher, dass im Instanzverzeichnisdateisystem mindestens 20 % freier Speicherbereich verfügbar ist. Führen Sie die für Ihr Betriebssystem zutreffende Aktion aus:</p> <ul style="list-style-type: none"> <li>•  <b>AIX-Betriebssysteme</b> Um den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus: <pre>df -g Instanzverzeichnis</pre> <p>Dabei gibt <i>Instanzverzeichnis</i> das Instanzverzeichnis an.</p> </li> <li>•  <b>Linux-Betriebssysteme</b> Um den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus: <pre>df -h Instanzverzeichnis</pre> <p>Dabei gibt <i>Instanzverzeichnis</i> das Instanzverzeichnis an.</p> </li> <li>•  <b>Windows-Betriebssysteme</b> Klicken Sie in Windows-Explorer mit der rechten Maustaste auf das Dateisystem und klicken Sie auf Eigenschaften. Zeigen Sie die Kapazitätsdaten an.</li> </ul> <p>Die bevorzugte Position des Instanzverzeichnisses ist von dem Betriebssystem abhängig, unter dem der Server installiert ist:</p> <ul style="list-style-type: none"> <li>•  <b>AIX-Betriebssysteme</b></li> <li>•  <b>Linux-Betriebssysteme</b><br/>/home/tsminst1/tsminst1</li> <li>•  <b>Windows-Betriebssysteme</b><br/>C:\tsminst1</li> </ul> <p>Tipp: Wenn Sie ein Arbeitsblatt zur Planung ausgefüllt haben, ist die Position des Instanzverzeichnisses im Arbeitsblatt vermerkt.</p> |  |




| Task   | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung  |
|--|--|---|
| Ermitteln Sie nicht erwartete Clientaktivität. | <p>Um im Rahmen der Überwachung der Clientaktivität zu bestimmen, ob das Datenvolumen das erwartete Volumen überschreitet, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Clients'.</li> <li>2. Um die Aktivität der vergangen zwei Wochen anzuzeigen, doppelklicken Sie auf einen beliebigen Client.</li> <li>3. Um die Anzahl Byte anzuzeigen, die an den Client gesendet wurden, klicken Sie auf die Registerkarte Merkmale.</li> <li>4. Zeigen Sie im Bereich 'Letzte Sitzung' die Zeile 'An Client gesendet' an.</li> </ol> | <p>Wenn Sie auf einen Client in der Tabelle 'Clients' doppelklicken, wird im Bereich Aktivität im Lauf von 2 Wochen das Datenvolumen angezeigt, das vom Client jeden Tag an den Server gesendet wurde.</p> <p>Überprüfen Sie in regelmäßigen Abständen die SQL-Aktivitätsübersichtstabelle, die statistische Daten zu Clientsitzungen enthält. Um die aktuelle Aktivität mit der vorherigen Aktivität zu vergleichen, verwenden Sie eine Anweisung SQL SELECT. Wenn der Grad an Aktivität sich deutlich von dem für die vorherige Aktivität unterscheidet, kann dies eine Ransomware-Attacke anzeigen.</p> <p>Überprüfen Sie das Aktivitätenprotokoll in regelmäßigen Abständen. Suchen Sie nach ANE-Nachrichten, die angeben, wie viele Dateien gesichert und überprüft wurden. Vergleichen Sie die aktuellen Dateneduplizierungsraten mit den vorherigen Raten. Wenn eine ungewöhnlich hohe Anzahl Dateien gesichert wurde oder die Dateneduplizierungsrate wider Erwarten auf 0 fällt, kann dies eine Ransomware-Attacke anzeigen.</p> |

| Task  | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung  |
|---|--|---|
| <p>Überwachen Sie das Speicherpoolwachstum im Laufe der Zeit.</p> | <ol style="list-style-type: none"> <li>1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Pools'.</li> <li>2. Um die Kapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie einen Pool aus und klicken Sie auf Details.</li> </ol> | <p>Tipps:</p> <ul style="list-style-type: none"> <li>• Um die Zeit anzugeben, die verstreichen muss, bevor alle deduplizierten Speicherbereiche aus einem Verzeichniscontainerspeicherpool oder einem Cloud-Containerspeicherpool entfernt werden, nachdem sie nicht mehr vom Bestand referenziert werden, führen Sie die folgenden Schritte aus: <ol style="list-style-type: none"> <li>1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus.</li> <li>2. Klicken Sie auf Details &gt; Merkmale.</li> <li>3. Geben Sie im Feld <code>Verzögerungszeitraum für Containerwiederverwendung</code> den Zeitraum an.</li> </ol> </li> <li>• Bestimmen Sie die Dateneduplizierungsleistung für Verzeichniscontainer- und Cloud-Containerspeicherpools mithilfe des Befehls <code>GENERATE DEDUPSTATS</code>.</li> <li>• Um Deduplizierungsstatistikdaten für einen Speicherpool anzuzeigen, führen Sie die folgenden Schritte aus: <ol style="list-style-type: none"> <li>1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus.</li> <li>2. Klicken Sie auf Details &gt; Merkmale.</li> </ol> </li> </ul> <p>Verwenden Sie dementsprechend den Befehl <code>QUERY EXTENTUPDATES</code>, um Informationen zu Aktualisierungen an Datenbereichen in Verzeichniscontainer- oder Cloud-Containerspeicherpools anzuzeigen. Anhand der Befehlsausgabe können Sie die Datenbereiche bestimmen, die nicht mehr referenziert werden, sowie die Datenbereiche, die zum Löschen vom System auswählbar sind. Überwachen Sie in der Ausgabe die Anzahl Datenbereiche, die zum Löschen vom System auswählbar sind. Diese Messgröße steht in direkten Zusammenhang mit dem Umfang des freien Speicherbereichs in dem Containerspeicherpool.</p> <ul style="list-style-type: none"> <li>• Um den Umfang des physischen Speicherbereichs anzuzeigen, der von einem Dateibereich nach dem Entfernen der Dateneduplizierungseinsparungen belegt wird, verwenden Sie den Befehl <code>select * from occupancy</code>. Die Befehlsausgabe umfasst den Wert für <code>LOGICAL_MB</code>. <code>LOGICAL_MB</code> gibt an, wie viel Speicherbereich von diesem Dateibereich belegt wird.</li> </ul> |



| Task   | Basisprozeduren  | Erweiterte Prozeduren und Fehlerbehebung   |
|--|--|--|
| Werten Sie das Timing von Clientzeitplänen aus. Stellen Sie sicher, dass die Start- und Endzeiten von Clientzeitplänen Ihre Geschäftsanforderungen erfüllen. | Klicken Sie auf der Seite Übersicht im Operations Center auf Clients > Zeitpläne.<br><br>In der Tabelle 'Zeitpläne' wird in der Spalte 'Start' die konfigurierte Startzeit für die geplante Operation angezeigt. Um anzuzeigen, wann die letzte Operation gestartet wurde, bewegen Sie den Mauszeiger über das Uhersymbol. | Tipp: Wenn die Ausführung einer Clientoperation länger als erwartet dauert, empfangen Sie unter Umständen eine Warnung. Führen Sie die folgenden Schritte aus:<br><br><ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite 'Übersicht' im Operations Center den Mauszeiger über Clients und klicken Sie auf Zeitpläne.</li> <li>2. Wählen Sie einen Zeitplan aus und klicken Sie auf Details.</li> <li>3. Zeigen Sie die Details eines Zeitplans an, indem Sie auf den blauen Pfeil neben der Zeile klicken.</li> <li>4. Geben Sie im Feld Ausführungszeitalert die Uhrzeit an, zu der eine Warnung ausgegeben wird, wenn die geplante Operation nicht ausgeführt wird.</li> <li>5. Klicken Sie auf Sichern.</li> </ol> |
| Werten Sie das Timing von Verwaltungstasks aus. Stellen Sie sicher, dass die Start- und Endzeiten von Verwaltungstasks Ihre Geschäftsanforderungen erfüllen. | Klicken Sie auf der Seite Übersicht im Operations Center auf Server > Verwaltung.<br><br>Überprüfen Sie in der Tabelle 'Verwaltung' die Informationen in der Spalte 'Letzte Ausführungsdauer'. Um anzuzeigen, wann die letzte Verwaltungstask gestartet wurde, bewegen Sie den Mauszeiger über das Uhersymbol.             | Tipp: Wenn die Ausführung einer Verwaltungstask zu lange dauert, ändern Sie die Startzeit oder die maximale Ausführungszeit. Führen Sie die folgenden Schritte aus:<br><br><ol style="list-style-type: none"> <li>1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.</li> <li>2. Um die Startzeit oder die maximale Ausführungszeit für eine Task zu ändern, geben Sie den Befehl UPDATE SCHEDULE aus. Anweisungen finden Sie in UPDATE SCHEDULE (Clientzeitplan aktualisieren).</li> </ol>   |

**Zugehörige Verweise:**

-  QUERY ACTLOG (Aktivitätenprotokoll abfragen)
-  UPDATE STGPOOL (Speicherpool aktualisieren)
-  QUERY EXTENTUPDATES (Aktualisierte Datenbereiche abfragen)

## Lizenzeinhaltung überprüfen

Stellen Sie sicher, dass die Bedingungen Ihrer Lizenzvereinbarung von Ihrer IBM Spectrum Protect-Lösung eingehalten werden. Indem die Einhaltung regelmäßig überprüft wird, können Sie Trends beim Datenwachstum oder der PVU-Nutzung verfolgen. Planen Sie anhand dieser Informationen den weiteren Kauf von Lizenzen.

### Informationen zu diesem Vorgang

Die Methode zur Überprüfung der Einhaltung der Lizenzbedingungen durch Ihre Lösung variiert abhängig von den Bedingungen Ihrer IBM Spectrum Protect-Lizenzvereinbarung.

**Front-End-Kapazitätslizenzierung**

Das Front-End-Modell bestimmt die Lizenzvoraussetzungen auf der Basis des zurückgemeldeten Volumens an primären Daten, das von Clients gesichert wird. Clients umfassen Anwendungen, virtuelle Maschinen und Systeme.

**Back-End-Kapazitätslizenzierung**

Das Back-End-Modell bestimmt Lizenzvoraussetzungen auf der Basis der Terabyte Daten, die in primären Speicherpools und Repositories gespeichert werden.

Tipps:

- Um die Genauigkeit von Schätzungen der Front-End- und Back-End-Kapazität zu gewährleisten, installieren Sie die neueste Version der Client-Software auf jedem Clientknoten.
- Die Informationen zur Front-End- und Back-End-Kapazität im Operations Center dienen zum Zweck der Planung und Schätzung.

**PVU-Lizenzierung**



Das PVU-Modell basiert auf der Nutzung von PVUs durch Servereinheiten.

Wichtig: Die von IBM Spectrum Protect bereitgestellten PVU-Berechnungen werden als Schätzungen betrachtet und sind nicht rechtsverbindlich. Die von IBM Spectrum Protect zurückgemeldeten PVU-Lizenzinformationen werden nicht als zulässiger Ersatz für das IBM® License Metric Tool angesehen.

Die neuesten Informationen zu Lizenzierungsmodellen finden Sie in den Informationen zu Produktdetails und Lizenzen auf der Website der IBM Spectrum Protect-Produktfamilie. Wenden Sie sich bei Fragen oder Problemstellungen zu Lizenzierungsanforderungen an Ihren IBM Spectrum Protect-Software-Provider.

## Vorgehensweise

Führen Sie zur Überwachung der Lizenz Einhaltung die Schritte aus, die den Bedingungen Ihrer Lizenzvereinbarung entsprechen. Tipp: Das Operations Center stellt einen E-Mail-Bericht bereit, in dem die Front-End- und Back-End-Kapazitätsnutzung zusammengefasst sind. Berichte können automatisch regelmäßig an einen oder mehrere Empfänger gesendet werden. Klicken Sie für die Konfiguration und Verwaltung von E-Mail-Berichten in der Menüleiste des Operations Center auf Berichte.

| Option                  | Bezeichnung   |
|-------------------------|---|
| <b>Front-End-Modell</b> | <p>a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen  und klicken Sie auf Lizenzierung.</p> <p>Die Schätzung der Front-End-Kapazität wird auf der Seite 'Front-End-Nutzung' angezeigt.</p> <p>b. Wenn in der Spalte 'Keine Zurückmeldung' ein Wert angezeigt wird, klicken Sie auf die Zahl, um Clients zu identifizieren, von denen keine Kapazitätsnutzung zurückgemeldet wurde.</p> <p>c. Um die Kapazität für Clients zu schätzen, für die keine Kapazitätsnutzung zurückgemeldet wurde, rufen Sie die folgende FTP-Site auf, auf der Tools und Anweisungen zum Messen der Kapazität bereitgestellt werden:</p> <p><code>ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools</code></p> <p>Um die Front-End-Kapazität mithilfe eines Scripts zu messen, führen Sie die Anweisungen im aktuellen Lizenzierungshandbuch aus.</p> <p>d. Addieren Sie den Operations Center-Schätzwert und alle Schätzwerte, die Sie mithilfe eines Scripts ermittelt haben.</p> <p>e. Überprüfen Sie, ob die geschätzte Kapazität die Bedingungen Ihrer Lizenzvereinbarung einhält.</p> |
| <b>Back-End-Modell</b>  | <p>Einschränkung: Wenn der Quellen- und der Zielreplikationsserver nicht dieselben Maßnahmeneinstellungen verwenden, können Sie das Operations Center nicht zur Überwachung der Back-End-Kapazitätsnutzung für replizierte Clients verwenden. Informationen zur Schätzung der Kapazitätsnutzung für diese Clients finden Sie in Technote 1656476.</p> <p>a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen  und klicken Sie auf Lizenzierung.</p> <p>b. Klicken Sie auf die Registerkarte Back-End.</p> <p>c. Überprüfen Sie, ob das geschätzte Datenvolumen die Bedingungen Ihrer Lizenzvereinbarung einhält.</p>   |
| <b>PVU-Modell</b>       | Informationen zur Vorgehensweise beim Prüfen der Einhaltung der PVU-Lizenzbedingungen finden Sie in Einhaltung des PVU-Lizenzierungsmodells prüfen.   |

- Einhaltung des PVU-Lizenzierungsmodells prüfen  
Wenn Sie IBM Spectrum Protect unter dem Prozessor-Value-Unit-Lizenzierungsmodell (PVU-Lizenzierungsmodell) gekauft haben, stellen Sie sicher, dass Ihre Lösung die Lizenzbedingungen einhält. Überprüfen Sie die PVU-Schätzungen in regelmäßigen Abständen, um den weiteren Kauf von Lizenzen zu planen. Wenn sich beispielsweise PVU-Schätzungen erhöhen oder Sie die Installation weiterer Server planen, müssen Sie gegebenenfalls weitere Lizenzen kaufen.

## Systemstatus mithilfe von E-Mail-Berichten verfolgen

Konfigurieren Sie das Operations Center für die Generierung von E-Mail-Berichten zur Zusammenfassung des Systemstatus. Sie können eine Mail-Server-Verbindung konfigurieren, Berichtseinstellungen ändern und wahlweise angepasste SQL-Berichte erstellen.

## Vorbereitende Schritte

Bevor Sie E-Mail-Berichte konfigurieren, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- Es ist ein SMTP-Host-Server (SMTP = Simple Mail Transfer Protocol) verfügbar, um Berichte als E-Mail senden und empfangen zu können. Der SMTP-Server muss als offenes Mail-Relay konfiguriert sein. Außerdem müssen Sie sicherstellen, dass der IBM Spectrum Protect-Server, der E-Mail-Nachrichten sendet, Zugriff auf den SMTP-Server hat. Wenn das Operations Center auf einem anderen Computer installiert ist, ist für diesen Computer kein Zugriff auf den SMTP-Server erforderlich.
- Um E-Mail-Berichte konfigurieren zu können, müssen Sie über Systemberechtigung für den Server verfügen.
- Um die Empfänger anzugeben, können Sie eine oder mehrere E-Mail-Adressen oder Administrator-IDs eingeben. Wenn eine Administrator-ID eingegeben werden soll, muss die ID auf dem Hub-Server registriert sein und der ID muss eine E-Mail-Adresse zugeordnet sein. Eine E-Mail-Adresse für einen Administrator können Sie mithilfe des Parameters EMAILADDRESS im Befehl UPDATE ADMIN angeben.

## Informationen zu diesem Vorgang

Sie können das Operations Center zum Senden eines Berichts über allgemeine Operationen, eines Lizenzinhaltsberichts und eines oder mehrerer angepasster Berichte, die SQL-Anweisungen SELECT zum Abfragen verwalteter Server verwenden, konfigurieren.

## Vorgehensweise

Um E-Mail-Berichte zu konfigurieren und zu verwalten, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Menüleiste des Operations Center auf Berichte.
2. Wenn noch keine E-Mail-Server-Verbindung konfiguriert ist, klicken Sie auf Mail-Server konfigurieren und füllen Sie die Felder aus. Nach der Konfiguration des Mail-Servers sind der Bericht über allgemeine Operationen und der Lizenzinhaltsbericht aktiviert.
3. Um Berichtseinstellungen zu ändern, wählen Sie einen Bericht aus, klicken Sie auf Details und aktualisieren Sie das Formular.
4. Optional: Um einen angepassten SQL-Bericht hinzuzufügen, klicken Sie auf + Bericht und füllen Sie die Felder aus.  
Tipp: Um einen Bericht sofort auszuführen und zu senden, wählen Sie den Bericht aus und klicken Sie auf Senden.

## Ergebnisse

Aktivierte Berichte werden gemäß den angegebenen Einstellungen gesendet.

### Zugehörige Verweise:

[UPDATE ADMIN \(Administrator aktualisieren\)](#)

### Zugehörige Informationen:

[Beispiele für angepasste Berichte](#)

## Überwachungstools auswählen, konfigurieren und verwenden

Verwenden Sie das Operations Center, um eine Übersicht über den Systemstatus abzurufen und ein Drilldown zu detaillierten Informationen durchzuführen. In einigen Fällen möchten Sie vielleicht erweiterte Tools verwenden, um bestimmte Überwachungsdaten zu erfassen.



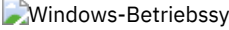

## Vorgehensweise

Wählen Sie die für Ihre Lösung geeigneten Überwachungstools aus und konfigurieren Sie diese.

Tabelle 1. Überwachungstools

| Tooltyp | Anwendungsfälle | Links zu weiteren Informationen |
|---------|-----------------|---------------------------------|
|---------|-----------------|---------------------------------|

| Tooltyp                                 | Anwendungsfälle  | Links zu weiteren Informationen  |
|---|--|--|
| Operations Center                       | <ul style="list-style-type: none"> <li>• Verwenden Sie die grafische Benutzerschnittstelle, um den Systemstatus zu überprüfen und Probleme zu diagnostizieren.</li> <li>• Konfigurieren Sie das Operations Center für das Senden täglicher E-Mail-Zusammenfassungsberichte.</li> <li>• Optional: Passen Sie die Alerts an, die im Operations Center angezeigt werden, und konfigurieren Sie E-Mail-Benachrichtigungen für die Alerts.</li> <li>• Optional: Überwachen Sie die Speicherumgebung über Fernzugriff, indem Sie die Seite Übersicht im Web-Browser einer mobilen Einheit anzeigen. Sie können beispielsweise den Apple Safari-Web-Browser auf einem Apple iPad-Gerät verwenden. Es können auch andere mobile Einheiten verwendet werden.</li> </ul> <p>Tipp: Wenn Sie IBM Spectrum Protect-Clientverwaltungsservices auf einem Client für Sichern/Archivieren installieren, können Sie mithilfe des Operations Center Fehlerbehebungsinformationen für den Client für Sichern/Archivieren abrufen. Der Clientverwaltungsservice kann nur unter Linux- oder Windows-Betriebssystemen installiert werden.</p> |  |
| IBM Spectrum Protect-Verwaltungsbefehle | <p>Lesen Sie die ausführlichen Informationen. Verwenden Sie die für Ihre Lösung zutreffende Methode:</p> <ul style="list-style-type: none"> <li>• Um Nachrichten anzuzeigen, die vom Server und Client generiert wurden, verwenden Sie den Befehl QUERY ACTLOG.<br/>Tipp: Sie können Verwaltungsbefehle über den Command Builder von Operations Center ausführen.</li> <li>• Um Aktivitäten, wie beispielsweise Serverumlagerung und Clientanmeldungen, zu überwachen, verwenden Sie den Verwaltungsclient im Konsolenmodus. Führen Sie den Befehl <code>dsmadm -consolemode</code> aus.</li> </ul>  | <ul style="list-style-type: none"> <li>• Verwaltungsbefehle</li> <li>• QUERY ACTLOG (Aktivitätenprotokoll abfragen)</li> <li>• Serveraktivitäten über den Verwaltungsclient überwachen</li> <li>• Verwaltungsclientoptionen</li> </ul> |

| Tooltyp   | Anwendungsfälle   | Links zu weiteren Informationen   |
|---|---|---|
| Ereignisprotokollierung                           | Protokollieren Sie Servernachrichten und die meisten Clientnachrichten als Ereignisse in einem oder mehreren Repositories, die als Empfänger bezeichnet werden.   |  <br> Anweisungen zur Verwendung der Ereignisprotokollierung zur Überwachung einer Lösung finden Sie in IBM Spectrum Protect-Ereignisse in Empfängern protokollieren (Version 7.1.1).<br><br> Anweisungen zur Protokollierung von Ereignissen in einem Linux-Systemprotokoll finden Sie in Ereignisse im Linux-Systemprotokoll protokollieren (Version 7.1.4). |
| SQL-Abfragen                                      | Erstellen und formatieren Sie angepasste Abfragen der Serverdatenbank. Sie können beispielsweise die SQL-Aktivitätsübersichtstabelle abfragen, um Statistikdaten zu Clientoperationen und Serverprozessen anzuzeigen. Um alle Informationen in der Übersichtstabelle anzuzeigen, geben Sie den folgenden Befehl über den Verwaltungsclient aus:<br><br><code>select * from summary</code> | Befehle SELECT verwenden (Version 7.1.1)  |
| Betriebssystemtools                               | Überwachen und testen Sie die Systemleistung.   |   |
| Einheitenüberwachungstools                        | Überwachen Sie Einheiten auf Verfügbarkeit, Kapazität und Leistung. Verwenden Sie beispielsweise IBM Spectrum Control oder Tools, die Bestandteil der Einheitenhardwarepakete sind.   | <p>Um den Einheitengesamtstatus mithilfe von IBM Spectrum Control zu überwachen, führen Sie die Anweisungen in Status und Zustand von Ressourcen überwachen aus.</p> <p>Um die Leistung mithilfe von IBM Spectrum Control zu überwachen, führen Sie die Anweisungen in Leistung von Ressourcen überwachen aus.</p>  |
| IBM® Tivoli Monitoring for Tivoli Storage Manager | Überwachen Sie IBM Spectrum Protect-Server und erstellen Sie Langzeitberichte über Server- und Clientaktivitäten. Tipp: Das Operations Center ist das bevorzugte Tool für die Überwachung. Tivoli Monitoring for Tivoli Storage Manager ist jedoch für die Erstellung von Langzeitberichten, die auf der Technologie von IBM Cognos Business Intelligence basieren, geeignet.             | Tivoli Monitoring for Tivoli Storage Manager  |

## Operationen verwalten

Durch die effektive Verwaltung von Server- und Clientoperationen können Sie die Leistung Ihrer Speicherumgebung optimieren. Überwachen Sie als ersten Schritt die Umgebung mithilfe des Operations Center. Ergreifen Sie dann Maßnahmen, um potenzielle Probleme zu verhindern und die Leistung zu verbessern.

### Informationen zu diesem Vorgang

- Serveroperationen verwalten  
Sie können den Server starten und stoppen, die Bestandskapazität verwalten sowie die Speichernutzung und Prozessorauslastung verwalten. Sie können auch die Datenübertragung zwischen Servern optimieren, ein Upgrade für den Server durchführen und geplante Aktivitäten optimieren.
- Clientoperationen verwalten  
Sie können Fehler, die einen Client für Sichern/Archivieren betreffen, mithilfe des Operations Center, das Vorschläge zur

Behebung von Fehlern bereitstellt, auswerten und beheben. Bei Fehlern für andere Typen von Clients müssen Sie die Fehlerprotokolle auf dem Client überprüfen und in der Produktdokumentation nachlesen.

- Operations Center verwalten  
Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt.

## Serveroperationen verwalten

---

Sie können den Server starten und stoppen, die Bestandskapazität verwalten sowie die Speichernutzung und Prozessorauslastung verwalten. Sie können auch die Datenübertragung zwischen Servern optimieren, ein Upgrade für den Server durchführen und geplante Aktivitäten optimieren.

- Server stoppen und starten  
Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.
- Bestandskapazität verwalten  
Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.
- Speichernutzung und Prozessorauslastung verwalten  
Der Speicherbedarf und die Prozessorauslastung müssen verwaltet werden, um sicherzustellen, dass der Server Datenprozesse wie Sicherung und Datenduplizierung ausführen kann. Berücksichtigen Sie die Auswirkung auf die Leistung, wenn Sie bestimmte Prozesse ausführen.
- Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann  
Wenn Ihr IBM Spectrum Protect-Server Knoten auf einen fernen Server repliziert oder Speicherpools auf einem fernen Server schützt, prüfen Sie, ob der Datendurchsatz an den fernen Server mithilfe der Technologie von Aspera Fast Adaptive Secure Protocol (FASP) verbessert werden kann. Bevor Sie die Aspera FASP-Technologie aktivieren, müssen Sie die entsprechenden Lizenzen anfordern. Es sind sowohl Test- als auch Volllizenzen verfügbar.
- Durchführung eines Upgrades für den Server planen  
Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.
- Geplante Aktivitäten optimieren  
Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

## Server stoppen und starten

---

Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.

### Vorbereitende Schritte

---

Um den IBM Spectrum Protect-Server stoppen und starten zu können, müssen Sie über System- oder Bedienerberechtigung verfügen.

- Server stoppen  
Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.
- Server für Verwaltungs- oder Rekonfigurationstasks starten  
Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

## Server stoppen

---

Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.

## Informationen zu diesem Vorgang

---

Wenn Sie den Befehl HALT zum Stoppen des Servers ausgeben, werden die folgenden Aktionen ausgeführt:

- Alle Prozesse und Clientknotensitzungen werden abgebrochen.
- Alle aktuellen Transaktionen werden gestoppt. (Die Transaktionen werden rückgängig gemacht, wenn der Server erneut gestartet wird.)

## Vorgehensweise

---

Um das System vorzubereiten und den Server zu stoppen, führen Sie die folgenden Schritte aus:

1. Verhindern Sie, dass neue Clientknotensitzungen gestartet werden, indem Sie den Befehl DISABLE SESSIONS ausgeben:

```
disable sessions all
```

2. Bestimmen Sie, ob Clientknotensitzungen oder -prozesse aktiv sind, indem Sie die folgenden Schritte ausführen:
  - a. Rufen Sie die Seite Übersicht im Operations Center auf, auf der im Bereich Aktivität die Gesamtzahl Prozesse und Sitzungen angezeigt wird, die derzeit aktiv sind. Wenn die Zahlen erheblich von den Zahlen abweichen, die normalerweise während Ihrer täglichen Speicherwaltungsroutine angezeigt werden, überprüfen Sie mithilfe weiterer Statusanzeiger im Operations Center, ob ein Problem vorliegt.
  - b. Zeigen Sie das Diagramm im Bereich Aktivität an, um den Umfang des Datenaustauschs im Netz für die folgenden Perioden zu vergleichen:
    - Die laufende Periode, d. h. die letzte 24-Stunden-Periode
    - Die vorherige Periode, d. h. die 24 Stunden vor der laufenden Periode

Wenn das Diagramm für die vorherige Periode den erwarteten Umfang des Datenaustauschs darstellt, können deutliche Abweichungen in dem Diagramm für die laufende Periode auf ein Problem hindeuten.

- c. Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details. Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, rufen Sie mithilfe von Verwaltungsbefehlen Informationen zu Prozessen ab. Geben Sie den Befehl QUERY PROCESS aus, um Prozesse abzufragen; geben Sie den Befehl QUERY SESSION aus, um Informationen zu Sitzungen abzurufen.
3. Warten Sie, bis die Clientknotensitzungen abgeschlossen sind oder brechen Sie diese ab. Um Prozesse und Sitzungen abzubrechen, führen Sie die folgenden Schritte aus:
    - Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details.
    - Klicken Sie auf die Registerkarte Aktive Tasks und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
    - Klicken Sie auf Abbrechen.
    - Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, brechen Sie Sitzungen mithilfe von Verwaltungsbefehlen ab. Geben Sie den Befehl CANCEL SESSION aus, um eine Sitzung abzubrechen; geben Sie den Befehl CANCEL PROCESS aus, um Prozesse abzubrechen.

Tipp: Wenn der Prozess, der abgebrochen werden soll, auf die Bereitstellung eines Banddatenträgers wartet, wird die Mountanforderung abgebrochen. Wenn Sie beispielsweise einen Befehl EXPORT, IMPORT oder MOVE DATA ausgeben, leitet der Befehl möglicherweise einen Prozess ein, der die Bereitstellung eines Banddatenträgers erfordert. Wenn jedoch ein Banddatenträger durch ein automatisiertes Speicherarchiv bereitgestellt wird, wird die Abbruchoperation unter Umständen erst wirksam, wenn der Bereitstellungsprozess abgeschlossen ist. Abhängig von Ihrer Systemumgebung kann dies mehrere Minuten dauern.
  4. Stoppen Sie den Server, indem Sie den Befehl HALT ausgeben:

```
halt
```

## Server für Verwaltungs- oder Rekonfigurationstasks starten

---

Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

## Informationen zu diesem Vorgang

---

Starten Sie den Server im Verwaltungsmodus, indem Sie das Dienstprogramm DSMSEV mit dem Parameter MAINTENANCE ausführen.

Im Verwaltungsmodus sind die folgenden Operationen inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Konsolidierung von Speicherbereich auf dem Server

- Bestandsverfall
- Umlagerung von Speicherpools

Darüber hinaus wird verhindert, dass Clients Sitzungen mit dem Server starten können.

Tipps:

- Sie müssen die Serveroptionsdatei, `dmserv.opt`, nicht editieren, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Speicherbereichskonsolidierung (-wiederherstellung), den Bestandsverfall und Umlagerungsprozesse für Speicherpools manuell starten.

## Vorgehensweise

---

Um den Server im Verwaltungsmodus zu starten, geben Sie den folgenden Befehl aus:

```
dmserv maintenance
```

Tipp: Ein Video zum Starten des Servers im Verwaltungsmodus kann über [Server im Verwaltungsmodus starten](#) angezeigt werden.

## Nächste Schritte




---

Um Serveroperationen im Produktionsmodus wiederaufzunehmen, führen Sie die folgenden Schritte aus:

1. Fahren Sie den Server herunter, indem Sie den Befehl `HALT` ausgeben:

```
halt
```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden. Führen Sie die Anweisungen für Ihr Betriebssystem aus:

-  AIX-BetriebssystemeServerinstanz starten
-  Linux-BetriebssystemeServerinstanz starten
-  Windows-BetriebssystemeServerinstanz starten

Operationen, die im Verwaltungsmodus inaktiviert waren, werden wieder aktiviert.

## Bestandskapazität verwalten

---

Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.

## Vorbereitende Schritte

---

Die aktive Protokolldatei und das Archivprotokoll haben die folgenden Merkmale:

- Die Größe der aktiven Protokolldatei kann maximal 512 GB betragen. Weitere Informationen zum Festlegen der Größe der aktiven Protokolldatei für Ihr System finden Sie in [Planung der Speicherarrays](#).
- Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist. Die Größe des Archivprotokolls ist im Gegensatz zur Größe der aktiven Protokolldatei nicht auf eine vordefinierte Größe festgelegt. Archivprotokolldateien werden automatisch gelöscht, wenn sie nicht mehr benötigt werden.

Als Best Practice können Sie wahlweise ein Archivübernahmeprotokoll erstellen, in dem Archivprotokolldateien gespeichert werden, wenn das Archivprotokollverzeichnis voll ist.

Bestimmen Sie über das Operations Center, welche Komponente des Bestands voll ist. Stellen Sie sicher, dass der Server gestoppt wird, bevor Sie eine der Bestandskomponenten vergrößern.

## Vorgehensweise

---

- Um die Datenbank zu vergrößern, führen Sie die folgenden Schritte aus:
  - Erstellen Sie in unterschiedlichen Laufwerken oder Dateisystemen ein oder mehrere Verzeichnisse für die Datenbank.
  - Geben Sie den Befehl `EXTEND DBSPACE` aus, um der Datenbank das Verzeichnis oder die Verzeichnisse hinzuzufügen. Die Instanzbenutzer-ID des Datenbankmanagers muss Zugriff auf die Verzeichnisse haben. Standardmäßig erfolgt eine Neuverteilung der Daten auf alle Datenbankverzeichnisse und eine Konsolidierung des Speicherbereichs.

Tipps:

- Die Zeit, die für die vollständige Neuverteilung von Daten und die Konsolidierung von Speicherbereich erforderlich ist, variiert abhängig von der Größe Ihrer Datenbank. Stellen Sie sicher, dass Sie dies bei der Planung berücksichtigen.



- Stellen Sie sicher, dass die Verzeichnisse, die Sie angeben, dieselbe Größe wie vorhandene Verzeichnisse haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorabesezugriff und zur Verteilung der Datenbank verringert.
    - Stoppen Sie den Server und starten Sie ihn erneut, um die neuen Verzeichnisse vollständig nutzen zu können.
    - Reorganisieren Sie die Datenbank, falls erforderlich. Die Index- und Tabellenreorganisation für die Serverdatenbank kann dazu beitragen, unerwartetes Datenbankwachstum und Leistungsprobleme zu verhindern. Weitere Informationen zur Reorganisation der Datenbank finden Sie in Technote 1683633.
- Um die Datenbank für Server der Version 7.1 und höher zu verkleinern, geben Sie im Serverinstanzverzeichnis die folgenden DB2-Befehle aus:

Einschränkung: Die Befehle können die E/A-Aktivität erhöhen und sich unter Umständen auf die Serverleistung auswirken. Um Leistungsprobleme auf ein Mindestmaß zu reduzieren, warten Sie, bis ein Befehl abgeschlossen ist, bevor Sie den nächsten Befehl ausgeben. Die DB2-Befehle können ausgegeben werden, wenn der Server aktiv ist.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE5 REDUCE MAX
```

- Um die aktive Protokolldatei zu vergrößern oder zu verkleinern, führen Sie die folgenden Schritte aus:
  1. Stellen Sie sicher, dass die Position für die aktive Protokolldatei über genügend Speicherbereich für die erhöhte Protokollgröße verfügt. Wenn ein Protokollspiegel vorhanden ist, muss auch die Position für den Spiegel über genügend Speicherbereich für die erhöhte Protokollgröße verfügen.
  2. Stoppen Sie den Server.
  3. Aktualisieren Sie in der Datei dmserv.opt die Option ACTIVELOGSIZE mit der neuen Größe der aktiven Protokolldatei (angegeben in Megabyte).

Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option ACTIVELOGSIZE. Die folgende Tabelle enthält Richtlinien für den Speicherbedarf:

Tabelle 1. Schätzen des Speicherbedarfs für Datenträger und Dateibereiche

| Wert für die Option ACTIVELOGSIZE | Größe des im Verzeichnis für aktive Protokolldateien zu reservierender freier Speicherbereich zusätzlich zum Speicherbereich für ACTIVELOGSIZE |
|-----------------------------------|--|
| 16 GB bis 128 GB                  | 5120 MB  |
| 129 GB bis 256 GB                 | 10240 MB   |
| 257 GB bis 512 GB                 | 20480 MB   |

Um die Größe der aktiven Protokolldatei in die maximale Größe von 512 GB zu ändern, geben Sie die folgende Serveroption ein:

```
activelogsiz 524288
```

- 4. Wenn Sie planen, ein neues Verzeichnis für aktive Protokolldateien zu verwenden, aktualisieren Sie den in der Serveroption ACTIVELOGDIRECTORY angegebenen Verzeichnisnamen. Das neue Verzeichnis muss leer sein und die Benutzer-ID des Datenbankmanagers muss Zugriff auf dieses Verzeichnis haben.
  5. Starten Sie den Server erneut.
- Komprimieren Sie die Archivprotokolle, um die Größe des Speicherbereichs, der zum Speichern benötigt wird, zu reduzieren. Aktivieren Sie die dynamische Komprimierung für das Archivprotokoll, indem Sie den folgenden Befehl ausgeben:

```
setopt archlogcompress yes
```

Einschränkung: Gehen Sie mit Vorsicht vor, wenn Sie die Serveroption ARCHLOGCOMPRESS auf Systemen mit kontinuierlich hoher Datenträgerverwendung und hohen Workloads aktivieren. Ein Aktivieren dieser Option in dieser Systemumgebung kann Verzögerungen beim Archivieren von Protokolldateien aus dem Dateisystem für aktive Protokolldateien in das Dateisystem für Archivprotokolle haben. Diese Verzögerung kann zur Folge haben, dass der Speicherbereich im Dateisystem für aktive Protokolldateien knapp wird. Sie müssen den verfügbaren Speicherbereich im Dateisystem für aktive Protokolldateien überwachen, nachdem die Komprimierung für das Archivprotokoll aktiviert wurde. Wenn für das Dateisystem für das Verzeichnis für aktive Protokolldateien fast kein Speicherbereich mehr verfügbar ist, muss die Serveroption ARCHLOGCOMPRESS inaktiviert werden. Mit dem Befehl SETOPT können Sie die Komprimierung für das Archivprotokoll sofort inaktivieren, ohne den Server stoppen zu müssen.

#### Zugehörige Verweise:

- ➔ Serveroption ACTIVELOGSIZE
- ➔ EXTEND DBSPACE (Speicherbereich für die Datenbank vergrößern)
- ➔ SETOPT (Serveroption für dynamische Aktualisierung definieren)

## Speichernutzung und Prozessorauslastung verwalten

---

Der Speicherbedarf und die Prozessorauslastung müssen verwaltet werden, um sicherzustellen, dass der Server Datenprozesse wie Sicherung und Datenduplizierung ausführen kann. Berücksichtigen Sie die Auswirkung auf die Leistung, wenn Sie bestimmte Prozesse ausführen.

### Vorbereitende Schritte

---

- Stellen Sie sicher, dass Ihre Konfiguration die erforderliche Hardware und Software verwendet. Weitere Informationen finden Sie in IBM Spectrum Protect Supported Operating Systems.
- Weitere Informationen zur Verwaltung von Ressourcen, wie beispielsweise Datenbank und Wiederherstellungsprotokoll, finden Sie in Planung der Speicherarrays.
- Fügen Sie zusätzlichen Systemspeicher hinzu, um festzustellen, ob sich die Leistung verbessert. Überwachen Sie die Speichernutzung regelmäßig, um zu bestimmen, ob weiterer Speicher erforderlich ist.

### Vorgehensweise

---

1. Geben Sie, falls möglich, Speicherbereich aus dem Dateisystemcache frei.
2. Verwenden Sie zur Verwaltung des Systemspeichers, den jeder Server auf einem System verwendet, die Serveroption DBMEMPERCENT. Begrenzen Sie den Prozentsatz des Systemspeichers, der vom Datenbankmanager jedes Servers verwendet werden kann. Wenn alle Server gleich wichtig sind, verwenden Sie denselben Wert für jeden Server. Wenn ein Server der Produktionsserver ist und die anderen Server Testserver sind, definieren Sie für den Produktionsserver einen höheren Wert als für die Testserver.
3. Definieren Sie den Benutzerdatengrenzwert und den privaten Speicher für die Datenbank, um sicherzustellen, dass immer genügend privater Speicher verfügbar ist. Wenn der private Speicher knapp wird, kann dies Fehler, eine nicht optimale Leistung und Instabilität zur Folge haben.

 Linux-Betriebssysteme

## Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann

---

Wenn Ihr IBM Spectrum Protect-Server Knoten auf einen fernen Server repliziert oder Speicherpools auf einem fernen Server schützt, prüfen Sie, ob der Datendurchsatz an den fernen Server mithilfe der Technologie von Aspera Fast Adaptive Secure Protocol (FASP) verbessert werden kann. Bevor Sie die Aspera FASP-Technologie aktivieren, müssen Sie die entsprechenden Lizenzen anfordern. Es sind sowohl Test- als auch Vollizenzen verfügbar.

### Vorbereitende Schritte

---

Die Aspera FASP-Technologie wird zur Übertragung von Datenbereichen aus einem Containerspeicherpool auf einen fernen Server verwendet. Wenn die Aspera FASP-Technologie aktiviert ist, werden die Datenbereiche, unabhängig davon, ob das Protokoll Secure Sockets Layer (SSL) aktiviert ist, bei der Übertragung immer verschlüsselt. Soll jedoch die Netzverbindung geschützt werden, müssen Sie SSL aktivieren. Informationen zu SSL und zur Aktivierung von SSL finden Sie in Kommunikation über Secure Sockets Layer und Transport Layer Security.

### Informationen zu diesem Vorgang

---

Einschränkungen:

- Verwenden Sie die Aspera FASP-Technologie, wenn Ihr Weitverkehrsnetz (WAN-Netz) Anzeichen großer Paketverluste und/oder Datenübertragungsverzögerungen zeigt, die durch eine Beeinträchtigung des Netzes verursacht werden. Wenn die WAN-Leistung Ihre Geschäftsanforderungen erfüllt, aktivieren Sie nicht die Aspera FASP-Technologie.
- Um die Aspera FASP-Technologie für Knotenreplikationsoperationen zu aktivieren, müssen die Daten in einem Verzeichniscontainerspeicherpool gespeichert sein.

## Vorgehensweise

---

1. Bestimmen Sie, ob die Aspera FASP-Technologie für Ihre Systemumgebung geeignet ist. Wenn eine der folgenden Bedingungen erfüllt ist, aktivieren Sie die Aspera FASP-Technologie:
  - Durchschnittliche Verzögerungen bei Datenübertragungsoperationen überschreiten 50 Millisekunden.
  - Der Paketverlust ist größer als 0,01 %.Netzmerkmale können sehr unterschiedlich sein. Möglicherweise können Sie den Netzdurchsatz durch die Aktivierung der Aspera FASP-Technologie selbst dann verbessern, wenn die Datenübertragungsverzögerung weniger als 50 Millisekunden und der Paketverlust weniger als 0,01 % beträgt.
2. Fordern Sie die entsprechenden Lizenzen an und installieren Sie diese. Führen Sie eine der folgenden Aktionen aus:

### Testlizenzen anfordern und installieren

Um Testlizenzen, die eine Ablaufdauer von 30 Tagen haben, anzufordern und zu installieren, führen Sie die folgenden Schritte aus:

- a. Fordern Sie die Lizenzen an, indem Sie eine E-Mail an [alliances@asperasoft.com](mailto:alliances@asperasoft.com) senden:
  - Geben Sie den Namen Ihres Unternehmens, Ihre Adresse, Ihre Telefonnummer und die E-Mail-Adresse des primären Ansprechpartners in Ihrem Unternehmen an.
  - Geben Sie an, dass eine Testlizenz mit einer Gültigkeit von 30 Tagen erforderlich ist.
  - Geben Sie die Anzahl erforderlicher Lizenzen an.

Pro Server, der für die Datenübertragung mit der Aspera FASP-Technologie verwendet wird, ist jeweils eine Lizenz erforderlich. Wenn Sie beispielsweise einen Knoten von einem Quellenserver auf einen Zielserver replizieren, sind zwei Lizenzen erforderlich.

Wenn die Lizenzanforderung genehmigt wird, empfängt der primäre Ansprechpartner in der Regel innerhalb von 24 Stunden eine E-Mail. Die E-Mail-Anlage umfasst Lizenzdateien, die gemäß der folgenden Konvention benannt sind:

```
xxxxx-ConnectSrv-unlim.eval.aspera-license
```

Dabei ist xxxxx eine eindeutige Zahl.

- b. Kopieren Sie eine der Lizenzdateien in das Verzeichnis `server/bin` des Quellenservers. Wählen Sie eine der beiden Lizenzdateien aus. Das Verzeichnis befindet sich standardmäßig an der folgenden Position:

```
/opt/tivoli/tsm/server/bin
```

- c. Kopieren Sie die andere Lizenzdatei in das Verzeichnis `bin` auf dem Zielserver.
- d. Setzen Sie auf dem Quellen- und dem Zielserver die Berechtigungsstufe jeder Lizenzdatei auf 755. Wenn Sie beispielsweise das Standardinstallationsverzeichnis verwenden und die eindeutige Lizenznummer 47474 lautet, geben Sie den folgenden Befehl in einer einzigen Zeile aus:

```
chmod 755 /opt/tivoli/tsm/server/bin/  
47474-ConnectSrv-unlim.eval.aspera-license
```

### Volllizenzen anfordern und installieren

Um uneingeschränkte Volllizenzen ohne Ablaufdauer anzufordern und zu installieren, führen Sie die folgenden Schritte aus:

- a. Kaufen Sie das Produkt IBM Spectrum Protect High Speed Data Transfer. Die Produktidentifikationsnummer lautet 5725-Z10. Sie können das Produkt über Passport Advantage anfordern.

Pro Server, der für die Datenübertragung mit der Aspera FASP-Technologie verwendet wird, ist eine Instanz von IBM Spectrum Protect High Speed Data Transfer erforderlich. Wenn Sie beispielsweise einen Knoten von einem Quellenserver auf einen Zielserver replizieren, sind zwei Instanzen von IBM Spectrum Protect High Speed Data Transfer erforderlich.

- b. Installieren Sie IBM Spectrum Protect High Speed Data Transfer mithilfe des Installationsassistenten auf jedem Server.

Einschränkung: Wenn die erforderlichen Lizenzen fehlen oder abgelaufen sind, schlagen Operationen zum Replizieren von Knoten und Schützen von Speicherpools mithilfe der Aspera FASP-Technologie fehl.

3. Optional: Validieren Sie die Aspera FASP-Konfiguration, indem Sie den Befehl `VALIDATE ASPERA` ausgeben. Mit dem Befehl `VALIDATE ASPERA` können Sie sicherstellen, dass Ihre Systemumgebung für Aspera FASP korrekt konfiguriert ist und dass gültige Lizenzen installiert sind. Darüber hinaus können Sie mithilfe des Befehls die Geschwindigkeit des Netzdurchsatzes bei Verwendung der Aspera FASP-Technologie gegenüber der bei Verwendung der TCP/IP-Technologie vergleichen.

## Nächste Schritte

---

Um die Aspera FASP-Technologie zu aktivieren, führen Sie die Schritte in Datenübertragung durch Aktivierung der Aspera FASP-Technologie optimieren aus.

- Datenübertragung durch Aktivierung der Aspera FASP-Technologie optimieren  
Wenn Sie einen fernen Server für den Speicherpoolschutz oder die Knotenreplikation verwenden und Netzprobleme auftreten, möchten Sie möglicherweise die Datenübertragung mithilfe der Technologie von Aspera Fast Adaptive Secure Protocol (FASP) optimieren.

## Durchführung eines Upgrades für den Server planen

---

Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.

## Informationen zu diesem Vorgang

---

Beachten Sie diese Richtlinien:

- Bei der bevorzugten Methode erfolgt das Upgrade für den Server mithilfe des Installationsassistenten. Nachdem Sie den Assistenten gestartet haben, klicken Sie im Fenster IBM Installation Manager auf das Symbol zum Aktualisieren; klicken Sie nicht auf das Symbol zum Installieren oder Ändern!
- Wenn sowohl für die Serverkomponente als auch für die Operations Center-Komponente Upgrades verfügbar sind, wählen Sie die Kontrollkästchen aus, um das Upgrade für beide Komponenten durchzuführen.

## Vorgehensweise




---

1. Überprüfen Sie die Liste der Fixpacks und vorläufigen Fixes. Siehe Technote 1239415.
2. Studieren Sie die Produktverbesserungen, die in der Readme-Datei beschrieben sind.  
Tipp: Wenn Sie die Installationspaketdatei von der IBM Spectrum Protect-Unterstützungssite abrufen, können Sie auch auf die Readme-Datei zugreifen.
3. Stellen Sie sicher, dass die Version, auf die das Upgrade für Ihren Server durchgeführt wird, mit anderen Komponenten, wie beispielsweise Speicheragenten und Speicherarchivclients, kompatibel ist. Siehe Technote 1302789.
4. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden. Siehe Technote 1053218.
5. Lesen Sie die Upgradeanweisungen. Stellen Sie sicher, dass Sie die Serverdatenbank, die Einheitenkonfigurationsinformationen und die Protokolldatei für Datenträger sichern.

## Nächste Schritte

---

Um ein Fixpack oder einen vorläufigen Fix zu installieren, führen Sie die Anweisungen für Ihr Betriebssystem aus:

-  AIX-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
-  Linux-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
-  Windows-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren

## Geplante Aktivitäten optimieren

---

Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

## Vorgehensweise

---

1. Überwachen Sie die Systemleistung regelmäßig, um sicherzustellen, dass Clientsicherungs- und Serververwaltungstasks erfolgreich ausgeführt werden. Führen Sie die Anweisungen in Speicherlösungen überwachen aus.

2. Optional: Wenn die Überwachungsdaten anzeigen, dass sich die Server-Workload erhöht hat, überprüfen Sie die Planungsinformationen. Überprüfen Sie, ob die Kapazität des Systems in den folgenden Fällen ausreichend ist:
    - o Erhöhung der Anzahl Clients
    - o Zunahme des Datenvolumens, das gesichert wird
    - o Änderung des Zeitraums, der für Sicherungen verfügbar ist
  3. Bestimmen Sie, ob Ihre Lösung auf dem von Ihnen erwarteten Niveau ausgeführt wird. Überprüfen Sie die Clientzeitpläne dahingehend, ob Tasks innerhalb des geplanten Zeitrahmens ausgeführt werden:
    - a. Wählen Sie auf der Seite Clients im Operations Center den Client aus.
    - b. Klicken Sie auf Details.
    - c. Überprüfen Sie auf der Seite Zusammenfassung des Clients die für Gesichert und Repliziert angegebene Aktivität, um alle Risiken zu ermitteln.  
Passen Sie, falls erforderlich, den Zeitpunkt und die Häufigkeit für die Ausführung von Clientsicherungsoperationen an.
  4. Planen Sie ausreichend Zeit ein, um die folgenden Verwaltungstasks innerhalb von 24 Stunden erfolgreich ausführen zu können:
    - a. Schützen von Speicherpools
    - b. Replizieren von Knotendaten
    - c. Sichern der Datenbank
    - d. Ausführen der Verfallsverarbeitung, um Clientsicherungen und Archivierungsdateikopien aus dem Serverspeicher zu entfernen

Tipp: Planen Sie einen geeigneten Zeitpunkt für den Start von Verwaltungstasks und die Ausführung in der korrekten Reihenfolge. Planen Sie beispielsweise Replikationstasks im Anschluss an die erfolgreiche Ausführung von Clientsicherungen.
- Clients von einem Server auf einen anderen versetzen  
Um zu verhindern, dass der Speicherbereich auf einem Server knapp wird, oder um Workloadprobleme zu beheben, müssen Sie unter Umständen Clientknoten von einem Server auf einen anderen versetzen.

**Zugehörige Konzepte:**

☞ Leistung

**Zugehörige Tasks:**

☞ Daten deduplizieren (Version 7.1.1)

## Clientoperationen verwalten

---

Sie können Fehler, die einen Client für Sichern/Archivieren betreffen, mithilfe des Operations Center, das Vorschläge zur Behebung von Fehlern bereitstellt, auswerten und beheben. Bei Fehlern für andere Typen von Clients müssen Sie die Fehlerprotokolle auf dem Client überprüfen und in der Produktdokumentation nachlesen.

### Informationen zu diesem Vorgang

---

In einigen Fällen können Clientfehler behoben werden, indem der Clientakzeptor gestoppt und gestartet wird. Wenn Clientknoten oder Administrator-IDs gesperrt sind, können Sie das Problem beheben, indem Sie den Clientknoten bzw. die Administrator-ID entsperren und dann das Kennwort zurücksetzen.

Detaillierte Anweisungen zum Identifizieren und Beheben von Clientfehlern finden Sie in Clientprobleme lösen.

- Bereich einer Clientsicherung ändern  
Wenn Sie Clientsicherungsoperationen konfigurieren, ist das bevorzugte Verfahren das Ausschließen von Objekten, die nicht erforderlich sind. Angenommen, Sie möchten normalerweise temporäre Dateien von einer Sicherungsoperation ausschließen.
- Fehler in Clientfehlerprotokollen auswerten  
Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.
- Clientakzeptor stoppen und erneut starten  
Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.
- Kennwörter zurücksetzen  
Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.
- Clientknoten stilllegen  
Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.
- Daten zum Freigeben von Speicherbereich inaktivieren  
In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegebenen Datum und vor der angegebenen Uhrzeit

gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

- Client-Upgrades verwalten

Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.

## Bereich einer Clientsicherung ändern

---

Wenn Sie Clientsicherungsoperationen konfigurieren, ist das bevorzugte Verfahren das Ausschließen von Objekten, die nicht erforderlich sind. Angenommen, Sie möchten normalerweise temporäre Dateien von einer Sicherungsoperation ausschließen.

### Informationen zu diesem Vorgang

---

Indem Sie nicht benötigte Objekte von Sicherungsoperationen ausschließen, können Sie die Größe des Speicherbereichs, der für Sicherungsoperationen erforderlich ist, und die Speicherkosten besser steuern. Abhängig von Ihrem Lizenzpaket ist es unter Umständen auch möglich, die Lizenzierungskosten zu begrenzen.

### Vorgehensweise

---

Die Vorgehensweise beim Ändern des Bereichs von Sicherungsoperationen ist von dem Produkt abhängig, das auf dem Clientknoten installiert ist:

- Bei einem Client für Sichern/Archivieren können Sie eine Einschluss-/Ausschlussliste erstellen, um eine Datei, Dateigruppen oder Verzeichnisse in Sicherungsoperationen einzuschließen oder von Sicherungsoperationen auszuschließen. Um eine Einschluss-/Ausschlussliste zu erstellen, führen Sie die Anweisungen in Einschluss-/Ausschlussliste erstellen aus.

Um die konsistente Verwendung einer Einschluss-/Ausschlussliste für alle Clients eines bestimmten Typs zu gewährleisten, können Sie auf dem Server eine Clientoptionsgruppe erstellen, die die erforderlichen Optionen enthält. Anschließend ordnen Sie die Clientoptionsgruppe jedem Client desselben Typs zu. Ausführliche Informationen finden Sie in Clientoperationen über Clientoptionsgruppen steuern.

- Für einen Client für Sichern/Archivieren können Sie die Objekte, die in eine Teilsicherungsoperation eingeschlossen werden sollen, mithilfe der Option domain angeben. Führen Sie die Anweisungen in Clientoption 'domain' aus.
- Führen Sie für andere Produkte die Anweisungen in der Produktdokumentation aus, um zu definieren, welche Objekte in Sicherungsoperationen eingeschlossen und von Sicherungsoperationen ausgeschlossen werden sollen.

## Fehler in Clientfehlerprotokollen auswerten

---

Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.

### Vorbereitende Schritte

---

Um Fehler in einem Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem zu beheben, stellen Sie sicher, dass der Clientverwaltungsservice installiert und gestartet wurde. Installationsanweisungen finden Sie in Diagnoseinformationen mit Clientverwaltungsservices erfassen.

### Vorgehensweise

---

Um Clientfehler zu diagnostizieren und zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn der Clientverwaltungsservice auf dem Clientknoten installiert ist, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Details.
  3. Klicken Sie auf der Seite 'Zusammenfassung' auf die Registerkarte Diagnose.
  4. Überprüfen Sie die abgerufenen Protokollnachrichten.

Tipps:

  - Um das Fenster 'Clientprotokolle' ein- oder auszublenden, doppelklicken Sie auf den Rahmen des Fensters 'Clientprotokolle'.
  - Um die Größe des Fensters 'Clientprotokolle' zu ändern, klicken Sie auf den Rahmen des Fensters 'Clientprotokolle' und ziehen Sie den Rahmen.

Wenn auf der Seite 'Diagnose' Vorschläge angezeigt werden, wählen Sie einen Vorschlag aus. Im Fenster 'Clientprotokolle' sind die Clientprotokollnachrichten, auf die sich der Vorschlag bezieht, hervorgehoben.

5. Lösen Sie die in den Fehlernachrichten angegebenen Probleme mithilfe der Vorschläge.

Tipp: Vorschläge werden nur für einen Teil der Clientnachrichten bereitgestellt.

- Wenn der Clientverwaltungsservice nicht auf dem Clientknoten installiert ist, überprüfen Sie die Fehlerprotokolle für den installierten Client.

## Clientakzeptor stoppen und erneut starten

---

Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.

### Informationen zu diesem Vorgang

---

In einigen Fällen können Clientzeitplanungsprobleme behoben werden, indem der Clientakzeptor gestoppt und erneut gestartet wird. Der Clientakzeptor muss aktiv sein, um sicherzustellen, dass geplante Operationen auf dem Client erfolgen können. Wenn Sie beispielsweise die IP-Adresse oder den Domännennamen des Servers ändern, müssen Sie den Clientakzeptor erneut starten.

### Vorgehensweise

---

Führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

AIX und Oracle Solaris

- Um den Clientakzeptor zu stoppen, führen Sie die folgenden Schritte aus:
  - a. Bestimmen Sie die Prozess-ID für den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

```
ps -ef | grep dsmcad
```

Überprüfen Sie die Ausgabe. In der folgenden Beispielausgabe lautet die Prozess-ID für den Clientakzeptor 6764:

```
root 6764 1 0 16:26:35 ? 0:00 /usr/bin/dsmcad
```

- b. Geben Sie in der Befehlszeile den folgenden Befehl aus:

```
kill -9 PID
```

Dabei gibt *PID* die Prozess-ID für den Clientakzeptor an.

- Um den Clientakzeptor zu starten, geben Sie in der Befehlszeile den folgenden Befehl aus:

```
/usr/bin/dsmcad
```

Linux

- Um den Clientakzeptor zu stoppen, ohne ihn erneut zu starten, geben Sie den folgenden Befehl aus:

```
# service dsmcad stop
```

- Um den Clientakzeptor zu stoppen und erneut zu starten, geben Sie den folgenden Befehl aus:

```
# service dsmcad restart
```

MAC OS X

Klicken Sie auf Applications > Utilities > Terminal.

- Um den Clientakzeptor zu stoppen, geben Sie den folgenden Befehl aus:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Um den Clientakzeptor zu starten, geben Sie den folgenden Befehl aus:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```


Windows

- Um den Clientakzeptorservice zu stoppen, führen Sie die folgenden Schritte aus:

- a. Klicken Sie auf Start > Verwaltung > Dienste.
- b. Doppelklicken Sie auf den Clientakzeptorservice.
- c. Klicken Sie auf Beenden und OK.

- Um den Clientakzeptorservice erneut zu starten, führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf Start > Verwaltung > Dienste.
  - b. Doppelklicken Sie auf den Clientakzeptorservice.
  - c. Klicken Sie auf Starten und OK.

#### Zugehörige Verweise:

 Fehler für Clientzeitplanung beheben

## Kennwörter zurücksetzen

---

Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.

## Vorgehensweise

---

Um Kennwortprobleme zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn ein Client für Sichern/Archivieren auf einem Clientknoten installiert ist und das Kennwort verloren gegangen ist oder Sie das Kennwort vergessen haben, führen Sie die folgenden Schritte aus:

1. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

```
update node Knotenname neues_Kennwort forcepwreset=yes
```

Dabei gibt *Knotenname* den Clientknoten und *neues\_Kennwort* das Kennwort an, das Sie zuordnen.

2. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.  
Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf generate gesetzt haben.
- Wenn ein Administrator aufgrund von Kennwortproblemen ausgesperrt ist, führen Sie die folgenden Schritte aus:
    1. Um dem Administrator den Zugriff auf den Server zu ermöglichen, geben Sie den Befehl UNLOCK ADMIN aus. Anweisungen finden Sie in UNLOCK ADMIN (Administrator entsperren).
    2. Legen Sie mit dem Befehl UPDATE ADMIN ein neues Kennwort fest:

```
update admin Administratorname neues_Kennwort forcepwreset=yes
```

Dabei gibt *Administratorname* den Namen des Administrators und *neues\_Kennwort* das Kennwort an, das Sie zuordnen.

- Wenn ein Clientknoten gesperrt ist, führen Sie die folgenden Schritte aus:
  1. Bestimmen Sie, warum der Clientknoten gesperrt ist und ob er entsperrt werden muss. Wenn beispielsweise der Clientknoten stillgelegt ist, wird der Clientknoten aus der Produktionsumgebung entfernt. Sie können die Stilllegungsoperation nicht zurücknehmen und der Clientknoten bleibt gesperrt. Ein Clientknoten kann auch gesperrt sein, wenn die Clientdaten Gegenstand einer rechtlichen Untersuchung sind.
  2. Verwenden Sie zum Entsperren eines Clientknotens den Befehl UNLOCK NODE. Anweisungen finden Sie in UNLOCK NODE (Clientknoten entsperren).
  3. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

```
update node Knotenname neues_Kennwort forcepwreset=yes
```

Dabei gibt *Knotenname* den Namen des Knotens und *neues\_Kennwort* das Kennwort an, das Sie zuordnen.

4. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.  
Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf generate gesetzt haben.

## Clientknoten stilllegen

---

Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.

## Informationen zu diesem Vorgang

---



Wenn Sie den Stilllegungsprozess starten, sperrt der Server den Clientknoten, um zu verhindern, dass dieser auf den Server zugreift. Dateien, die zu dem Clientknoten gehören, werden nacheinander gelöscht; anschließend wird der Clientknoten gelöscht. Sie können die folgenden Typen von Clientknoten stilllegen:

#### Anwendungsclientknoten

Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

#### Systemclientknoten

Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

#### VM-Clientknoten

Clientknoten virtueller Maschinen bestehen aus einem einzelnen Gasthost in einem Hypervisor. Jede virtuelle Maschine wird als ein Dateibereich dargestellt.

Die einfachste Methode zur Stilllegung eines Clientknotens ist die Verwendung des Operations Center. Der Stilllegungsprozess wird im Hintergrund ausgeführt. Wenn der Client für die Replikation von Clientdaten konfiguriert ist, entfernt das Operations Center den Client automatisch aus der Replikation auf dem Quellen- und dem Zielreplikationsserver, bevor es den Client stilllegt.

Tipp: Sie können einen Clientknoten auch stilllegen, indem Sie den Befehl `DECOMMISSION NODE` oder `DECOMMISSION VM` ausgeben. Diese Methode kann beispielsweise in den folgenden Fällen verwendet werden:

- Um den Stilllegungsprozess für einen späteren Zeitpunkt zu planen oder eine Serie von Befehlen unter Verwendung eines Scripts auszuführen, geben Sie die Ausführung des Stilllegungsprozesses im Hintergrund an.
- Um den Stilllegungsprozess zu Zwecken der Fehlerbehebung zu überwachen, geben Sie die Ausführung des Stilllegungsprozesses im Vordergrund an. Wenn Sie den Prozess im Vordergrund ausführen, müssen Sie warten, bis der Prozess abgeschlossen ist, bevor Sie die Arbeit mit anderen Tasks fortsetzen können.

## Vorgehensweise

---

Führen Sie eine der folgenden Aktionen aus:

- Um einen Client mithilfe des Operations Center im Hintergrund stillzulegen, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Weitere > Stilllegen.
- Um einen Clientknoten mithilfe eines Verwaltungsbefehls stillzulegen, führen Sie die folgenden Schritte aus:
  1. Bestimmen Sie, ob der Clientknoten für die Knotenreplikation konfiguriert ist, indem Sie den Befehl `QUERY NODE` ausgeben. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, führen Sie den folgenden Befehl aus:

```
query node austin format=detailed
```

Überprüfen Sie das Ausgabefeld 'Replikationsstatus'.

2. Wenn der Clientknoten für die Replikation konfiguriert ist, entfernen Sie den Clientknoten aus der Replikation, indem Sie den Befehl `REMOVE REPLNODE` ausgeben. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

```
remove replnode austin
```

3. Führen Sie eine der folgenden Aktionen aus:

- Um einen Anwendungs- oder Systemclientknoten im Hintergrund stillzulegen, geben Sie den Befehl `DECOMMISSION NODE` aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

```
decommission node austin
```

- Um einen Anwendungs- oder Systemclientknoten im Vordergrund stillzulegen, geben Sie den Befehl `DECOMMISSION NODE` unter Angabe des Parameters `wait=yes` aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

```
decommission node austin wait=yes
```

- Um eine virtuelle Maschine im Hintergrund stillzulegen, geben Sie den Befehl `DECOMMISSION VM` aus. Wenn beispielsweise die virtuelle Maschine den Namen AUSTIN hat, der Dateibereich 7 ist und der Dateibereichsname über die Dateibereichs-ID angegeben wird, geben Sie den folgenden Befehl aus:

```
decommission vm austin 7 nametype=fsid
```

Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Um eine virtuelle Maschine im Vordergrund stillzulegen, geben Sie den Befehl DECOMMISSION VM unter Angabe des Parameters `wait=yes` aus. Geben Sie beispielsweise den folgenden Befehl aus:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

## Nächste Schritte

Achten Sie auf Fehlermeldungen, die unter Umständen in der Benutzerschnittstelle oder in der Befehlsausgabe unmittelbar nach der Ausführung des Prozesses angezeigt werden.

Um zu überprüfen, ob der Clientknoten stillgelegt wurde, gehen Sie wie folgt vor:

1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients.
2. Überprüfen Sie in der Tabelle 'Clients' in der Spalte 'Gefährdet' den Status:
  - Der Status 'Stillgelegt' (DECOMMISSIONED) gibt an, dass der Knoten stillgelegt wurde.
  - Ein Nullwert gibt an, dass der Knoten nicht stillgelegt wurde.
  - Der Status 'Anstehend' (PENDING) gibt an, dass der Knoten gerade stillgelegt wird oder der Stilllegungsprozess fehlgeschlagen ist.

Tipp: Wenn der Status eines anstehenden Stilllegungsprozesses bestimmt werden soll, geben Sie den folgenden Befehl aus:

```
query process
```

3. Überprüfen Sie die Befehlsausgabe:
  - Wenn für den Stilllegungsprozess ein Status angegeben ist, ist der Prozess in Bearbeitung. Beispiel:

```
query process
Prozess-      Prozessbeschreibung      Prozesstatus
nummer
-----      -
          3      DECOMMISSION NODE      Anzahl der für Knoten NODE1 inaktivierten
                                          Sicherungsobjekte: 8 Objekte inaktiviert.
```

- Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie keine Fehlermeldung empfangen haben, ist der Prozess unvollständig. Ein Prozess kann unvollständig sein, wenn Dateien, die dem Knoten zugeordnet sind, noch nicht inaktiviert wurden. Führen Sie nach der Inaktivierung der Dateien den Stilllegungsprozess erneut aus.
- Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie eine Fehlermeldung empfangen, ist der Prozess fehlgeschlagen. Führen Sie den Stilllegungsprozess erneut aus.

### Zugehörige Verweise:

- 🔗 [DECOMMISSION NODE](#) (Clientknoten stilllegen)
- 🔗 [DECOMMISSION VM](#) (Virtuelle Maschine stilllegen)
- 🔗 [QUERY NODE](#) (Knoten abfragen)
- 🔗 [REMOVE REPLNODE](#) (Clientknoten aus Replikation entfernen)

## Daten zum Freigeben von Speicherbereich inaktivieren

In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegebenen Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

### Informationen zu diesem Vorgang

Einige Anwendungsclients sichern Daten immer als aktive Sicherungsdaten auf dem Server. Da aktive Sicherungsdaten nicht durch die Bestandsverfallsmaßnahmen verwaltet werden, werden die Daten nicht automatisch gelöscht und belegen unbegrenzt Serverspeicher. Um den Speicherbereich freizugeben, der von veralteten Daten belegt wird, können Sie die Daten inaktivieren.

Wenn Sie den Inaktivierungsprozess ausführen, werden alle aktiven Sicherungsdaten, die vor dem angegebenen Datum gespeichert wurden, inaktiv. Die Daten werden gelöscht, sobald sie verfallen, und können nicht zurückgeschrieben werden. Die Inaktivierungsfunktion gilt nur für Anwendungsclients, die Oracle-Datenbanken schützen.

## Vorgehensweise

1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients.
2. Wählen Sie in der Tabelle 'Clients' einen oder mehrere Clients aus und klicken Sie auf Weitere > Bereinigen.  
Befehlszeilenmethode: Inaktivieren Sie Daten mit dem Befehl DEACTIVATE DATA.

### Zugehörige Verweise:

[☞](#) DEACTIVATE DATA (Daten für einen Clientknoten inaktivieren)

## Client-Upgrades verwalten

Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.

## Vorbereitende Schritte

1. Überprüfen Sie die Voraussetzungen für die Client/Server-Kompatibilität in Technote 1053218. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden.
2. Überprüfen Sie die Systemvoraussetzungen für den Client in IBM Spectrum Protect Supported Operating Systems.
3. Wenn die Lösung Speicheragenten oder Speicherarchivclients umfasst, überprüfen Sie die Informationen zur Kompatibilität von Speicheragenten bzw. Speicherarchivclients mit Servern, die als Speicherarchivmanager konfiguriert sind. Siehe Technote 1302789.

Wenn Sie planen, ein Upgrade für einen Speicherarchivmanager und einen Speicherarchivclient durchzuführen, müssen Sie zuerst das Upgrade für den Speicherarchivmanager durchführen.

## Vorgehensweise

Um ein Software-Upgrade durchzuführen, führen Sie die in der folgenden Tabelle aufgelisteten Anweisungen aus.

| Software  | Link zu Anweisungen   |
|---|---|
| IBM Spectrum Protect-Client für Sichern/Archivieren   | <ul style="list-style-type: none"> <li>• Clientaktualisierungen planen</li> </ul>   |
| IBM Spectrum Protect Snapshot                         | <ul style="list-style-type: none"> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen</li> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen</li> <li>• Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen</li> </ul>  |
| IBM Spectrum Protect for Databases                    | <ul style="list-style-type: none"> <li>• Upgrade für Data Protection for SQL Server durchführen</li> <li>• Installation von Data Protection for Oracle</li> <li>• Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li> </ul>   |
| IBM Spectrum Protect for Enterprise Resource Planning | <ul style="list-style-type: none"> <li>• Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 durchführen</li> <li>• Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle durchführen</li> </ul>   |
| IBM Spectrum Protect for Mail                         | <ul style="list-style-type: none"> <li>• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0)</li> <li>• Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0)</li> <li>• Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li> </ul> |

| Software                                      | Link zu Anweisungen   |
|---|---|
| IBM Spectrum Protect for Virtual Environments | <ul style="list-style-type: none"> <li>• Installation und Upgrade für Data Protection for VMware durchführen</li> <li>• Data Protection for Microsoft Hyper-V installieren</li> </ul> |

## Operations Center verwalten

---

Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt.

- Peripherieserver hinzufügen und entfernen  
In einer Umgebung mit mehreren Servern können Sie dem Hub-Server die anderen Server, die als *Peripherieserver* bezeichnet werden, hinzufügen.
- Web-Server starten und stoppen  
Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Unter Umständen müssen Sie den Web-Server stoppen und starten, um beispielsweise Konfigurationsänderungen durchzuführen.
- Assistenten für die Erstkonfiguration erneut starten  
Unter Umständen müssen Sie den Assistenten für die Erstkonfiguration im Operations Center erneut starten, um beispielsweise Konfigurationsänderungen durchzuführen.
- Hub-Server ändern  
Mithilfe des Operations Center können Sie den Hub-Server von IBM Spectrum Protect entfernen und einen anderen Hub-Server konfigurieren.
- Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben  
Wenn bestimmte Probleme auftreten, möchten Sie möglicherweise die Operations Center-Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben, bei dem die IBM Spectrum Protect-Server nicht als Hub- oder Peripherieserver definiert sind.

## Peripherieserver hinzufügen und entfernen

---

In einer Umgebung mit mehreren Servern können Sie dem Hub-Server die anderen Server, die als *Peripherieserver* bezeichnet werden, hinzufügen.

### Informationen zu diesem Vorgang

---

Die Peripherieserver senden Alerts und Statusinformationen an den Hub-Server. Das Operations Center zeigt eine konsolidierte Sicht der Alerts und Statusinformationen für den Hub-Server und alle Peripherieserver.

- Peripherieserver hinzufügen  
Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server einen oder mehrere Peripherieserver hinzufügen.
- Peripherieserver entfernen  
Sie können einen Peripherieserver aus dem Operations Center entfernen.

## Peripherieserver hinzufügen

---

Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server einen oder mehrere Peripherieserver hinzufügen.

### Vorbereitende Schritte

---

Die Kommunikation zwischen dem Peripherieserver und dem Hub-Server muss unter Verwendung des Protokolls Transport Layer Security (TLS) geschützt werden. Um die Kommunikation zu schützen, fügen Sie das Zertifikat des Peripherieservers der Truststore-Datei des Hub-Servers hinzu.

### Vorgehensweise

---

1. Klicken Sie in der Menüleiste des Operations Center auf Server. Die Seite Server wird geöffnet.

In der Tabelle auf der Seite Server könnte ein Server den Status "Nicht überwacht" haben. Dieser Status bedeutet, dass - obwohl ein Administrator diesen Server mit dem Befehl DEFINE SERVER für den Hub-Server definiert hat - der Server noch nicht als Peripherieserver konfiguriert ist.

2. Führen Sie einen der folgenden Schritte aus:
  - Klicken Sie auf den Server, um ihn hervorzuheben, und klicken Sie in der Menüleiste der Tabelle auf Peripherieserver überwachen.
  - Wenn der Server, der hinzugefügt werden soll, in der Tabelle nicht angezeigt wird und die sichere SSL-/TLS-Kommunikation nicht erforderlich ist, klicken Sie in der Menüleiste der Tabelle auf +Peripherieserver.
3. Geben Sie die erforderlichen Informationen an und führen Sie die Schritte im Konfigurationsassistenten für den Peripherieserver aus.  
Tipp: Wenn der Aufbewahrungszeitraum für Ereignissätze des Servers weniger als 14 Tage beträgt, wird der Zeitraum automatisch auf 14 Tage zurückgesetzt, wenn Sie den Server als Peripherieserver konfigurieren.

## Peripherieserver entfernen

---

Sie können einen Peripherieserver aus dem Operations Center entfernen.

### Informationen zu diesem Vorgang

---

Unter Umständen müssen Sie einen Peripherieserver in den folgenden Situationen entfernen:

- Der Peripherieserver soll von einem Hub-Server auf einen anderen Hub-Server versetzt werden.
- Der Peripherieserver soll stillgelegt werden.

### Vorgehensweise

---

Um den Peripherieserver aus der Gruppe der Server zu entfernen, die vom Hub-Server verwaltet werden, führen Sie die folgenden Schritte aus:

1. Geben Sie in der IBM Spectrum Protect-Befehlszeile auf dem Hub-Server den folgenden Befehl aus:

```
QUERY MONITORSETTINGS
```

2. Kopieren Sie in der Ausgabe des Befehls den Namen im Feld Überwachte Gruppe.
3. Geben Sie auf dem Hub-Server den folgenden Befehl aus; dabei ist *Gruppenname* der Name der überwachten Gruppe und *Mitgliedsname* der Name des Peripherieservers:

```
DELETE GRPMEMBER Gruppenname Mitgliedsname
```

4. Optional: Wenn der Peripherieserver von einem Hub-Server auf einen anderen Hub-Server versetzt werden soll, dürfen Sie diesen Schritt **nicht** ausführen. Andernfalls können Sie die Alertausgabe und Überwachung auf dem Peripherieserver inaktivieren, indem Sie auf dem Peripherieserver die folgenden Befehle ausgeben:

```
SET STATUSMONITOR OFF  
SET ALERTMONITOR OFF
```

5. Optional: Wenn die Definition des Peripherieservers für andere Zwecke verwendet wird, wie beispielsweise unternehmensweite Konfiguration, Befehlsweiterleitung, Speichern virtueller Datenträger oder Speicherarchivverwaltung, dürfen Sie diesen Schritt **nicht** ausführen. Andernfalls können Sie die Definition des Peripherieservers auf dem Hub-Server löschen, indem Sie auf dem Hub-Server den folgenden Befehl ausgeben:

```
DELETE SERVER Name_des_Peripherieservers
```

Tipp: Wenn eine Serverdefinition sofort nach dem Entfernen des Servers aus der überwachten Gruppe gelöscht wird, können Statusinformationen für den Server ohne zeitliche Begrenzung im Operations Center verbleiben.

Um dieses Problem zu verhindern, warten Sie, bis das Intervall für die Erfassung von Statusdaten überschritten wurde, bevor Sie die Serverdefinition löschen. Das Intervall für die Erfassung von Statusdaten wird auf der Seite 'Einstellungen' des Operations Center angezeigt.


## Web-Server starten und stoppen

---


Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Unter Umständen müssen Sie den Web-Server stoppen und starten, um beispielsweise Konfigurationsänderungen durchzuführen.

### Vorgehensweise

---

1. Stoppen Sie den Web-Server.
  -  Geben Sie im Verzeichnis */Installationsverzeichnis/ui/utls* (dabei gibt *Installationsverzeichnis* das Verzeichnis an, in dem das Operations Center installiert ist) den folgenden Befehl aus:


```
./stopserver.sh
```

-  Linux-Betriebssysteme Geben Sie den folgenden Befehl aus:


```
service opscenter.rc stop
```

-  Windows-Betriebssysteme Stoppen Sie den Dienst IBM Spectrum Protect Operations Center im Fenster Dienste.

## 2. Starten Sie den Web-Server.

-  AIX-Betriebssysteme Geben Sie im Verzeichnis */Installationsverzeichnis/ui/utls* (dabei gibt *Installationsverzeichnis* das Verzeichnis an, in dem das Operations Center installiert ist) den folgenden Befehl aus:

```
./startserver.sh
```

-  Linux-Betriebssysteme Geben Sie die folgenden Befehle aus:

Starten Sie den Server:

```
service opscenter.rc start
```

Starten Sie den Server erneut:

```
service opscenter.rc restart
```

Bestimmen Sie, ob der Server aktiv ist:

```
service opscenter.rc status
```

-  Windows-Betriebssysteme Starten Sie den Dienst IBM Spectrum Protect Operations Center im Fenster Dienste.

## Assistenten für die Erstkonfiguration erneut starten

---

Unter Umständen müssen Sie den Assistenten für die Erstkonfiguration im Operations Center erneut starten, um beispielsweise Konfigurationsänderungen durchzuführen.

### Vorbereitende Schritte

---

Um die folgenden Einstellungen zu ändern, verwenden Sie die Seite Einstellungen im Operations Center, anstatt den Assistenten für die Erstkonfiguration erneut zu starten:

- Häufigkeit, mit der Statusdaten aktualisiert werden
- Dauer, die Alerts aktiv, inaktiv oder geschlossen bleiben
- Bedingungen, die angeben, dass Clients gefährdet sind

Die Hilfe des Operations Center enthält weitere Informationen zum Ändern dieser Einstellungen.





### Informationen zu diesem Vorgang

---

Um den Assistenten für die Erstkonfiguration erneut zu starten, müssen Sie eine Merkmaldatei löschen, die Informationen zur Hub-Server-Verbindung enthält. Alle für den Hub-Server konfigurierten Einstellungen für Alertausgabe, Überwachung oder Gefährdung bzw. serverübergreifenden Einstellungen werden nicht gelöscht. Diese Einstellungen werden als Standardeinstellungen im Konfigurationsassistenten verwendet, wenn der Assistent erneut gestartet wird.

### Vorgehensweise

---

1. Stoppen Sie den Web-Server des Operations Center.
2. Wechseln Sie auf dem Computer, auf dem das Operations Center installiert ist, in das folgende Verzeichnis (dabei ist *Installationsverzeichnis* das Verzeichnis, in dem das Operations Center installiert ist):
  -  Linux-Betriebssysteme *Installationsverzeichnis/ui/Liberty/usr/servers/guiServer*
  -  Windows-Betriebssysteme *Installationsverzeichnis\ui\Liberty\usr\servers\guiServer*Beispiel:
  -  Linux-Betriebssysteme */opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer*
  -  Windows-Betriebssysteme *c:\Programme\Tivoli\TSM\ui\Liberty\usr\servers\guiServer*
3. Löschen Sie im Verzeichnis *guiServer* die Datei *serverConnection.properties*.
4. Starten Sie den Web-Server des Operations Center.
5. Öffnen Sie das Operations Center.
6. Rekonfigurieren Sie mithilfe des Konfigurationsassistenten das Operations Center. Geben Sie ein neues Kennwort für die Überwachungsadministrator-ID an.

7. Aktualisieren auf jedem Peripherieserver, der bereits zuvor mit dem Hub-Server verbunden war, das Kennwort für die Überwachungsadministrator-ID, indem Sie den folgenden Befehl in der IBM Spectrum Protect-Befehlszeilenschnittstelle ausgeben:

```
UPDATE ADMIN IBM-OC-Name_des_Hub-Servers neues_Kennwort
```

Einschränkung: Übernehmen Sie alle anderen Einstellungen für diese Administrator-ID unverändert. Nachdem Sie das Anfangskennwort angegeben haben, wird dieses Kennwort automatisch vom Operations Center verwaltet.

## Hub-Server ändern

---

Mithilfe des Operations Center können Sie den Hub-Server von IBM Spectrum Protect entfernen und einen anderen Hub-Server konfigurieren.

### Vorgehensweise

---

1. Starten Sie den Assistenten für die Erstkonfiguration des Operations Center erneut. Im Rahmen dieser Prozedur löschen Sie die bestehende Hub-Server-Verbindung.
2. Verwenden Sie den Assistenten, um das Operations Center für die Verbindung zu dem neuen Hub-Server zu konfigurieren.

#### Zugehörige Tasks:

Assistenten für die Erstkonfiguration erneut starten

## Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben

---

Wenn bestimmte Probleme auftreten, möchten Sie möglicherweise die Operations Center-Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben, bei dem die IBM Spectrum Protect-Server nicht als Hub- oder Peripherieserver definiert sind.

### Vorgehensweise

---

Um die Konfiguration zurückzuschreiben, führen Sie die folgenden Schritte aus:

1. Stoppen Sie den Web-Server des Operations Center.
2. Dekonfigurieren Sie den Hub-Server, indem Sie die folgenden Schritte ausführen:

- a. Geben Sie auf dem Hub-Server die folgenden Befehle aus:

```
SET MONITORINGADMIN ""
SET MONITOREDSEVERGROUP ""
SET STATUSMONITOR OFF
SET ALERTMONITOR OFF
REMOVE ADMIN IBM-OC-Name_des_Hub-Servers
```

Tipp: *IBM-OC-Name\_des\_Hub-Servers* ist die Überwachungsadministrator-ID, die bei der Erstkonfiguration des Hub-Servers automatisch erstellt wurde.

- b. Setzen Sie das Kennwort für den Hub-Server zurück, indem Sie den folgenden Befehl auf dem Hub-Server ausgeben:

```
SET SERVERPASSWORD ""
```

Achtung: Führen Sie diesen Schritt nicht aus, wenn der Hub-Server für andere Server für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation konfiguriert ist.

3. Dekonfigurieren Sie alle Peripherieserver, indem Sie die folgenden Schritte ausführen:

- a. Um zu bestimmen, ob noch Peripherieserver vorhanden sind, die als Mitglieder der Servergruppe definiert sind, geben Sie auf dem Hub-Server den folgenden Befehl aus:

```
QUERY SERVERGROUP IBM-OC-Name_des_Hub-Servers
```

Tipp: *IBM-OC-Name\_des\_Hub-Servers* ist der Name der überwachten Servergruppe, die bei der Konfiguration des ersten Peripherieservers automatisch erstellt wurde. Dieser Servergruppenname stimmt auch mit der Überwachungsadministrator-ID überein, die bei der Erstkonfiguration des Hub-Servers automatisch erstellt wurde.

- b. Um Peripherieserver aus der Servergruppe zu löschen, geben Sie auf dem Hub-Server für jeden Peripherieserver den folgenden Befehl aus:

```
DELETE GRPMEMBER IBM-OC-Name_des_Hub-Servers Name_des_Peripherieservers
```

- c. Nachdem alle Peripherieserver aus der Servergruppe gelöscht wurden, geben Sie auf dem Hub-Server die folgenden Befehle aus:

```
DELETE SERVERGROUP IBM-OC-Name_des_Hub-Servers
SET MONITOREDSEVERGROUP ""
```

d. Geben Sie auf jedem Peripherieserver die folgenden Befehle aus:

```
REMOVE ADMIN IBM-OC-Name_des_Hub-Servers
SETOPT PUSHSTATUS NO
SET ALERTMONITOR OFF
SET STATUSMONITOR OFF
```

e. Löschen Sie die Definition des Hub-Servers, indem Sie auf jedem Peripherieserver den folgenden Befehl ausgeben:

```
DELETE SERVER Name_des_Hub-Servers
```

Achtung: Führen Sie diesen Schritt nicht aus, wenn die Definition für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation verwendet wird.

f. Löschen Sie die Definition jedes Peripherieservers, indem Sie auf dem Hub-Server den folgenden Befehl ausgeben:

```
DELETE SERVER Name_des_Peripherieservers
```

Achtung: Führen Sie diesen Schritt nicht aus, wenn die Serverdefinition für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation verwendet wird.

4. Schreiben Sie die Standardeinstellungen auf jeden Server zurück, indem Sie die folgenden Befehle ausgeben:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Starten Sie den Assistenten für die Erstkonfiguration des Operations Center erneut.





#### Zugehörige Tasks:

Assistenten für die Erstkonfiguration erneut starten  
Web-Server starten und stoppen

## Virtuelle Bandarchive konfigurieren

---

Ein virtuelles Bandarchiv (VTL) verwendet keine physischen Banddatenträger. Wenn Sie VTL-Speicher implementieren, kann die Kapazität eines physischen Bandarchivs überschritten werden. Aufgrund der Möglichkeit, viele Datenträger und Laufwerke definieren zu können, kann größere Flexibilität für die Speicherumgebung bereitgestellt werden.

- Hinweise zur Verwendung virtueller Bandarchive  
Beim Definieren eines Speicherarchivs als virtuelles Bandarchiv (VTL), einschließlich Erweiterungen zur Leistungsverbesserung und Konfiguration Ihrer Hardware, sind einige Hinweise zu beachten.
- Virtuelles Bandarchiv Ihrer Umgebung hinzufügen  
Definieren Sie ein virtuelles Bandarchiv (VTL), um die Vorteile der Mountleistung und Skalierbarkeit nutzen zu können.
- Alle Laufwerke und Pfade für ein einzelnes Speicherarchiv definieren  
Verwenden Sie den Befehl PERFORM LIBACTION, um ein einzelnes SCSI-Speicherarchiv oder ein einzelnes virtuelles Bandarchiv (VTL) in einem einzigen Schritt zu konfigurieren.
-   Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit einem einzigen Laufwerkeinheitentyp konfigurieren  
Konfigurieren Sie ein VTL oder ein SCSI-Speicherarchiv, das zwei LTO-Bandlaufwerke enthält.
-   Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit mehreren Laufwerkeinheitentypen konfigurieren  
Sie können ein Speicherarchiv mit mehreren Laufwerkeinheitentypen konfigurieren, beispielsweise ein StorageTek L40-Speicherarchiv, das ein DLT-Laufwerk und ein LTO Ultrium-Laufwerk enthält.

## Hinweise zur Verwendung virtueller Bandarchive

---

Beim Definieren eines Speicherarchivs als virtuelles Bandarchiv (VTL), einschließlich Erweiterungen zur Leistungsverbesserung und Konfiguration Ihrer Hardware, sind einige Hinweise zu beachten.

### Informationen zu diesem Vorgang

---



Das Definieren eines virtuellen Bandarchivs (VTL) für den IBM Spectrum Protect-Server kann zu einer Leistungsverbesserung führen, da der Server die Mountpunktverarbeitung für VTLs anders als bei realen Bandarchiven handhabt. Die physischen Einschränkungen für reale Bandhardware gelten nicht für ein VTL, das Optionen zur besseren Skalierbarkeit bietet.

Sie können ein VTL für jedes virtuelle Bandarchiv verwenden, wenn die folgenden Bedingungen erfüllt sind:

- Für das VTL werden keine gemischten Datenträger verwendet. In dem Speicherarchiv wird nur ein einziger Typ und eine einzige Generation von Laufwerk und Datenträger emuliert.
- Jeder Server und jeder Speicheragent mit Zugriff auf das VTL hat Pfade, die für alle Laufwerke in dem Bandarchiv definiert sind.

Ist eine dieser Bedingungen nicht erfüllt, kann der Vorteil in Bezug auf die Mountleistung, der durch das Definieren eines VTL-Speicherarchivs für den IBM Spectrum Protect-Server entsteht, geringer ausfallen oder negiert werden.

VTLs sind mit früheren Versionen von Speicherarchivclients und Speicheragenten kompatibel. Der Typ von Speicherarchiv, der für Speicher verwendet wird, hat keine Auswirkungen auf den Speicherarchivclient oder den Speicheragenten. Wenn die Bedingungen in Bezug auf gemischte Datenträger und Pfad für ein SCSI-Speicherarchiv erfüllt sind, kann es mit LIBTYPE=VTL definiert oder aktualisiert werden.

- **Speicherkapazität für virtuelle Bandarchive**  
Da virtuelle Bandarchive (VTLs) nicht den physischen Einschränkungen realer Bandhardware unterliegen, ist ihre Speicherkapazität flexibler.
- **Laufwerkconfiguration für virtuelle Bandarchive**  
Abhängig von den Anforderungen Ihrer Umgebung ist die Laufwerkconfiguration in einem virtuellen Bandarchiv (VTL) variabel.

## Speicherkapazität für virtuelle Bandarchive

---

Da virtuelle Bandarchive (VTLs) nicht den physischen Einschränkungen realer Bandhardware unterliegen, ist ihre Speicherkapazität flexibler.

Das Konzept der Speicherkapazität in einem virtuellen Bandarchiv unterscheidet sich von dem in physischer Bandhardware. In einem physischen Bandarchiv hat jeder Datenträger eine definierte Kapazität und die Kapazität des Bandarchivs ist als Gesamtzahl Datenträger in dem Bandarchiv definiert. Die Kapazität eines virtuellen Bandarchivs hingegen, ist als insgesamt verfügbarer Plattenspeicherplatz definiert. Sie können die Anzahl und Größe der Datenträger auf der Platte erhöhen oder reduzieren.

Diese Variabilität hat Auswirkungen auf knappen Speicherbereich in einem virtuellen Bandarchiv. Beispielsweise kann auf einem Datenträger in einem virtuellen Bandarchiv der Speicherbereich knapp werden, bevor die zugeordnete Kapazität erreicht wird, wenn auf der zu Grunde liegenden Platte der Speicherbereich knapp wird. In dieser Situation kann der Server eine Datenträgerendenachricht empfangen, ohne dass eine Warnung ausgegeben würde, was Sicherungsfehler zur Folge hat.

Wenn Fehler aufgrund fehlenden Speicherbereichs oder Sicherungsfehler auftreten, ist in der Regel noch Plattenspeicherplatz in dem virtuellen Bandarchiv verfügbar. Er ist in Datenträgern verborgen, die nicht im Gebrauch sind. Beispielsweise werden Datenträger, die im IBM Spectrum Protect-Server logisch gelöscht oder wieder in den Arbeitsstatus versetzt werden, nur in der Serverdatenbank gelöscht. Das virtuelle Bandarchiv wird nicht benachrichtigt und verwaltet die vollständige Größe des Datenträgers gemäß der Kapazitätszuordnung.

Um zu verhindern, dass Fehler aufgrund fehlenden Speicherbereichs auftreten, müssen Sie sicherstellen, dass jedes SCSI-Speicherarchiv, das mit LIBTYPE=VTL aktualisiert wird, unter Angabe von YES für den Parameter RELABELSCRATCH aktualisiert wird. Die Option RELABELSCRATCH ermöglicht es dem Server, den Kennsatz für jeden gelöschten Datenträger zu überschreiben und im Speicherarchiv in den Arbeitsstatus zurückzusetzen. Für den Parameter RELABELSCRATCH wird standardmäßig für jedes als VTL definierte Speicherarchiv YES angenommen.

### **Zugehörige Verweise:**

UPDATE LIBRARY (Speicherarchiv aktualisieren)

## Laufwerkconfiguration für virtuelle Bandarchive

---

Abhängig von den Anforderungen Ihrer Umgebung ist die Laufwerkconfiguration in einem virtuellen Bandarchiv (VTL) variabel.

Die meisten VTL-Umgebungen verwenden so viele Laufwerke wie möglich, um die Anzahl gleichzeitig ablaufender Bandoperationen zu maximieren. Ein einzelner Bandmount in einer VTL-Umgebung erfolgt in der Regel schneller ein physischer Bandmount. Werden jedoch viele Laufwerke verwendet, verlängert sich die Zeit, die der IBM Spectrum Protect-Server benötigt, wenn ein Mount angefordert wird. Der Auswahlprozess dauert länger, da sich die Anzahl Laufwerke, die in einem einzigen Speicherarchivobjekt definiert ist, erhöht. Virtuelle Bandmounts können abhängig von der Anzahl Laufwerke in dem VTL genauso lange oder länger als physische Bandmounts dauern.

Überprüfen Sie zusammen mit Ihrem VTL-Anbieter die einheitenspezifischen Empfehlungen, um die besten Ergebnisse beim Erstellen von Laufwerken zu erzielen. Sind mehr als 300-500 Laufwerke für jedes VTL erforderlich, können Sie das VTL logisch in mehrere Speicherarchive partitionieren und jedem Speicherarchiv Laufwerke zuordnen. Möglicherweise unterliegt die Anzahl Einheiten, die innerhalb des VTL-Speicherarchivs verwendet werden können, aufgrund des Betriebssystems und der SAN-Hardwarekonfiguration gewissen Einschränkungen.

## Virtuelles Bandarchiv Ihrer Umgebung hinzufügen

---

Definieren Sie ein virtuelles Bandarchiv (VTL), um die Vorteile der Mountleistung und Skalierbarkeit nutzen zu können.

### Informationen zu diesem Vorgang

---

VTLs werden mithilfe des Befehls `DEFINE LIBRARY` unter Angabe des Parameters `LIBTYPE=VTL` angegeben. Da ein VTL-Speicherarchiv funktional mit dem Server auf dieselbe Art und Weise wie ein SCSI-Speicherarchiv interagiert, können Sie den Befehl `UPDATE LIBRARY` verwenden, um den Speicherarchivtyp eines bereits definierten SCSI-Speicherarchivs zu ändern. Sie müssen das Speicherarchiv nicht erneut definieren.

### Vorgehensweise

---

- Fügen Sie ein neues VTL-Speicherarchiv hinzu. Definieren Sie ein Speicherarchiv wie in dem folgenden Beispiel gezeigt als ein VTL für den Server:

```
define library chester libtype=vtl
```

Damit wird das neue VTL-Speicherarchiv konfiguriert und die Option `RELABELSCRATCH` aktiviert, damit Datenträgern, die gelöscht und wieder in den Arbeitsstatus versetzt wurden, ein neuer Kennsatz zugeordnet werden kann.

- Ändern Sie ein SCSI-Speicherarchiv in ein VTL. Wenn ein SCSI-Speicherarchiv vorhanden ist, das in ein VTL-Speicherarchiv geändert werden soll, verwenden Sie den Befehl `UPDATE LIBRARY`, um den Speicherarchivtyp zu ändern:

```
update library calzone libtype=vtl
```

Sie können diesen Befehl nur ausgeben, wenn das Speicherarchiv, das aktualisiert wird, mit dem Parameter `LIBTYPE=SCSI` definiert ist.

#### Zugehörige Verweise:

`DEFINE LIBRARY` (Speicherarchiv definieren)

`UPDATE LIBRARY` (Speicherarchiv aktualisieren)

## Alle Laufwerke und Pfade für ein einzelnes Speicherarchiv definieren

---

Verwenden Sie den Befehl `PERFORM LIBACTION`, um ein einzelnes SCSI-Speicherarchiv oder ein einzelnes virtuelles Bandarchiv (VTL) in einem einzigen Schritt zu konfigurieren.

### Informationen zu diesem Vorgang

---

Wenn Sie Ihre Hardwareumgebung konfigurieren oder ändern und eine große Anzahl Laufwerkdefinitionen erstellen oder ändern müssen, kann diese Task durch die Verwendung des Befehls `PERFORM LIBACTION` erheblich vereinfacht werden. Sie können ein neues Speicherarchiv definieren und dann alle Laufwerke und Pfade zu den Laufwerken definieren. Wenn ein vorhandenes Speicherarchiv gelöscht werden soll, können Sie alle vorhandenen Laufwerke und ihre zugehörigen Pfade auch in einem einzigen Schritt löschen.

Mit dem Parameter `PREVIEW` können Sie die Ausgabe der Befehle vor ihrer Verarbeitung anzeigen, um die Aktion, die ausgeführt werden soll, zu überprüfen. Wenn Sie ein Speicherarchiv definieren, muss bereits ein Pfad zu dem Speicherarchiv definiert sein, wenn der Parameter `PREVIEW` angegeben werden soll. Die Parameter `PREVIEW` und `DEVICE` können nicht zusammen verwendet werden.

Der Befehl `PERFORM LIBACTION` kann nur für SCSI- und VTL-Speicherarchive verwendet werden. Wenn Sie Laufwerke und Pfade für ein Speicherarchiv definieren, muss die Option `SANDISCOVERY` unterstützt werden und aktiviert sein. Das Bandarchiv muss die Zuordnung zwischen Laufwerkseriennummer und Laufwerkadresse zurückgeben können.

### Vorgehensweise

---

Um ein VTL-Speicherarchiv mit dem Namen `ODIN` zu konfigurieren, führen Sie diese Schritte aus:

1. Definieren Sie das Speicherarchiv.

```
define library odin libtype=vtl
```

## 2. Definieren Sie zwei Laufwerke und die zugehörigen Pfade für Ihr neues Speicherarchiv ODIN.

### AIX-Betriebssysteme

```
perform libaction odin action=define device=/dev/lb3 prefix=dr
```

Der Server gibt dann die folgenden Befehle aus:

```
define path tsmserver odin srct=server destt=library device=/dev/
lb3 define drive odin dr0
define path tsmserver dr0 srct=server destt=drive library=odin
device=/dev/mt1 define drive odin dr1
define path tsmserver dr1 srct=server destt=drive library=odin
device=/dev/mt2
```

### Linux-Betriebssysteme

```
perform libaction odin action=define device=/dev/tmsmcsi/lb3 prefix=dr
```

Der Server gibt dann die folgenden Befehle aus:

```
define path tsmserver odin srct=server destt=library device=/dev/tmsmcsi/lb3
define drive odin dr0
define path tsmserver dr0 srct=server destt=drive library=odin
device=/dev/tmsmcsi/mt1 define drive odin dr1
define path tsmserver dr1 srct=server destt=drive library=odin
device=/dev/tmsmcsi/mt2
```

### Windows-Betriebssysteme

```
perform libaction odin action=define device=lb0.0.0.2 prefix=dr
```

Der Server gibt dann die folgenden Befehle aus:

```
define path tsmserver odin srct=server destt=library device=lb0.0.0.2
define drive odin dr0
define path tsmserver dr0 srct=server destt=drive library=odin
device=mt0.1.0.2 define drive odin dr1
define path tsmserver dr1 srct=server destt=drive library=odin
device=mt0.2.0.2
```

#### Zugehörige Verweise:

DEFINE LIBRARY (Speicherarchiv definieren)

DEFINE PATH (Pfad definieren, wenn Ziel ein Laufwerk ist)

PERFORM LIBACTION (Alle Laufwerke und Pfade für ein Speicherarchiv definieren oder löschen)

## Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit einem einzigen Laufwerkeinheitentyp konfigurieren

---

Konfigurieren Sie ein VTL oder ein SCSI-Speicherarchiv, das zwei LTO-Bandlaufwerke enthält.

### Informationen zu diesem Vorgang

---

Diese Prozedur ist ein Beispiel für die Konfiguration eines automatisierten SCSI-Speicherarchivs, das zwei Laufwerke enthält, für das Serversystem. Das Speicherarchiv wird nicht mit anderen IBM Spectrum Protect-Servern oder Speicheragenten gemeinsam genutzt und ist normalerweise über SCSI-Kabel an das Serversystem angeschlossen.

In dieser Konfiguration haben beide Laufwerke in dem Speicherarchiv denselben Einheitentyp. Definieren Sie exakt eine Einheitenklasse. Die Vorgehensweise ist bis auf den Schritt zum Definieren des Speicherarchivs für SCSI-Speicherarchive und VTLs identisch. Definieren Sie für SCSI-Speicherarchive das Speicherarchiv mit `libtype=scsi`. Definieren Sie für VTL-Speicherarchive das Speicherarchiv mit `libtype=vtl`.

### Vorgehensweise

---


#### 1. Definieren Sie ein SCSI-Speicherarchiv mit dem Namen AUTODTLIB.

```
define library autoltolib libtype=scsi
```

Wenn das Speicherarchiv einen Barcodeleser hat und Bändern automatisch Kennsätze zugeordnet werden sollen, bevor sie zurückgestellt werden, können Sie den Parameter AUTOLABEL auf YES setzen. Beispiel:

```
define library autoltolib libtype=scsi autolabel=yes
```

2. Definieren Sie einen Pfad vom Server zum Speicherarchiv.

 AIX-Betriebssysteme

```
define path server1 autoltolib srctype=server desttype=library
device=/dev/lb3
```

 Linux-Betriebssysteme

```
define path server1 autoltolib srctype=server desttype=library
device=/dev/tmscsi/lb3
```

 Windows-Betriebssysteme

```
define path server1 autoltolib srctype=server desttype=library
device=lb0.0.0.3
```

3. Definieren Sie die Laufwerke im Speicherarchiv. Beide Laufwerke gehören zum Speicherarchiv AUTODTLIB.

```
define drive autoltolib drive01
define drive autoltolib drive02
```

Tipp: Mithilfe des Befehls `PERFORM LIBACTION` können Sie Laufwerke und Pfade für ein Speicherarchiv in einem einzigen Schritt definieren.

4. Definieren Sie einen Pfad vom Server zu jedem Laufwerk.

 AIX-Betriebssysteme

```
define path server1 drive01 srctype=server desttype=drive
library=autoltolib device=/dev/mt4
define path server1 drive02 srctype=server desttype=drive
library=autoltolib device=/dev/mt5
```

 Linux-Betriebssysteme

```
define path server1 drive01 srctype=server desttype=drive
library=autoltolib device=/dev/tmscsi/mt4
define path server1 drive02 srctype=server desttype=drive
library=autoltolib device=/dev/tmscsi/mt5
```

 Windows-Betriebssysteme

```
define path server1 drive01 srctype=server desttype=drive
library=autoltolib device=mt0.0.0.4
define path server1 drive02 srctype=server desttype=drive
library=autoltolib device=mt0.0.0.5
```

Wurde die Elementadresse bei der Definition des Laufwerks nicht angegeben, fragt der Server jetzt das Speicherarchiv nach der Standardelementadresse des Laufwerks ab.

5. Definieren Sie eine Einheitenklasse mit dem Namen `AUTODLT_CLASS` für die beiden Laufwerke im Speicherarchiv `AUTODTLIB`.

```
define devclass autolto_class library=autodtlib devtype=lto
```

6. Definieren Sie einen Speicherpool mit dem Namen `AUTOLTO_POOL`, der der Einheitenklasse mit dem Namen `AUTOLTO_CLASS` zugeordnet ist.

```
define stgpool autolto_pool autolto_class maxscratch=20
```

7. Ordnen Sie Datenträgern im Speicherarchiv Kennsätze zu und stellen Sie die Datenträger zurück.

```
label libvolume autoltolib search=yes labelsource=barcode checkin=scratch
```

8. Überprüfen Sie Ihre Definitionen, indem Sie die folgenden Befehle ausgeben:

```
query library
query drive
query path
query devclass
query stgpool
query libvolume
```

**Zugehörige Verweise:**

DEFINE DEVCLASS (Einheitenklasse definieren)

DEFINE LIBRARY (Speicherarchiv definieren)

DEFINE PATH (Pfad definieren, wenn Ziel ein Laufwerk ist)

# Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit mehreren Laufwerkeinheitentypen konfigurieren

Sie können ein Speicherarchiv mit mehreren Laufwerkeinheitentypen konfigurieren, beispielsweise ein StorageTek L40-Speicherarchiv, das ein DLT-Laufwerk und ein LTO Ultrium-Laufwerk enthält.

## Informationen zu diesem Vorgang

Diese Prozedur ist ein Beispiel für die Konfiguration eines automatisierten SCSI-Speicherarchivs, das zwei Laufwerke enthält, für das Serversystem. Das Speicherarchiv wird nicht mit anderen IBM Spectrum Protect-Servern oder Speicheragenten gemeinsam genutzt und ist normalerweise über SCSI-Kabel an das Serversystem angeschlossen.

In dieser Konfiguration haben die Laufwerke unterschiedliche Einheitentypen. Definieren Sie für jeden Laufwerkeinheitentyp eine Einheitenklasse. Laufwerke mit verschiedenen Einheitentypen werden in einem einzelnen Speicherarchiv unterstützt, wenn Sie für jeden Laufwerktyp eine Einheitenklasse definieren. Wenn die Konfiguration auf diese Art und Weise erfolgt, müssen Sie das spezifische Format für den Einheitentyp des Laufwerks einschließen, indem Sie den Parameter FORMAT mit einem anderen Wert als DRIVE verwenden.

Die Vorgehensweise ist bis auf den Schritt zum Definieren des Speicherarchivs für SCSI-Speicherarchive und VTLs identisch. Definieren Sie für SCSI-Speicherarchive das Speicherarchiv mit `libtype=scsi`. Definieren Sie für VTL-Speicherarchive das Speicherarchiv mit `libtype=vtl`.

## Vorgehensweise

1. Definieren Sie ein SCSI-Speicherarchiv mit dem Namen MIXEDLIB.

```
define library mixedlib libtype=scsi
```

2. Definieren Sie einen Pfad vom Server zum Speicherarchiv.

 AIX-Betriebssysteme

```
define path server1 mixedlib srctype=server desttype=library  
device=/dev/lb3
```

 Linux-Betriebssysteme

```
define path server1 mixedlib srctype=server desttype=library  
device=/dev/tmsmcsi/lb3
```


 Windows-Betriebssysteme

```
define path server1 mixedlib srctype=server desttype=library  
device=lb0.0.0.3
```

3. Definieren Sie die Laufwerke im Speicherarchiv. Beide Laufwerke gehören zum Speicherarchiv MIXEDLIB.

```
define drive mixedlib dlt1  
define drive mixedlib lto1
```

4. Definieren Sie einen Pfad vom Server zu jedem Laufwerk. Der Parameter DEVICE gibt den Namen des Einheitentreibers für das Laufwerk an; dabei handelt es sich um den Gerätedateinamen für die Einheit.

 AIX-Betriebssysteme

```
define path server1 dlt1 srctype=server desttype=drive  
library=mixedlib device=/dev/mt4  
define path server1 lto1 srctype=server desttype=drive  
library=mixedlib device=/dev/mt5
```

 Linux-Betriebssysteme

```
define path server1 dlt1 srctype=server desttype=drive  
library=mixedlib device=/dev/tmsmcsi/mt4  
define path server1 lto1 srctype=server desttype=drive  
library=mixedlib device=/dev/tmsmcsi/mt5
```

 Windows-Betriebssysteme

```
define path server1 drive01 srctype=server desttype=drive  
library=autoltolib device=mt0.0.0.4  
define path server1 drive02 srctype=server desttype=drive  
library=autoltolib device=mt0.0.0.5
```

Wurde die Elementadresse bei der Definition des Laufwerks nicht angegeben, fragt der Server jetzt das Speicherarchiv nach der Elementadresse des Laufwerks ab.

5. Definieren Sie Einheitenklassen.

Wichtig: Verwenden Sie nicht das Standardformat DRIVE. Da die Laufwerke verschiedene Typen haben, verwendet der Server die Formatspezifikation für die Auswahl eines Laufwerks. Das Ergebnis der Verwendung des Formats DRIVE in einem Speicherarchiv mit gemischten Datenträgern ist unvorhersehbar.

```
define devclass dlt_class library=mixedlib devtype=dlt format=dlt40
define devclass lto_class library=mixedlib devtype=lto format=ultriumc
```

6. Definieren Sie Speicherpools, die den Einheitenklassen zugeordnet sind.

```
define stgpool lto_pool lto_class maxscratch=20
define stgpool dlt_pool dlt_class maxscratch=20
```

7. Ordnen Sie Datenträgern im Speicherarchiv Kennsätze zu und stellen Sie die Datenträger zurück.

```
label libvolume mixedlib search=yes labelsource=barcode checkin=scratch
```

8. Überprüfen Sie Ihre Definitionen, indem Sie die folgenden Befehle ausgeben:

```
query library
query drive
query path
query devclass
query stgpool
query libvolume
```

## NAS-Dateiserver schützen

Sie können eine Sicherungsumgebung, die einen NAS-Dateiserver schützt, konfigurieren und verwalten.

Sie können den IBM Spectrum Protect-Server, den IBM Spectrum Protect-Client für Sichern/Archivieren oder IBM Spectrum Protect Snapshot wie in der folgenden Tabelle beschrieben zum Sichern und Zurückschreiben eines NAS-Dateiservers verwenden.

| Produkt   | Beschreibung  |
|---|---|
| IBM Spectrum Protect-Server                         | <p>Um NAS-Dateiserverdaten mithilfe des IBM Spectrum Protect-Servers sichern und zurückschreiben zu können, muss IBM Spectrum Protect Extended Edition installiert sein.</p> <p>Sie können den IBM Spectrum Protect-Server für die Verwendung von NDMP (Network Data Management Protocol) wie in den folgenden Themen in diesem Abschnitt beschrieben zum Sichern und Zurückschreiben von Daten konfigurieren.</p> <p>Um große NetApp-Dateisysteme zu schützen, können Sie auch stattdessen IBM Spectrum Protect für die Verwendung der NetApp-Funktion 'SnapMirror to Tape' (die auch als SMTape bekannt ist) konfigurieren. 'SnapMirror to Tape' verwendet eine Datenkopie auf Blockebene für die Sicherung, die schneller als eine traditionelle NDMP-Gesamtsicherung ist und verwendet werden kann, wenn NDMP-Gesamtsicherungen nicht geeignet sind.</p> <p>Informationen zur Verwendung der Funktion 'SnapMirror to Tape' zum Sichern und Zurückschreiben von Daten finden Sie in Sicherungs- und Zurückschreibungsoperationen mit der NetApp-Funktion 'SnapMirror to Tape'.</p> |
| IBM Spectrum Protect-Client für Sichern/Archivieren | <p>Sie können den -Client für Sichern/Archivieren zum Sichern und Zurückschreiben von Dateiserverdaten mithilfe des NFS-Protokolls (NFS = Network File System) oder des CIFS-Protokolls (CIFS = Common Internet File System) konfigurieren.</p> <p>Informationen zur Verwendung des Clients für Sichern/Archivieren zum Sichern und Zurückschreiben von Daten finden Sie in Daten mit Clients für Sichern/Archivieren sichern und zurückschreiben.</p>  |
| IBM Spectrum Protect Snapshot                       | <p>Sie können IBM Spectrum Protect Snapshot zum Sichern und Zurückschreiben von Dateiserverdaten verwenden, indem Sie die erweiterten Momentaufnahmetechnologien der Speichersysteme verwenden.</p> <p>Informationen zur Verwendung von IBM Spectrum Protect Snapshot zum Sichern und Zurückschreiben von Daten finden Sie in Übersicht über IBM Spectrum Protect Snapshot for UNIX and Linux oder Übersicht über IBM Spectrum Protect Snapshot for VMware.</p>   |

- NDMP-Anforderungen  
Um NDMP für Operationen mit NAS-Dateiservern verwenden zu können, muss IBM Spectrum Protect Extended Edition installiert sein und Ihre Dateiserverumgebung muss bestimmte Voraussetzungen erfüllen.
- Verwaltung von NDMP-Operationen  
Es gibt mehrere Administratoraktivitäten für NDMP-Operationen.

- IBM Spectrum Protect für NDMP-Operationen konfigurieren  
Sie können IBM Spectrum Protect zum Sichern und Wiederherstellen von Daten auf NAS-Dateiservern mithilfe von NDMP konfigurieren. Die Konfigurationsprozedur ist abhängig davon, ob Daten von einem NAS-Dateiserver ohne oder mit Clustering gesichert werden sollen, unterschiedlich.
- NAS-Dateiserver mithilfe von NDMP sichern und zurückschreiben  
Nach der Konfiguration von IBM Spectrum Protect für NDMP-Operationen können Sie mit der Verwendung von NDMP beginnen.
- Sicherung und Zurückschreibung auf Dateiebene für NDMP-Operationen  
Wenn Sie Daten mit NDMP sichern, können Sie angeben, dass der IBM Spectrum Protect-Server Informationen auf Dateiebene erfasst und in einem Inhaltsverzeichnis (TOC) speichert.
- Sicherungs- und Zurückschreibungsoperationen auf Verzeichnisebene  
Wenn Sie über ein großes NAS-Dateisystem verfügen, werden durch das Einleiten einer Sicherung auf Verzeichnisebene Sicherungs- und Zurückschreibungszeiten reduziert und größere Flexibilität beim Konfigurieren von NAS-Sicherungen bereitgestellt. Durch das Definieren virtueller Dateibereiche kann eine Dateisystemsicherung auf mehrere NDMP-Sicherungsoperationen und auf mehrere Bandlaufwerke verteilt werden. Sie können auch verschiedene Sicherungszeitpläne verwenden, um Unterverzeichnisstrukturen eines Dateisystems zu sichern.
- Sicherungs- und Zurückschreibungsoperationen mit der NetApp-Funktion 'SnapMirror to Tape'  
Sie können große NetApp-Dateisysteme mithilfe der NetApp-Funktion 'SnapMirror to Tape' (die auch als 'SMTape' bekannt ist) sichern. Durch die Verwendung einer Datenkopie auf Blockebene für die Sicherung ist die Methode 'SnapMirror to Tape' schneller als eine traditionelle NDMP-Gesamtsicherung und kann verwendet werden, wenn NDMP-Gesamtsicherungen nicht geeignet sind.
- NDMP-Sicherungsoperationen mithilfe von in Celerra-Dateiserver integrierten Prüfpunkten  
Wenn der IBM Spectrum Protect-Server eine NDMP-Sicherungsoperation auf einer Celerra-Einheit zum Versetzen von Daten einleitet, kann die Sicherung eines umfangreichen Dateisystems mehrere Stunden dauern. Ohne integrierte Celerra-Prüfpunkte werden alle auf dem Dateisystem vorgenommenen Änderungen in das Sicherungsimago geschrieben.
- NAS-Knoten replizieren  
Sie können einen NAS-Knoten, der NDMP für Sicherungsoperationen verwendet, replizieren. Machen Sie sich, bevor Sie die Replikationsoperation konfigurieren, mit den geltenden Einschränkungen vertraut.

## NDMP-Anforderungen

---

Um NDMP für Operationen mit NAS-Dateiservern verwenden zu können, muss IBM Spectrum Protect Extended Edition installiert sein und Ihre Dateiserverumgebung muss bestimmte Voraussetzungen erfüllen.

### NAS-Dateiserver

Das Betriebssystem auf dem Dateiserver muss von IBM Spectrum Protect unterstützt werden. Informationen zu den unterstützten NAS-Dateiservern finden Sie in Technote 1054144.

Die Kombination aus Dateiservermodell und Betriebssystem muss vom NAS-Dateiserver unterstützt werden. Weitere Spezifikationen enthält die Produktinformation für den NAS-Dateiserver.

### Bandarchive

Diese Anforderung gilt nur für eine Sicherung auf einer lokal angeschlossenen NAS-Einheit. Der IBM Spectrum Protect-Server unterstützt die folgenden Speicherarchivtypen für NDMP-Operationen:

#### SCSI

Ein SCSI-Speicherarchiv kann direkt an den IBM Spectrum Protect-Server oder an den NAS-Dateiserver angeschlossen werden. Wenn das Speicherarchiv direkt an den IBM Spectrum Protect-Server angeschlossen wird, steuert dieser Server die Speicherarchivoperationen, indem die SCSI-Befehle direkt an das Speicherarchiv übergeben werden. Wenn das Speicherarchiv direkt an den NAS-Dateiserver angeschlossen wird, steuert der IBM Spectrum Protect-Server das Speicherarchiv, indem SCSI-Befehle über den NAS-Dateiserver an das Speicherarchiv übergeben werden.

#### ACSLs

Ein ACSLS-Speicherarchiv kann direkt an den IBM Spectrum Protect-Server angeschlossen werden. Der IBM Spectrum Protect-Server steuert das Speicherarchiv, indem die Speicherarchivanforderung über TCP/IP an den Speicherarchivsteuerungsserver übergeben wird.  
Einschränkung: Der IBM Spectrum Protect-Server verfügt nicht über Unterstützung für externe Speicherarchive für das ACSLS-Speicherarchiv, wenn das Speicherarchiv für NDMP-Operationen verwendet wird.

#### VTL

Ein virtuelles Bandarchiv (VTL) kann direkt an den IBM Spectrum Protect-Server oder an den NAS-Dateiserver angeschlossen werden. Ein virtuelles Bandarchiv ist im Grunde ein SCSI-Speicherarchiv, das aber gemäß den Merkmalen virtueller Bandarchive funktional erweitert wurde und eine bessere Mountleistung ermöglicht.  
Wenn Sie ein VTL definieren, darf Ihre Umgebung keine gemischten Datenträger umfassen. Pfade müssen zwischen allen Laufwerken in dem Speicherarchiv und allen definierten Servern, einschließlich Speicheragenten, die das Speicherarchiv verwenden, definiert sein. Wenn diese Bedingungen nicht erfüllt sind, kann sich die Gesamtleistung insbesondere während Zeiten mit hoher Belastung auf dieselbe Leistungsstufen wie bei Speicherarchiven des Typs SCSI verschlechtern.

349X

Ein 349X-Speicherarchiv kann direkt nur an den IBM Spectrum Protect-Server angeschlossen werden. Der IBM Spectrum Protect-Server steuert das Speicherarchiv, indem die Speicherarchivanforderung über TCP/IP an den Speicherarchivmanager übergeben wird.

**Gemeinsame Speicherarchivnutzung:** Bei dem IBM Spectrum Protect-Server, der NDMP-Operationen ausführt, kann es sich um einen Speicherarchivmanager für ein ACSLS-, SCSI-, VTL- oder 349X-Speicherarchiv handeln, jedoch nicht um einen Speicherarchivclient. Der IBM Spectrum Protect-Server kann auch ein Speicherarchivclient sein; dies ist in einer Konfiguration der Fall, bei der der NAS-Dateiserver Daten unter Verwendung von TCP/IP an den Server und nicht an ein Bandarchiv sendet, das an den Dateiserver angeschlossen ist. Wenn der IBM Spectrum Protect-Server, der NDMP-Operationen ausführt, ein Speicherarchivmanager ist, muss dieser Server das Speicherarchiv direkt steuern und nicht durch die Übergabe von Befehlen über den NAS-Dateiserver.

#### Bandlaufwerke

Ein Bandlaufwerk ist nur für die Sicherung auf einer lokal angeschlossenen NAS-Einheit erforderlich. Der NAS-Dateiserver muss Zugriff auf die Laufwerke haben. Eine NAS-Einheit wird in einem Speicherarchiv mit gemischten Einheiten nicht unterstützt. Bei den Laufwerken muss Unterstützung für Bandsicherungsoperationen durch den NAS-Dateiserver und das dazugehörige Betriebssystem vorliegen. Die Produktdokumentation zum NAS-Dateiserver enthält ausführliche Informationen zur NDMP-Einheitenunterstützung.

**Gemeinsame Laufwerknutzung:** Die Bandlaufwerke können vom IBM Spectrum Protect-Server und einem oder mehreren NAS-Dateiservern gemeinsam genutzt werden. Wenn ein SCSI-, VTL- oder 349X-Speicherarchiv an den Server und nicht an den NAS-Dateiserver angeschlossen ist, können außerdem die Laufwerke mit einem oder mehreren NAS-Dateiservern gemeinsam genutzt werden. Die Laufwerke können auch von einem oder mehreren IBM Spectrum Protect-Speicherarchivclients und Speicheragenten gemeinsam genutzt werden.

**Laufwerkreservierungen:** Wenn Bandlaufwerke an NAS-Einheiten angeschlossen sind und der Parameter RESETDRIVES=YES für den Befehl DEFINE LIBRARY angegeben ist gelten die folgenden Einschränkungen:

- Wenn ein Bandlaufwerk von einem IBM Spectrum Protect-Server und einer NAS-Einheit gemeinsam genutzt wird, wird die Zurückstellung der Laufwerkreservierung unterstützt, wenn die NAS-Einheit die persistente Reserve unterstützt und diese aktiviert ist. Weitere Informationen zum Definieren der persistenten Reserve enthält die Dokumentation zu Ihrer NAS-Einheit.
- Wenn ein Bandlaufwerk nur an eine NAS-Einheit angeschlossen ist und nicht mit einem IBM Spectrum Protect-Server gemeinsam genutzt wird, wird die Zurückstellung der Laufwerkreservierung nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung durch die NAS-Einheit definiert, aber nie gelöscht wird, müssen Sie eine andere Methode zum Löschen der Reservierung verwenden.

Klären Sie die Kompatibilität bestimmter Kombinationen aus NAS-Dateiserver, Bändeinheiten und an ein SAN angeschlossener Einheiten mit dem Hersteller der Hardware ab.

**Tipp:** IBM Spectrum Protect unterstützt NDMP Version 4 für alle NDMP-Operationen. IBM Spectrum Protect unterstützt weiterhin alle NDMP-Sicherungs- und -Zurückschreibungsoperationen mit einer NAS-Einheit, auf der NDMP Version 3 ausgeführt wird. Der IBM Spectrum Protect-Server vereinbart mit dem NDMP-Server die höchste Protokollversion (entweder Version 3 oder Version 4), wenn er eine NDMP-Verbindung aufbaut. Treten bei Verwendung von Version 4 Probleme auf, können Sie versuchsweise Version 3 verwenden.

- **Schnittstellen für NDMP-Operationen**  
Sie können verschiedene Schnittstellen zur Ausführung von NDMP-Operationen verwenden. Sie können eine NDMP-Operation mit dem Befehl BACKUP NODE oder RESTORE NODE planen und einen Zeitplan für die Verarbeitung des Befehls erstellen.
- **Datenformate für NDMP-Sicherungsoperationen**  
Daten, die mithilfe von NDMP gesichert werden, haben nicht dasselbe Format wie die Daten, die für typische IBM Spectrum Protect-Sicherungsoperationen verwendet werden. Der NAS-Dateiserver steuert das Format der Sicherungsdaten.

## Schnittstellen für NDMP-Operationen

---

Sie können verschiedene Schnittstellen zur Ausführung von NDMP-Operationen verwenden. Sie können eine NDMP-Operation mit dem Befehl BACKUP NODE oder RESTORE NODE planen und einen Zeitplan für die Verarbeitung des Befehls erstellen.

#### Clientschnittstellen:

- Befehlszeilenclient für Sichern/Archivieren (auf einem Windows, AIX (64-Bit) oder Oracle Solaris-System (64-Bit))
- Web-Client

#### Serverschnittstellen:

- Serverkonsole
  - Befehlszeile auf dem Verwaltungsclient
- Tipp: Alle Beispiele für NDMP-Operationen verwenden Serverbefehle.

Bei der IBM Spectrum Protect-Web-Client-Schnittstelle, die mit dem Client für Sichern/Archivieren verfügbar ist, werden die Dateisysteme des NAS-Dateiservers in einer grafischen Sicht angezeigt. Die Clientfunktion ist nicht erforderlich, aber die



Clientschnittstellen können für NDMP-Operationen verwendet werden. Die Clientfunktion ist die bevorzugte Methode für Zurückschreibungsoperationen auf Dateiebene. Weitere Informationen zu Zurückschreibungsoperationen auf Dateiebene finden Sie in Sicherung und Zurückschreibung auf Dateiebene für NDMP-Operationen.

IBM Spectrum Protect fordert Sie zur Eingabe einer Administrator-ID und des zugehörigen Kennworts auf, wenn Sie NDMP-Funktionen mit einer der Clientschnittstellen ausführen. Weitere Informationen zum Installieren und Aktivieren von Clientschnittstellen finden Sie in IBM Spectrum Protect-Clients für Sichern/Archivieren installieren.

Um den IBM Spectrum Protect-Client für Sichern/Archivieren oder den Web-Client für NAS-Operationen verwenden zu können, muss das erste Zeichen der Dateisystemnamen auf der NAS-Einheit ein Schrägstrich (/) sein. Diese Einschränkung hat keine Auswirkungen auf NAS-Operationen, die über die IBM Spectrum Protect-Serverbefehlszeile gestartet werden.

## Datenformate für NDMP-Sicherungsoperationen

Daten, die mithilfe von NDMP gesichert werden, haben nicht dasselbe Format wie die Daten, die für typische IBM Spectrum Protect-Sicherungsoperationen verwendet werden. Der NAS-Dateiserver steuert das Format der Sicherungsdaten.

Daten, die in einem Speicherarchiv gesichert werden, das direkt an den Dateiserver angeschlossen ist, müssen in einen Speicherpool mit dem korrekten Datenformat übertragen werden. Wenn Sie einen Speicherpool für NDMP-Operationen definieren, geben Sie eines der folgenden Datenformate an:

- NETAPPDUMP, wenn der NAS-Dateiserver eine NetApp-Einheit oder eine IBM® System Storage N Series-Einheit ist
- CELERRADUMP, wenn der NAS-Dateiserver eine EMC Celerra-Einheit ist
- NDMPDUMP für alle anderen Einheiten

Daten, die über das Netz in der lokalen IBM Spectrum Protect-Hierarchie gesichert werden, können an jeden beliebigen primären Speicherpool mit wahlfreiem oder sequenziellem Zugriff übertragen werden. Das Format der Daten ändert sich jedoch nicht.

## Verwaltung von NDMP-Operationen

Es gibt mehrere Administratoraktivitäten für NDMP-Operationen.

- NAS-Dateiserverknoten verwalten  
Sie können NAS-Dateiserverknoten abfragen, aktualisieren, umbenennen und entfernen.
- In NDMP-Operationen verwendete Einheiten zum Versetzen von Daten verwalten  
Sie können die für NAS-Dateiserver definierten Einheiten zum Versetzen von Daten abfragen, aktualisieren und löschen.
- IBM Spectrum Protect-Laufwerk für NDMP-Operationen dedizieren  
Wenn Sie bereits ein Laufwerk für IBM Spectrum Protect-Operationen verwenden, können Sie dieses Laufwerk für NDMP-Operationen dedizieren.
- Speicherpoolverwaltung für NDMP-Operationen  
Wenn NETAPPDUMP, CELERRADUMP oder NDMPDUMP als Speicherpooltyp angegeben wird, unterscheidet sich die Verwaltung von Speicherpools, die von NDMP-Operationen erstellt werden, von der Verwaltung von Speicherpools, die Datenträger für traditionelle IBM Spectrum Protect-Sicherungen enthalten.
- Inhaltsverzeichnisse verwalten  
Sie können mehrere Befehle für die Verwaltung unterschiedlicher Aspekte Ihres Dateninhalts verwenden.
- Schließen inaktiver NDMP-Verbindungen mit langer Laufzeit verhindern  
Um zu verhindern, dass Firewalls inaktive NDMP-Verbindungen mit langer Laufzeit schließen, können Sie den TCP-Keepalive-Mechanismus auf den NDMP-Steuerverbindungen aktivieren.

## NAS-Dateiserverknoten verwalten

Sie können NAS-Dateiserverknoten abfragen, aktualisieren, umbenennen und entfernen.

### Vorgehensweise

Verwenden Sie einen der folgenden Befehle, um NAS-Dateiserverknoten zu verwalten:

| Befehl            | Prozedur   |
|-------------------|--|
| <b>QUERY NODE</b> | Um einen Knoten abzufragen, geben Sie den Befehl QUERY NODE mit den entsprechenden Parametern aus. Wenn beispielsweise der NAS-Knoten NASNODE1 abgefragt werden soll, geben Sie den folgenden Befehl aus:<br><br><code>query node nasnode1 type=nas</code> |

| Befehl             | Prozedur   |
|--------------------|--|
| <b>UPDATE NODE</b> | <p>Um einen Knoten zu aktualisieren, geben Sie den Befehl UPDATE NODE mit den entsprechenden Parametern aus. Wenn Sie beispielsweise eine neue Maßnahmendomäne mit dem Namen NASDOMAIN für NAS-Knoten erstellt haben und der Knoten NASNODE1 aktualisiert werden soll, um ihn in die neue Domäne einzuschließen, geben Sie den folgenden Befehl aus:</p> <pre>update node nasnode1 domain=nasdomain</pre>  |
| <b>RENAME NODE</b> | <p>Zum Umbenennen eines NAS-Knotens müssen Sie auch die zugehörige NAS-Einheit zum Versetzen von Daten umbenennen, da beide denselben Namen haben müssen.</p> <p>Um beispielsweise NASNODE1 in NAS1 umzubenennen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Löschen Sie alle Pfade zwischen der Einheit NASNODE1 zum Versetzen von Daten und den Speicherarchiven sowie zwischen der Einheit NASNODE1 zum Versetzen von Daten und den Laufwerken.</li> <li>2. Löschen Sie die für den NAS-Knoten definierte Einheit zum Versetzen von Daten.</li> <li>3. Geben Sie folgenden Befehl aus, um NASNODE1 in NAS1 umzubenennen: <pre>rename node nasnode1 nas1</pre> </li> <li>4. Definieren Sie die Einheit zum Versetzen von Daten unter Verwendung des neuen Knotennamens. In diesem Beispiel müssen Sie eine neue Einheit zum Versetzen von Daten mit dem Namen NAS1 mit denselben Parametern definieren, die beim Definieren von NASNODE1 verwendet wurden. Wichtig: Wenn Sie eine neue Einheit zum Versetzen von Daten für einen umbenannten Knoten definieren, stellen Sie sicher, dass der Name der Einheit zum Versetzen von Daten mit dem neuen Knotennamen übereinstimmt. Stellen Sie außerdem sicher, dass die Parameter für die neue Einheit zum Versetzen von Daten mit den Parametern der ursprünglichen Einheit zum Versetzen von Daten identisch sind. Wenn der Knotenname nicht mit dem Namen der Einheit zum Versetzen von Daten übereinstimmt bzw. die Parameter der neuen Einheit zum Versetzen von Daten nicht identisch mit den Parametern der ursprünglichen Einheit zum Versetzen von Daten sind, kann unter Umständen keine Sitzung mit dem NAS-Dateiserver aufgebaut werden.</li> <li>5. Definieren Sie für SCSI- oder 349X-Speicherarchive nur dann einen Pfad zwischen der NAS-Einheit zum Versetzen von Daten und einem Speicherarchiv, wenn das Bandarchiv physisch über eine Direktverbindung mit dem NAS-Dateiserver verbunden ist.</li> <li>6. Definieren Sie Pfade zwischen der NAS-Einheit zum Versetzen von Daten und allen Laufwerken, die für NDMP-Operationen verwendet werden.</li> </ol> |

| Befehl             | Prozedur  |
|--------------------|---|
| <b>REMOVE NODE</b> | <p>Um einen Knoten zu entfernen, führen Sie die folgenden Schritte aus:</p> <ol style="list-style-type: none"> <li>1. Löschen Sie alle Definitionen des virtuellen Dateibereichs für den Knoten.</li> <li>2. Löschen Sie alle Pfade zwischen der Einheit zum Versetzen von Daten und den Speicherarchiven sowie zwischen der Einheit zum Versetzen von Daten und den Laufwerken.</li> <li>3. Löschen Sie den Knoten. Wenn beispielsweise ein Knoten mit dem Namen NAS1 entfernt werden soll, geben Sie den folgenden Befehl aus:</li> </ol> <pre>remove node nas1</pre> |

**Zugehörige Verweise:**

- QUERY NODE (Knoten abfragen)
- UPDATE NODE (Knotenattribute aktualisieren)
- RENAME NODE (Knoten umbenennen)
- REMOVE NODE (Knoten oder zugeordneten Maschinenknoten löschen)

## In NDMP-Operationen verwendete Einheiten zum Versetzen von Daten verwalten

Sie können die für NAS-Dateiserver definierten Einheiten zum Versetzen von Daten abfragen, aktualisieren und löschen.

### Vorgehensweise

Verwenden Sie einen der folgenden Befehle, um Einheiten zum Versetzen von Daten zu verwalten:

| Befehl                  | Prozedur  |
|-------------------------|---|
| <b>QUERY DATAMOVER</b>  | <p>Um eine Einheit zum Versetzen von Daten abzufragen, geben Sie den Befehl QUERY DATAMOVER mit den entsprechenden Parametern aus. Wenn beispielsweise die Einheit zum Versetzen von Daten mit dem Namen NASNODE1 abgefragt werden soll, geben Sie den folgenden Befehl aus:</p> <pre>query datamover nasnode1</pre>  |
| <b>UPDATE DATAMOVER</b> | <p>Um eine Einheit zum Versetzen von Daten zu aktualisieren, geben Sie den Befehl UPDATE DATAMOVER mit den entsprechenden Parametern aus. Wenn Sie beispielsweise einen NAS-Dateiserver zu Wartungszwecken herunterfahren und die Einheit zum Versetzen von Daten in den Offlinestatus versetzt werden soll, geben Sie den folgenden Befehl aus:</p> <pre>update datamover nasnode1 online=no</pre>   |
| <b>DELETE DATAMOVER</b> | <p>Um eine Einheit zum Versetzen von Daten zu löschen, geben Sie den Befehl DELETE DATAMOVER aus. Wenn beispielsweise die Einheit zum Versetzen von Daten mit dem Namen NASNODE1 gelöscht werden soll, geben Sie den folgenden Befehl aus:</p> <pre>delete datamover nasnode1</pre> <p>Einschränkung: Wenn die Einheit zum Versetzen von Daten über einen Pfad zu einem Speicherarchiv verfügt und die Einheit zum Versetzen von Daten gelöscht bzw. in den Offlinestatus versetzt wird, inaktivieren Sie damit den Zugriff auf das Speicherarchiv.</p> |

**Zugehörige Verweise:**

- QUERY DATAMOVER (Definitionen für Einheiten zum Versetzen von Daten anzeigen)
- UPDATE DATAMOVER (Einheit zum Versetzen von Daten aktualisieren)
- DELETE DATAMOVER (Einheit zum Versetzen von Daten löschen)

## IBM Spectrum Protect-Laufwerk für NDMP-Operationen dedizieren

---

Wenn Sie bereits ein Laufwerk für IBM Spectrum Protect-Operationen verwenden, können Sie dieses Laufwerk für NDMP-Operationen dedizieren.

### Vorgehensweise

---

Entfernen Sie den IBM Spectrum Protect-Serverzugriff, indem Sie die Pfaddefinition löschen. Wenn beispielsweise der Servername SERVER1 und der Laufwerkname NASDRIVE1 lautet, geben Sie den folgenden Befehl aus:

```
delete path server1 nasdrive1 srctype=server desttype=drive library=naslib
```

## Speicherpoolverwaltung für NDMP-Operationen

---

Wenn NETAPPDUMP, CELERRADUMP oder NDMPDUMP als Speicherpooltyp angegeben wird, unterscheidet sich die Verwaltung von Speicherpools, die von NDMP-Operationen erstellt werden, von der Verwaltung von Speicherpools, die Datenträger für traditionelle IBM Spectrum Protect-Sicherungen enthalten.

Für Speicherpools des Typs NETAPPDUMP, CELERRADUMP und NDMPDUMP, die von NDMP-Operationen erstellt werden, gelten die folgenden Richtlinien und Einschränkungen:

- Sie können Speicherpools abfragen und aktualisieren, der Parameter DATAFORMAT kann jedoch nicht aktualisiert werden.
- Sie können keinen CENTERA-Speicherpool, Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool als Zielpool von NDMP-Operationen angeben.
- Unterschiedliche Speicherpools für Daten verschiedener NAS-Anbieter zu verwalten ist selbst dann das bevorzugte Verfahren, wenn beide das Datenformat NDMPDUMP haben.
- Die folgenden Parameter der Befehle DEFINE STGPOOL und UPDATE STGPOOL werden ignoriert, da Speicherpoolhierarchien, Konsolidierung und Umlagerung für diese Speicherpools nicht unterstützt werden:
  - MAXSIZE
  - NEXTSTGPOOL
  - LOWMIG
  - HIGHMIG
  - MIGDELAY
  - MIGCONTINUE
  - RECLAIMSTGPOOL
  - OVFLOCATION

Wichtig: Stellen Sie sicher, dass Sie Speicherpools, die für NDMP-Operationen definiert wurden, nicht versehentlich für traditionelle IBM Spectrum Protect-Operationen verwenden. Gehen Sie mit besonderer Sorgfalt vor, wenn Sie den Speicherpoolnamen als Wert für den Parameter DESTINATION im Befehl DEFINE COPYGROUP zuordnen. Wenn der Zielspeicherpool nicht das geeignete Datenformat aufweist, schlägt die Sicherung fehl.

## Inhaltsverzeichnisse verwalten

---

Sie können mehrere Befehle für die Verwaltung unterschiedlicher Aspekte Ihres Dateninhalts verwenden.

### Informationen zu diesem Vorgang

---

Mit dem Befehl SET TOCLOADRETENTION können Sie angeben, wie lange ungefähr (in Minuten) ein Inhaltsverzeichnis, auf das nicht verwiesen wird, in der IBM Spectrum Protect-Datenbank geladen bleibt. Der serverweite Wert für den Aufbewahrungszeitraum von Inhaltsverzeichnissen (TOC) in IBM Spectrum Protect legt fest, wie lange ein geladenes Inhaltsverzeichnis nach dem letzten Zugriff auf Informationen in dem Inhaltsverzeichnis in der Datenbank aufbewahrt wird.

Da die Inhaltsverzeichnisinformationen in temporäre Datenbanktabellen geladen werden, gehen diese Informationen verloren, wenn der Server angehalten wird, auch wenn der Aufbewahrungszeitraum für das Inhaltsverzeichnis noch nicht abgelaufen ist. Bei der Installation wird für den Aufbewahrungszeitraum der Wert 120 Minuten definiert. Sie können den Aufbewahrungszeitraum für das Inhaltsverzeichnis mit dem Befehl QUERY STATUS anzeigen.

Geben Sie den Befehl QUERY NASBACKUP aus, um Informationen zu den Dateisystemimageobjekten anzuzeigen, die für einen bestimmten NAS-Knoten und -Dateibereich gesichert wurden. Wenn Sie den Befehl ausgeben, wird eine Anzeige aller von NDMP generierten Sicherungsimagen mit der Angabe, ob jedes Image über ein entsprechendes Inhaltsverzeichnis (TOC) verfügt, aufgerufen. Tipp: Der IBM Spectrum Protect-Server kann zusätzlich zu der von Ihnen angegebenen Anzahl Versionen eine Gesamtsicherung speichern, wenn diese Gesamtsicherung über abhängige Differenzsicherungen verfügt. NAS-Gesamtsicherungen mit abhängigen Differenzsicherungen verhalten sich wie andere Basisdateien mit abhängigen Subdateien. Aufgrund des Aufbewahrungszeitraums, der in

der Einstellung RETEXTRA angegeben ist, wird die NAS-Gesamtsicherung nicht als verfallen definiert und die Version wird in der Ausgabe eines Befehls QUERY NASBACKUP angezeigt. Informationen zum Definieren von Datenaufbewahrungsmaßnahmen finden Sie in Maßnahmen anpassen.

Zeigen Sie mit dem Befehl QUERY TOC Dateien und Verzeichnisse in einem mit NDMP generierten Sicherungsbild an. Durch Ausgabe des Serverbefehls QUERY TOC können Sie alle Verzeichnisse und Dateien in einem einzelnen angegebenen Inhaltsverzeichnis (TOC) anzeigen. Auf das angegebene Inhaltsverzeichnis wird bei jeder Ausgabe des Befehls QUERY TOC in einem Speicherpool zugegriffen, da dieser Befehl keine Inhaltsverzeichnisinformationen in die IBM Spectrum Protect-Datenbank lädt. Verwenden Sie dann den Befehl RESTORE NODE mit dem Parameter FILELIST, um einzelne Dateien zurückzuschreiben.

## Schließen inaktiver NDMP-Verbindungen mit langer Laufzeit verhindern

---

Um zu verhindern, dass Firewalls inaktive NDMP-Verbindungen mit langer Laufzeit schließen, können Sie den TCP-Keepalive-Mechanismus auf den NDMP-Steuerverbindungen aktivieren.

### Informationen zu diesem Vorgang




---

Der IBM Spectrum Protect-Server baut Steuerverbindungen zu NAS-Einheiten während NDMP-Sicherungs- oder -Zurückschreibungsoperationen auf. Es kann vorkommen, dass diese Steuerverbindungen für längere Zeit offen und inaktiv bleiben. Angenommen, zwei NDMP-Operationen werden für dieselbe NAS-Einheit gestartet. Die Steuerverbindung für eine NDMP-Operation kann offen, aber inaktiv bleiben, wenn die Operation eine Ressource erfordert, beispielsweise ein Bandlaufwerk oder einen sequenziellen Datenträger, der von der anderen NDMP-Operation verwendet wird.

Bestimmte Firewall-Software ist so konfiguriert, dass Netzverbindungen, die für eine bestimmte Dauer inaktiv sind, automatisch geschlossen werden. Wenn zwischen einem IBM Spectrum Protect-Server und einer NAS-Einheit eine Firewall vorhanden ist, kann es vorkommen, dass die Firewall NDMP-Steuerverbindungen wider Erwarten schließt und das Fehlschlagen der NDMP-Operation verursacht.

Der IBM Spectrum Protect-Server stellt einen Mechanismus, den TCP-Keepalive-Mechanismus, bereit, den Sie aktivieren können, um das Schließen inaktiver Verbindungen mit langer Laufzeit zu verhindern. Wenn der TCP-Keepalive-Mechanismus aktiviert ist, werden kleine Pakete in vordefinierten Intervallen über das Netz an den Verbindungspartner gesendet.

Einschränkung: Um Fehler zu vermeiden, dürfen Sie den TCP-Keepalive-Mechanismus in bestimmten Typen von Umgebungen nicht aktivieren. Ein Beispiel sind Umgebungen, die über keine Firewalls zwischen dem IBM Spectrum Protect-Server und einer NAS-Einheit verfügen. Ein anderes Beispiel sind Umgebungen mit Firewalls, die inaktive Verbindungen mit langer Laufzeit tolerieren. Das Aktivieren des TCP-Keepalive-Mechanismus in diesen Typen von Umgebungen kann zur Folge haben, dass eine inaktive Verbindung versehentlich geschlossen wird, wenn der Verbindungspartner vorübergehend nicht auf TCP-Keepalive-Pakete antwortet.

- TCP-Keepalive-Mechanismus aktivieren  
Um den TCP-Keepalive-Mechanismus, der verhindert, dass NDMP-Verbindungen geschlossen werden, zu aktivieren, verwenden Sie die Serveroption NDMPENABLEKEEPALIVE.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme Inaktivitätsdauer für Verbindungen für den TCP-Keepalive-Mechanismus angeben  
Um die Inaktivitätsdauer für Verbindungen (in Minuten) anzugeben, bevor das erste TCP-Keepalive-Paket gesendet wird, verwenden Sie die Serveroption NDMPKEEPIDLEMINUTES.

## TCP-Keepalive-Mechanismus aktivieren

---

Um den TCP-Keepalive-Mechanismus, der verhindert, dass NDMP-Verbindungen geschlossen werden, zu aktivieren, verwenden Sie die Serveroption NDMPENABLEKEEPALIVE.

### Vorgehensweise

---

Fügen Sie die Option der Serveroptionsdatei dsmserv.opt hinzu:

```
ndmpenablekeepalive yes
```

#### Zugehörige Verweise:

NDMPENABLEKEEPALIVE

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Inaktivitätsdauer für Verbindungen für den TCP-Keepalive-Mechanismus angeben

---

Um die Inaktivitätsdauer für Verbindungen (in Minuten) anzugeben, bevor das erste TCP-Keepalive-Paket gesendet wird, verwenden Sie die Serveroption NDMPKEEPIDLEMINUTES.

## Vorgehensweise

---

Fügen Sie die Option der Serveroptionsdatei dsmserv.opt hinzu:

```
ndmpkeepidleminutes Minuten
```

**Zugehörige Verweise:**  
NDMPKEEPIDLEMINUTES

## IBM Spectrum Protect für NDMP-Operationen konfigurieren

---

Sie können IBM Spectrum Protect zum Sichern und Wiederherstellen von Daten auf NAS-Dateiservern mithilfe von NDMP konfigurieren. Die Konfigurationsprozedur ist abhängig davon, ob Daten von einem NAS-Dateiserver ohne oder mit Clustering gesichert werden sollen, unterschiedlich.

- IBM Spectrum Protect für NDMP-Operationen in einer Umgebung ohne Clustering konfigurieren  
Bevor Sie IBM Spectrum Protect für NDMP-Operationen in einer Umgebung ohne Clustering konfigurieren, müssen Sie die erforderliche Lizenz registrieren.
- IBM Spectrum Protect für NDMP-Operationen in einer NetApp-Centerumgebung konfigurieren  
Sie können Daten von einem NetApp-Cluster auf einer direkt angeschlossenen Bandeinheit oder einem IBM Spectrum Protect-Server sichern, der die Daten in einem Speicherpool speichert. Sie können den gesamten Cluster auf einem einzigen IBM Spectrum Protect-Knoten oder Teile des Clusters auf mehreren Knoten sichern.

## IBM Spectrum Protect für NDMP-Operationen in einer Umgebung ohne Clustering konfigurieren



---


Bevor Sie IBM Spectrum Protect für NDMP-Operationen in einer Umgebung ohne Clustering konfigurieren, müssen Sie die erforderliche Lizenz registrieren.

## Vorgehensweise

---

1. Definieren Sie das Bandarchiv und Datenträger. Siehe Bandarchiv für NDMP-Operationen konfigurieren; dort werden die folgenden Schritte ausführlicher erläutert.
  - a. Schließen Sie das SCSI-Bandarchiv oder das virtuelle Bandarchiv (VTL = Virtual Tape Library) an den NAS-Dateiserver oder an den IBM Spectrum Protect-Server an oder schließen Sie das ACSLS-Speicherarchiv oder das 349X-Speicherarchiv an den IBM Spectrum Protect-Server an.
  - b. Definieren Sie das Speicherarchiv mit dem Speicherarchivtyp SCSI, VTL, ACSLS oder 349X.
  - c. Definieren Sie eine Einheitenklasse für die Bandlaufwerke.
  - d. Definieren Sie einen Speicherpool für NAS-Sicherungsdatenträger.
  - e. Optional: Definieren Sie einen Speicherpool für die Speicherung eines Inhaltsverzeichnisses.
2. Konfigurieren Sie eine IBM Spectrum Protect-Maßnahme für die Verwaltung von NAS-Imagesicherungen. Siehe IBM Spectrum Protect-Maßnahme für NDMP-Operationen konfigurieren.
3. Registrieren Sie einen NAS-Dateiserverknoten beim IBM Spectrum Protect-Server. Siehe NAS-Knoten im IBM Spectrum Protect-Server registrieren.
4. Definieren Sie eine Einheit zum Versetzen von Daten für den NAS-Dateiserver. Siehe Einheit zum Versetzen von Daten für einen NAS-Dateiserver definieren.
5. Einen Pfad vom IBM Spectrum Protect-Server oder vom NAS-Dateiserver zum Bandarchiv definieren. Siehe Pfade zu Speicherarchiven für NDMP-Operationen definieren.
6. Bandlaufwerke für IBM Spectrum Protect definieren und Pfade zu den betreffenden Laufwerken vom NAS-Dateiserver und optional vom IBM Spectrum Protect-Server aus definieren. Siehe Pfade für NDMP-Operationen definieren.
7. Stellen Sie Bänder in das Speicherarchiv und ordnen Sie den Bändern Kennsätze zu.

 AIX-Betriebssysteme  Linux-Betriebssysteme Banddatenträgern müssen Kennsätze zugeordnet werden, bevor sie vom Server verwendet werden können. Dazu können Sie den Befehl LABEL LIBVOLUME verwenden oder die Befehle DEFINE LIBRARY und UPDATE LIBRARY unter Angabe des Parameters AUTOLABEL.

 Windows-Betriebssysteme Allen Datenträgern müssen Kennsätze zugeordnet werden. Um Datenträgern bei einem automatisierten Speicherarchiv Kennsätze zuzuordnen, müssen Sie die Datenträger in das Speicherarchiv zurückstellen. Um Datenträgern mit dem Befehl LABEL LIBVOLUME Kennsätze zuzuordnen, geben Sie den Parameter CHECKIN an. Um Banddatenträgern in SCSI-Speicherarchiven automatisch Kennsätze zuzuordnen, verwenden Sie den Parameter AUTOLABEL in den Befehlen DEFINE LIBRARY und UPDATE LIBRARY.

Anweisungen finden Sie in den Beschreibungen der Befehle LABEL LIBVOLUME, DEFINE LIBRARY und UPDATE LIBRARY.

8. Optional: Definieren Sie geplante Sicherungen für NAS-Dateiserver. Siehe NDMP-Operationen planen.
  9. Optional: Definieren Sie den Namen eines virtuellen Dateibereichs. Siehe Virtuelle Dateibereiche definieren.
  10. Optional: Band-zu-Band-Kopie zum Sichern von Daten konfigurieren. Siehe Daten mit der Band-zu-Band-Kopierfunktion sichern.
  11. Optional: Band-zu-Band-Kopie zum Versetzen von Daten in eine andere Bandtechnologie konfigurieren. Siehe Daten mit der Band-zu-Band-Kopierfunktion versetzen.
- IBM Spectrum Protect-Maßnahme für NDMP-Operationen konfigurieren  
Mithilfe von Maßnahmen können Sie die Anzahl und den Aufbewahrungszeitraum von NDMP-Imagesicherungsversionen verwalten.
  - Bandarchive und -laufwerke für NDMP-Operationen  
Der größte Teil der Planung für die Implementierung von Sicherungs- und Zurückschreibungsoperationen mit NDMP betrifft die Einheitenkonfiguration. Sie können auswählen, wie die Speicherarchive und Laufwerke angeschlossen und verwendet werden sollen.
  - Greifarme des Bandarchivs für NAS-Speicherarchive anschließen  
Wenn Sie planen, NAS-Daten in einem Speicherarchiv zu sichern, das direkt an die NAS-Einheit angeschlossen ist, und wenn Sie ein SCSI-Bandarchiv verwenden, müssen Sie die Anschlussposition für das Speicherarchiv festlegen.
  - NAS-Knoten im IBM Spectrum Protect-Server registrieren  
Registrieren Sie den NAS-Dateiserver unter Angabe von TYPE=NAS als einen IBM Spectrum Protect-Knoten. Anhand dieses Knotennamens werden die Imagesicherungen für den NAS-Dateiserver protokolliert.
  - Einheit zum Versetzen von Daten für einen NAS-Dateiserver definieren  
Definieren Sie eine Einheit zum Versetzen von Daten für jeden NAS-Dateiserver unter Verwendung von NDMP-Operationen in Ihrer Umgebung. Der Name der Einheit zum Versetzen von Daten muss mit dem Knotennamen übereinstimmen, den Sie angegeben haben, als Sie den NAS-Knoten für den IBM Spectrum Protect-Server registriert haben.
  - Pfade für NDMP-Operationen definieren  
Für NDMP-Operationen müssen Sie Pfade zu Laufwerken und Speicherarchiven erstellen.
  - NDMP-Operationen planen  
Sie können Sicherungs- oder Zurückschreibungsoperationen für Images planen, die von NDMP-Operationen erstellt werden. Verwenden Sie Verwaltungszeitpläne, die den Verwaltungsbefehl BACKUP NODE oder RESTORE NODE verarbeiten.
  - Virtuelle Dateibereiche definieren  
Verwenden Sie die Definition eines virtuellen Dateibereichs, um NAS-Sicherungen auf Verzeichnisebene auszuführen. Um die Sicherungs- und Zurückschreibungszeiten für große Dateisysteme zu reduzieren, ordnen Sie einen Verzeichnispfad von einem NAS-Dateiserver zum Namen eines virtuellen Dateibereichs auf dem IBM Spectrum Protect-Server zu.
  - Daten mit der Band-zu-Band-Kopierfunktion sichern  
Wenn Sie die NDMP-Band-zu-Band-Kopierfunktion zum Sichern von Daten verwenden, kann der Speicherarchivtyp SCSI, 349X oder ACSLS (Automated Cartridge System Library Software) sein. Laufwerke können von den NAS-Einheiten und dem IBM Spectrum Protect-Server gemeinsam genutzt werden.
  - Daten mit der Band-zu-Band-Kopierfunktion versetzen  
Um Daten unter Verwendung der NDMP-Band-zu-Band-Kopieroperation von einer vorherigen Bandtechnologie in eine neue Bandtechnologie zu versetzen, müssen Sie die Standardschritte in Ihrem Konfigurationssetup sowie weitere Schritte ausführen.

## IBM Spectrum Protect-Maßnahme für NDMP-Operationen konfigurieren

---

Mithilfe von Maßnahmen können Sie die Anzahl und den Aufbewahrungszeitraum von NDMP-Imagesicherungsversionen verwalten.

### Informationen zu diesem Vorgang

---

Weitere Informationen finden Sie in Maßnahmen für Sicherungen, die von einem IBM Spectrum Protect-Server eingeleitet werden.

### Vorgehensweise

---

Führen Sie die folgenden Schritte aus, um eine Maßnahme für NDMP-Operationen zu konfigurieren:

1. Erstellen Sie eine Maßnahmendomäne für NAS-Dateiserver (NAS = Network-attached Storage). Geben Sie beispielsweise folgenden Befehl ein, um die Maßnahmendomäne NASDOMAIN zu definieren:

```
define domain nasdomain description='Maßnahmendomäne für NAS-Dateiserver'
```

2. Erstellen Sie eine Maßnahmengruppe in dieser Domäne. Um beispielsweise eine Maßnahmengruppe mit dem Namen STANDARD in der Maßnahmendomäne NASDOMAIN zu definieren, geben Sie den folgenden Befehl aus:

```
define policyset nasdomain standard
```

3. Definieren Sie die Verwaltungsklasse und ordnen Sie dann die Verwaltungsklasse als Standardwert für die Maßnahmengruppe zu. Um beispielsweise eine Verwaltungsklasse mit dem Namen MC1 in der Maßnahmengruppe STANDARD zu definieren und

anschließend als Standard zuzuordnen, geben Sie die folgenden Befehle aus:

```
define mgmtclass nasdomain standard mcl
assign defmgmtclass nasdomain standard mcl
```

- Definieren Sie eine Sicherungskopiengruppe in der Standardverwaltungsklasse. Das Ziel muss der Speicherpool sein, den Sie für die durch NDMP-Operationen generierten Sicherungsbilder erstellt hatten. Zusätzlich können Sie die Anzahl der Sicherungsversionen angeben, die aufbewahrt werden sollen. Um beispielsweise eine Sicherungskopiengruppe für die Verwaltungsklasse MC1 zu definieren und bis zu vier Versionen jedes Dateisystems im Speicherpool mit dem Namen NASPOOL aufzubewahren, geben Sie den folgenden Befehl aus:

```
define copygroup nasdomain standard mcl destination=naspool verexists=4
```

Wenn ein Inhaltsverzeichnis (TOC) für Ihre Sicherungen erstellt werden soll, muss der Parameter TOCDESTINATION der Kopiengruppe den Namen des primären Speicherpools enthalten.

```
define copygroup nasdomain standard mcl destination=naspool
tocdestination=tocpool verexists=4
```

Wichtig: Wenn Sie eine Kopiengruppe für eine Verwaltungsklasse definieren, an die ein durch NDMP generiertes Dateisystem gebunden ist, müssen Sie sicherstellen, dass der Parameter DESTINATION den Namen eines Speicherpools angibt, der für NDMP-Operationen definiert ist. Wenn im Parameter DESTINATION ein ungültiger Speicherpool angegeben ist, schlagen Sicherungen mit NDMP fehl.

- Aktivieren Sie die Maßnahmengruppe. Um beispielsweise die Maßnahmengruppe STANDARD in der Maßnahmendomäne NASDOMAIN zu aktivieren, geben Sie den folgenden Befehl aus:

```
activate policysset nasdomain standard
```

Die Maßnahme kann jetzt verwendet werden. Knoten werden bei ihrer Registrierung einer Maßnahme zugeordnet. Weitere Informationen finden Sie in NAS-Knoten im IBM Spectrum Protect-Server registrieren.

- Maßnahmen für Sicherungen, die von einem IBM Spectrum Protect-Server eingeleitet werden  
Sie können einen NAS-Dateiserver unter Verwendung von NDMP-Operationen als Knoten registrieren. Unter der Steuerung des IBM Spectrum Protect-Servers sichert der NAS-Dateiserver ein Dateisystem und Verzeichnisimages und schreibt diese in ein Bandarchiv zurück.
- Maßnahmen für Sicherungen, die mit der Clientschnittstelle eingeleitet werden  
Wenn ein Clientknoten eine Sicherung einleitet, hat die Optionsdatei für den betreffenden Clientknoten Auswirkungen auf die Maßnahme.
- Festlegung der NAS-Sicherungsposition  
Wenn IBM Spectrum Protect NDMP zum Schützen von NAS-Dateiservern verwendet, werden Operationen durch den IBM Spectrum Protect-Server gesteuert. Während dieser Zeit überträgt der NAS-Dateiserver die Daten entweder an ein angeschlossenes Speicherarchiv oder direkt an den IBM Spectrum Protect-Server.

## Maßnahmen für Sicherungen, die von einem IBM Spectrum Protect-Server eingeleitet werden

---

Sie können einen NAS-Dateiserver unter Verwendung von NDMP-Operationen als Knoten registrieren. Unter der Steuerung des IBM Spectrum Protect-Servers sichert der NAS-Dateiserver ein Dateisystem und Verzeichnisimages und schreibt diese in ein Bandarchiv zurück.

Der IBM Spectrum Protect-Server leitet die Sicherung ein, ordnet ein Laufwerk zu, wählt die Datenträger aus und lädt sie. Der NAS-Dateiserver überträgt dann die Daten auf Band.

Da der NAS-Dateiserver die Daten sichert, werden die Daten im Format des NAS-Dateiservers gespeichert. Bei den meisten NAS-Dateiservern werden die Daten im Datenformat NDMPDUMP gespeichert. Bei NetApp-Dateiservern werden die Daten im Datenformat NETAPPDUMP gespeichert. Bei EMC-Dateiservern werden die Daten im Datenformat CELERRADUMP gespeichert. Zum Verwalten von Imagesicherungen des NAS-Dateiservers müssen Kopiengruppen für NAS-Knoten auf einen Speicherpool zeigen, der das Datenformat NDMPDUMP, NETAPPDUMP oder CELERRADUMP hat.

Die folgenden Attribute für Sicherungskopiengruppen werden für NAS-Images ignoriert:

- Häufigkeit
- Modus
- Einzige Version aufbewahren
- Durchnummerierung
- Versionen gelöschter Daten



Um die erforderliche Maßnahme für NAS-Knoten zu definieren, können Sie eine neue, separate Maßnahmendomäne definieren.

Wenn der IBM Spectrum Protect-Server ein Inhaltsverzeichnis erstellt, können Sie eine Sammlung einzelner Dateien und Verzeichnisse anzeigen, die unter Verwendung von NDMP gesichert werden. Anschließend können Sie die zurückzuschreibenden Dateien und Verzeichnisse auswählen. Um festzulegen, wohin Daten gesendet werden sollen und wo das Inhaltsverzeichnis gespeichert werden soll, definieren Sie die Maßnahme wie folgt:

- Stellen Sie sicher, dass Imagesicherungsdaten an einen Speicherpool mit dem Format NDMPDUMP, NETAPPDUMP oder CELERRADUMP gesendet werden.
- Stellen Sie sicher, dass das Inhaltsverzeichnis an einen Speicherpool mit dem Format NATIVE oder NONBLOCK gesendet wird.

## Maßnahmen für Sicherungen, die mit der Clientschnittstelle eingeleitet werden

Wenn ein Clientknoten eine Sicherung einleitet, hat die Optionsdatei für den betreffenden Clientknoten Auswirkungen auf die Maßnahme.

Sie können die Verwaltungsklassen steuern, die auf Sicherungsbildern angewendet werden, die durch NDMP-Operationen (NDMP = Network Data Management Protocol) generiert wurden, und zwar unabhängig davon, welcher Knoten die Sicherung einleitet. Sie können diese Task ausführen, indem Sie eine Gruppe von Optionen erstellen, die von den Clientknoten verwendet werden sollen. Die Optionsgruppe kann eine Anweisung `include.fs.nas` enthalten, um die Verwaltungsklasse für NAS-Dateiserverversicherungen anzugeben.

Tipp: Sie können eine Optionsgruppe mit dem Befehl `DEFINE CLOPTSET` definieren. Fügen Sie dann der Optionsgruppe mit dem Befehl `DEFINE CLIENTOPT` eine Clientoption hinzu. Sie können einem Client eine Optionsgruppe zuordnen, indem Sie die folgenden Schritte ausführen:

1. Öffnen Sie die Seite Übersicht im Operations Center und klicken Sie auf Clients.
2. Doppelklicken Sie auf den Client und klicken Sie auf Merkmale.
3. Wählen Sie im Feld Optionsgruppe eine Option aus und klicken Sie auf Sichern.

Anweisungen zur Verwendung des Befehls `DEFINE CLOPTSET` finden Sie in `DEFINE CLOPTSET` (Clientoptionsgruppennamen definieren). Anweisungen zur Verwendung des Befehls `DEFINE CLIENTOPT` finden Sie in `DEFINE CLIENTOPT` (Option für eine Optionsgruppe definieren).

## Festlegung der NAS-Sicherungsposition

Wenn IBM Spectrum Protect NDMP zum Schützen von NAS-Dateiservern verwendet, werden Operationen durch den IBM Spectrum Protect-Server gesteuert. Während dieser Zeit überträgt der NAS-Dateiserver die Daten entweder an ein angeschlossenes Speicherarchiv oder direkt an den IBM Spectrum Protect-Server.

Sie können auch einen Client für Sichern/Archivieren verwenden, um einen NAS-Dateiserver zu sichern, indem das NAS-Dateisystem auf dem Client-Computer bereitgestellt wird und dann die Sicherung wie gewohnt ausgeführt wird. Sie können entweder einen NFS-Mount oder eine CIFS-Map verwenden.

Eine Beschreibung der Methoden zur Sicherung und Zurückschreibung finden Sie in Tabelle 1.

Tipp: Sie können eine einzelne Methode oder eine Kombination der Methoden in Ihrer individuellen Speicherumgebung verwenden.

Tabelle 1. Vergleich der Methoden zum Sichern von NDMP-Daten

| Merkmal              | NDMP: Vom Dateiserver auf den Server  | NDMP: Vom Dateiserver in ein angeschlossenes Speicherarchiv                                       | Vom Client für Sichern/Archivieren auf den Server   |
|----------------------|---|---|---|
| Datenverkehr im Netz | Alle Sicherungsdaten werden über das LAN vom NAS-Dateiserver zum Server übertragen. | Der Server steuert Operationen über Remotezugriff, aber die NAS-Einheit versetzt die Daten lokal. | Alle Sicherungsdaten werden über das LAN von der NAS-Einheit zum Client und dann zum Server übertragen. |

| <b>Merkmal</b>   | <b>NDMP: Vom Dateiserver auf den Server</b>  | <b>NDMP: Vom Dateiserver in ein angeschlossenes Speicherarchiv</b>   | <b>Vom Client für Sichern/Archivieren auf den Server</b>  |
|--|--|--|---|
| Dateiserververarbeitung während der Sicherung  | Im Vergleich zur Sicherungsmethode mit dem Client für Sichern/Archivieren ist weniger Dateiserververarbeitung erforderlich, da bei der Sicherung keine Dateizugriffsprotokolle wie zum Beispiel NFS und CIFS verwendet werden. | Im Vergleich zur Sicherungsmethode mit dem Client für Sichern/Archivieren ist weniger Dateiserververarbeitung erforderlich, da bei der Sicherung keine Dateizugriffsprotokolle wie zum Beispiel NFS und CIFS verwendet werden. | Dateisicherungsoperationen erfordern mehr Serververarbeitungsressourcen für Dateizugriffsprotokolle wie NFS und CIFS. |
| Entfernung zwischen Einheiten  | Der IBM Spectrum Protect-Server muss sich innerhalb des SCSI- bzw. Fibre Channel-Bereichs des Bandarchivs befinden.  | Der IBM Spectrum Protect-Server muss sich nicht lokal auf dem NAS-Dateiserver und nicht innerhalb des Bandarchivs befinden.  | Der IBM Spectrum Protect-Server muss sich innerhalb des SCSI- bzw. Fibre Channel-Bereichs des Bandarchivs befinden.   |
| Firewallaspekte  | Strikter als bei der Übertragung zwischen Dateiserver und angeschlossenen Speicherarchiv, da die Übertragung entweder vom IBM Spectrum Protect-Server oder vom NAS-Dateiserver eingeleitet werden kann.                        | Weniger strikt als bei der Übertragung zwischen Dateiserver und Server, da die Übertragung nur vom IBM Spectrum Protect-Server eingeleitet werden kann.  | Clientkennwörter und -daten werden verschlüsselt.   |
| Sicherheitsaspekte   | Daten werden entschlüsselt von einem NAS-Dateiserver an einen IBM Spectrum Protect-Server gesendet.  | Diese Methode muss in einer vertrauenswürdigen Umgebung verwendet werden, da Portnummern nicht sicher sind.  | Die Portnummernkonfiguration ermöglicht sichere Verwaltungssitzungen in einem privaten Netz.                          |
| Last auf dem IBM Spectrum Protect-Server   | Höhere CPU-Workload ist erforderlich, um alle Back-End-Datenprozesse zu verwalten (beispielsweise Umlagerung).   | Die CPU-Workload verringert sich, da Umlagerung und Konsolidierung nicht unterstützt werden.   | Höhere CPU-Workload ist erforderlich, um alle Back-End-Datenprozesse zu verwalten.                                    |
| Sicherung von primären Speicherpools in Kopierspeicherpools                          | Daten können nur in Kopierspeicherpools gesichert werden, die das Datenformat NATIVE haben.  | Daten können nur in Kopierspeicherpools gesichert werden, die dasselbe NDMP-Datenformat haben (NETAPPDUMP, CELERRADUMP oder NDMPDUMP).   | Daten können nur in Kopierspeicherpools gesichert werden, die das Datenformat NATIVE haben.                           |
| Zurückschreibung von primären Speicherpools und Datenträgern aus Kopierspeicherpools | Daten können nur in Speicherpools und auf Datenträger zurückgeschrieben werden, die das Datenformat NATIVE haben.  | Daten können nur in Speicherpools und auf Datenträger zurückgeschrieben werden, die dasselbe NDMP-Format haben.  | Daten können nur in Speicherpools und auf Datenträger zurückgeschrieben werden, die das Datenformat NATIVE haben.     |
| Versetzen von NDMP-Daten von Speicherpool datenträgern                               | Daten können nur in einen anderen Speicherpool versetzt werden, wenn er das Datenformat NATIVE hat.  | Daten können nur in einen anderen Speicherpool versetzt werden, wenn er dasselbe NDMP-Datenformat hat.   | Daten können nur in einen anderen Speicherpool versetzt werden, wenn er das Datenformat NATIVE hat.                   |
| Umlagerung aus einem primären Speicherpool in einen anderen Speicherpool             | Unterstützt  | Nicht unterstützt  | Unterstützt   |
| Konsolidierung eines Speicherpools   | Unterstützt  | Nicht unterstützt  | Unterstützt   |
| Operationen für gleichzeitiges Schreiben während Sicherungen                         | Nicht unterstützt  | Nicht unterstützt  | Unterstützt   |
| Export- und Importoperationen  | Nicht unterstützt  | Nicht unterstützt  | Unterstützt   |

| Merkmal  | NDMP: Vom Dateiserver auf den Server | NDMP: Vom Dateiserver in ein angeschlossenes Speicherarchiv | Vom Client für Sichern/Archivieren auf den Server |
|--|--------------------------------------|---|---|
| Generierung von Sicherungsgruppen  | Nicht unterstützt                    | Nicht unterstützt   | Unterstützt                                       |
| Zyklische Blockprüfung (CRC), wenn Daten unter Verwendung von IBM Spectrum Protect-Prozessen versetzt werden | Unterstützt                          | Nicht unterstützt   | Unterstützt                                       |
| Prüfung unter Verwendung von IBM Spectrum Protect-Prüfbefehlen   | Unterstützt                          | Nicht unterstützt   | Unterstützt                                       |
| Disaster Recovery Manager  | Unterstützt                          | Unterstützt   | Unterstützt                                       |

## Bandarchive und -laufwerke für NDMP-Operationen

Der größte Teil der Planung für die Implementierung von Sicherungs- und Zurückschreibungsoperationen mit NDMP betrifft die Einheitenkonfiguration. Sie können auswählen, wie die Speicherarchive und Laufwerke angeschlossen und verwendet werden sollen.

Viele der Konfigurationsauswahlmöglichkeiten, die für Speicherarchive und Laufwerke zur Verfügung stehen, werden von den Hardware-Features Ihrer Speicherarchive bestimmt. Sie können NDMP-Operationen für alle unterstützten Speicherarchive und Laufwerke definieren. Je mehr Features jedoch für Ihr Speicherarchiv zur Verfügung stehen, desto flexibler lässt sich die Implementierung gestalten.

Zunächst sollten Sie folgende Fragen beantworten:

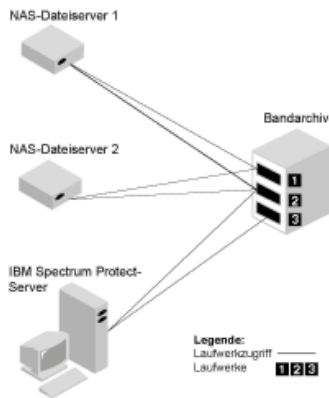
- Welcher Speicherarchivtyp (SCSI, ACSLS, 349X) wird verwendet?
- Bei Verwendung eines SCSI-Speicherarchivs: Sollen die Greifarme des Bandarchivs an den IBM Spectrum Protect-Server oder den NAS-Dateiserver angeschlossen werden?
- Sollen Ihre NDMP-Daten auf Band versetzt werden?
- Wie sollen die Bandlaufwerke im Speicherarchiv verwendet werden?
  - Ordnen Sie alle Bandlaufwerke NDMP-Operationen zu.
  - Ordnen Sie einige Bandlaufwerke NDMP-Operationen und andere traditionellen IBM Spectrum Protect-Operationen zu.
  - Nutzen Sie Bandlaufwerke für NDMP-Operationen und traditionelle IBM Spectrum Protect-Operationen gemeinsam.
- Werden Daten für Funktionen zur Wiederherstellung nach einem Katastrophenfall von Band zu Band gesichert?
- Werden Sicherungsdaten an einen einzelnen IBM Spectrum Protect-Server gesendet, anstatt ein Bandarchiv an jede NAS-Einheit anzuschließen?
- Soll sich die gesamte Hardware auf dem IBM Spectrum Protect-Server befinden und sollen NDMP-Daten über das LAN gesendet werden?
- Speicherarchivlaufwerknutzung bei der Sicherung auf NAS-Speicherarchiven bestimmen  
Laufwerke können aufgrund der bei IBM Spectrum Protect möglichen flexiblen Konfigurationen für vielfältige Zwecke eingesetzt werden. Für NDMP-Operationen muss der NAS-Dateiserver Zugriff auf das Laufwerk haben. Der IBM Spectrum Protect-Server kann ebenfalls Zugriff auf dasselbe Laufwerk haben, in Abhängigkeit von den vorliegenden Hardwareverbindungen und -einschränkungen.
- Bandarchiv für NDMP-Operationen konfigurieren  
Sie können ein Bandarchiv zum Sichern einer NAS-Einheit (NAS = Network-attached Storage) auf Band konfigurieren.

## Speicherarchivlaufwerknutzung bei der Sicherung auf NAS-Speicherarchiven bestimmen

Laufwerke können aufgrund der bei IBM Spectrum Protect möglichen flexiblen Konfigurationen für vielfältige Zwecke eingesetzt werden. Für NDMP-Operationen muss der NAS-Dateiserver Zugriff auf das Laufwerk haben. Der IBM Spectrum Protect-Server kann ebenfalls Zugriff auf dasselbe Laufwerk haben, in Abhängigkeit von den vorliegenden Hardwareverbindungen und -einschränkungen.

### Informationen zu diesem Vorgang

Alle Laufwerke werden für den IBM Spectrum Protect-Server definiert. Dasselbe Laufwerk kann jedoch sowohl für traditionelle IBM Spectrum Protect-Operationen als auch für NDMP-Operationen definiert werden. Abbildung 1 zeigt eine der möglichen Konfigurationen. Der IBM Spectrum Protect-Server hat Zugriff auf die Laufwerke 2 und 3, und jeder NAS-Dateiserver hat Zugriff auf die Laufwerke 1 und 2. Abbildung 1. Beispiel für die Verwendung von IBM Spectrum Protect-Laufwerken



Um die in Abbildung 1 gezeigte Konfiguration zu erstellen, führen Sie die folgenden Schritte aus:

## Vorgehensweise

1. Alle drei Laufwerke für IBM Spectrum Protect definieren.
2. Pfade vom IBM Spectrum Protect-Server zu den Laufwerken 2 und 3 definieren. Da der Server nicht auf Laufwerk 1 zugreift, wird kein Pfad zu diesem Laufwerk definiert.
3. Jeden NAS-Dateiserver als separate Einheit zum Versetzen von Daten definieren.
4. Pfade von jeder Einheit zum Versetzen von Daten zu Laufwerk 1 und 2 definieren.

## Ergebnisse

Für die Verwendung der Back-End-Datenversetzungsoperationen in IBM Spectrum Protect erfordert der IBM Spectrum Protect-Server zwei verfügbare Laufwerkpfade von einer einzelnen NAS-Einheit zum Versetzen von Daten. Die Laufwerke können sich in verschiedenen Speicherarchiven befinden und können verschiedene Einheitentypen haben, die von NDMP unterstützt werden. Sie können Kopien zwischen zwei verschiedenen Bänderinheiten erstellen. Beispielsweise kann das Quellenbandlaufwerk ein DLT-Laufwerk in einem Speicherarchiv sein und das Ziellaufwerk ein LTO-Laufwerk in einem anderen Speicherarchiv.

Während der Back-End-Datenversetzungsoperationen in IBM Spectrum Protect sucht der IBM Spectrum Protect-Server eine NAS-Einheit zum Versetzen von Daten, die dasselbe Datenformat wie das Format der Daten unterstützt, aus denen kopiert wird, und die über zwei verfügbare Mountpunkte und Pfade zu den Laufwerken verfügt. Kann der IBM Spectrum Protect-Server eine solche Einheit zum Versetzen von Daten nicht finden, wird die angeforderte Datenversetzungsoperation nicht ausgeführt. Die Anzahl verfügbarer Mountpunkte und Laufwerke ist von den Mount-Limits der Einheitenklassen für die Speicherpools abhängig, die an den Back-End-Datenversetzungsoperationen beteiligt sind.

Unterstützt die Back-End-Datenversetzungsfunktion den Mehrprozessorbetrieb, erfordert jeder gleichzeitig ablaufende Back-End-Datenversetzungsprozess in IBM Spectrum Protect zwei verfügbare Mountpunkte und zwei verfügbare Laufwerke. Um zwei IBM Spectrum Protect-Prozesse gleichzeitig auszuführen, müssen mindestens vier Mountpunkte und vier Laufwerke verfügbar sein.

Weitere Informationen finden Sie in Pfaden für NDMP-Operationen definieren.

## Bandarchiv für NDMP-Operationen konfigurieren

Sie können ein Bandarchiv zum Sichern einer NAS-Einheit (NAS = Network-attached Storage) auf Band konfigurieren.

## Vorgehensweise

Führen Sie die folgenden Schritte aus, um Bandarchive für NDMP-Operationen zu konfigurieren:

1. Schließen Sie das Bandarchiv und die Laufwerke, die für NDMP-Operationen verwendet werden sollen, an.
  - a. Schließen Sie das SCSI-Bandarchiv an. Legen Sie, bevor Sie ein SCSI-Bandarchiv für NDMP-Operationen definieren, fest, ob die Steuerung für die Greifarme des Speicherarchivs an den IBM Spectrum Protect-Server oder den NAS-Dateiserver angeschlossen werden soll. Siehe Bandarchive und -laufwerke für NDMP-Operationen. Schließen Sie die Greifarme des SCSI-Bandarchivs an den IBM Spectrum Protect-Server oder an den NAS-Dateiserver an. Anweisungen finden Sie in der Dokumentation des Einheitenherstellers.

Wenn das Speicherarchiv an den IBM Spectrum Protect-Server angeschlossen ist, stellen Sie eine SCSI- oder Fibre Channel-Verbindung zwischen dem IBM Spectrum Protect-Server und dem Steueranschluss für die Greifarme des

Speicherarchivs her. Schließen Sie dann den NAS-Dateiserver an die Laufwerke an.

Wenn das Speicherarchiv an den NAS-Dateiserver angeschlossen ist, stellen Sie eine SCSI- oder Fibre Channel-Verbindung zwischen dem NAS-Dateiserver und den Greifarmen des Speicherarchivs und den Laufwerken her.

b. Schließen Sie das ACSLS-Speicherarchiv an. Schließen Sie das ACSLS-Bandarchiv an den IBM Spectrum Protect-Server an.

c. Schließen Sie das 349X-Speicherarchiv an. Schließen Sie das 349X-Bandarchiv an den IBM Spectrum Protect-Server an.

2. Definieren Sie das Speicherarchiv für Ihre Speicherarchivereinheit, indem Sie den Befehl DEFINE LIBRARY ausgeben. Das Speicherarchiv darf keine gemischte Einheitentypen haben, sondern muss einen einzelnen Einheitentyp haben. Geben Sie einen der folgenden Befehle aus, um das Speicherarchiv abhängig vom Typ der Einheit, die Sie konfigurieren, zu definieren:

SCSI-Speicherarchiv

```
define library tsmlib libtype=scsi
```

ACSL-Speicherarchiv

```
define library acslib libtype=acsls acsid=1
```

349X-Speicherarchiv

```
define library tsmlib libtype=349x
```

3. Definieren Sie eine Einheitenklasse für Ihre NDMP-Einheit, indem Sie den Befehl DEFINE DEVCLASS ausgeben.

Tipp: Eine Einheitenklasse, die mit dem Einheitentyp NAS definiert ist, ist nicht explizit einem bestimmten Laufwerktyp, wie beispielsweise LTO, zugeordnet. Das bevorzugte Verfahren ist jedoch, für unterschiedliche Laufwerktypen jeweils eine andere Einheitenklasse zu definieren.

Verwenden Sie im Befehl DEFINE DEVCLASS die folgenden Parameter und Werte:

- o Geben Sie DEVTYPE=NAS an.
- o Geben Sie MOUNTRETENTION=0 an. Diese Angabe ist für NDMP-Operationen erforderlich.
- o Geben Sie einen Wert für den Parameter ESTCAPACITY an.

Um beispielsweise eine Einheitenklasse mit dem Namen NASCLASS für ein Speicherarchiv mit dem Namen NASLIB mit einer geschätzten Kapazität von 40 GB für die Datenträger zu definieren, geben Sie den folgenden Befehl aus:

```
define devclass nasclass devtype=nas library=naslib mountretention=0  
estcapacity=40g
```

4. Definieren Sie einen Speicherpool für NDMP-Datenträger, indem Sie den Befehl DEFINE STGPOOL ausgeben. Wenn NETAPPDUMP, CELERRADUMP oder NDMPDUMP als Speicherpooltyp angegeben wird, unterscheidet sich die Verwaltung von Speicherpools, die von NDMP-Operationen erstellt werden, von der Verwaltung von Speicherpools, die Datenträger für traditionelle IBM Spectrum Protect-Sicherungen enthalten. IBM Spectrum Protect-Operationen verwenden Speicherpools, die mit dem Datenformat NATIVE oder NONBLOCK definiert sind. Wenn Sie NETAPPDUMP, CELERRADUMP oder NDMPDUMP auswählen, erfordern NDMP-Operationen Speicherpools mit einem Datenformat, das dem NAS-Dateiserver und der ausgewählten Sicherungsmethode entspricht. Unterschiedliche Speicherpools für Daten verschiedener NAS-Anbieter zu verwalten ist selbst dann optimal, wenn beide das Datenformat NDMPDUMP haben. Um beispielsweise einen Speicherpool mit dem Namen NDMPPOOL für einen Dateiserver zu definieren, der kein NetApp- oder kein Celerra-Dateiserver ist, geben Sie den folgenden Befehl aus:

```
define stgpool ndmpool nasclass maxscratch=10 dataformat=ndmpdump
```

Um einen Speicherpool mit dem Namen NASPOOL für einen NetApp-Dateiserver zu definieren, geben Sie den folgenden Befehl aus:

```
define stgpool naspool nasclass maxscratch=10 dataformat=netappdump
```

Um einen Speicherpool mit dem Namen CELERRAPOOL für einen EMC Celerra-Dateiserver zu definieren, geben Sie den folgenden Befehl aus:



```
define stgpool celerrapool nasclass maxscratch=10 dataformat=celerradump
```

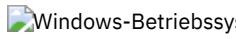
Achtung: Stellen Sie sicher, dass Sie Speicherpools, die für NDMP-Operationen definiert sind, nicht versehentlich für traditionelle IBM Spectrum Protect-Operationen verwenden. Gehen Sie mit besonderer Sorgfalt vor, wenn Sie den Speicherpoolnamen als Wert für den Parameter DESTINATION im Befehl DEFINE COPYGROUP zuordnen. Wenn der Zielspeicherpool nicht das geeignete Datenformat aufweist, kann die Sicherung fehlschlagen.


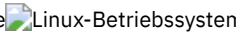
5. Optional: Definieren Sie einen Speicherpool für ein Inhaltsverzeichnis. Wenn Sie planen, ein Inhaltsverzeichnis zu erstellen, müssen Sie auch einen Plattenspeicherpool zum Speichern des Inhaltsverzeichnisses definieren. Sie müssen die Maßnahme so definieren, dass der IBM Spectrum Protect-Server das Inhaltsverzeichnis in einem anderen Speicherpool speichert als das Sicherungsimage. Das Inhaltsverzeichnis wird wie jedes andere Objekt in diesem Speicherpool behandelt. Um beispielsweise einen Speicherpool mit dem Namen TOCPool für eine Einheitenklasse DISK zu definieren, geben Sie den folgenden Befehl aus:

```
define stgpool tocpool disk
```

Definieren Sie dann Datenträger für den Speicherpool.

  Weitere Informationen zum Definieren von Datenträgern befinden sich in Datenträger mit wahlfreiem Zugriff auf Platteneinheiten konfigurieren (Version 7.1.1).

 Weitere Informationen zum Definieren von Datenträgern befinden sich in Datenträger mit wahlfreiem Zugriff auf Platteneinheiten konfigurieren (Version 7.1.1).

  Weitere Informationen zum Konfigurieren von Speicherarchiven finden Sie in Speicherarchive für die Verwendung durch einen Server konfigurieren.

**Zugehörige Verweise:**

DEFINE DEVCLASS (Einheitenklasse definieren)

## Greifarme des Bandarchivs für NAS-Speicherarchive anschließen

Wenn Sie planen, NAS-Daten in einem Speicherarchiv zu sichern, das direkt an die NAS-Einheit angeschlossen ist, und wenn Sie ein SCSI-Bandarchiv verwenden, müssen Sie die Anschlussposition für das Speicherarchiv festlegen.

### Informationen zu diesem Vorgang













Sie müssen festlegen, ob die Greifarme des Speicherarchivs an den IBM Spectrum Protect-Server oder den NAS-Dateiserver angeschlossen werden sollen. Unabhängig davon, wo die Greifarme des Speicherarchivs angeschlossen werden, müssen die Bandlaufwerke für NDMP-Operationen immer an den NAS-Dateiserver angeschlossen werden.

Berücksichtigt werden müssen auch die Entfernung und die verfügbaren Hardwareverbindungen für SCSI-Speicherarchive. Wenn das Speicherarchiv keine separaten Ports für die Greifarmsteuerung und den Laufwerkzugriff hat, muss das Speicherarchiv an den NAS-Dateiserver angeschlossen werden, da der NAS-Dateiserver Zugriff auf die Laufwerke haben muss. Wenn Ihr SCSI-Speicherarchiv über separate Ports für die Greifarmsteuerung und den Laufwerkzugriff verfügt, können Sie wählen, ob die Greifarme des Speicherarchivs an den IBM Spectrum Protect-Server oder den NAS-Dateiserver angeschlossen werden sollen. Wenn sich der NAS-Dateiserver an einem anderen Standort befindet als der IBM Spectrum Protect-Server, kann dies bedeuten, dass Sie das Speicherarchiv an den NAS-Dateiserver anschließen müssen.

Unabhängig davon, ob Sie ein SCSI-, ACSLS- oder 349X-Speicherarchiv verwenden, haben Sie die Wahl, das Speicherarchiv NDMP-Operationen zuzuordnen oder das Speicherarchiv für NDMP-Operationen zu verwenden. Sie können das Speicherarchiv auch für die meisten traditionellen IBM Spectrum Protect-Operationen verwenden.

Tabelle 1. Zusammenfassung der Konfigurationen für NDMP-Operationen

| Konfiguration  | Entfernung zwischen IBM Spectrum Protect-Server und Speicherarchiv | Gemeinsame Speicherarchivnutzung | Gemeinsame Laufwerknutzung zwischen IBM Spectrum Protect und NAS-Dateiserver | Gemeinsame Laufwerknutzung zwischen NAS-Dateiservern | Gemeinsame Laufwerknutzung zwischen Speicheragent und NAS-Dateiserver |
|--|--|----------------------------------|--|--|---|
| Konfiguration 1 (An den IBM Spectrum Protect-Server angeschlossenes SCSI-Speicherarchiv) | Begrenzt durch SCSI- oder FC-Verbindung                            | Unterstützt                      | Unterstützt  | Unterstützt  | Unterstützt   |
| Konfiguration 2 (An den NAS-Dateiserver angeschlossenes SCSI-Speicherarchiv)             | Keine Begrenzung   | Nicht unterstützt                | Unterstützt  | Unterstützt  | Nicht unterstützt   |
| Konfiguration 3 (349X-Speicherarchiv)  | Kann durch 349X-Verbindung begrenzt sein                           | Unterstützt                      | Unterstützt  | Unterstützt  | Unterstützt   |

| Konfiguration   | Entfernung zwischen IBM Spectrum Protect-Server und Speicherarchiv  | Gemeinsame Speicherarchivnutzung  | Gemeinsame Laufwerknutzung zwischen IBM Spectrum Protect und NAS-Dateiserver  | Gemeinsame Laufwerknutzung zwischen NAS-Dateiservern  | Gemeinsame Laufwerknutzung zwischen Speicheragent und NAS-Dateiserver   |
|---|---|---|---|---|---|
|  AIX-Betriebssysteme<br> Windows-Betriebssysteme<br>Konfiguration 4 (ACSL-Speicherarchiv) |  AIX-Betriebssysteme<br> Windows-Betriebssysteme<br>Kann durch ACSLS-Verbindung begrenzt sein |  AIX-Betriebssysteme<br> Windows-Betriebssysteme<br>Unterstützt |  AIX-Betriebssysteme<br> Windows-Betriebssysteme<br>Unterstützt |  AIX-Betriebssysteme<br> Windows-Betriebssysteme<br>Unterstützt |  AIX-Betriebssysteme<br> Windows-Betriebssysteme<br>Unterstützt |

- Konfiguration 1: An den IBM Spectrum Protect-Server angeschlossenes SCSI-Speicherarchiv  
Bei dieser Konfiguration muss das Bandarchiv über separate Ports für die Greifarmsteuerung und den Laufwerkzugriff verfügen. Außerdem muss sich das Speicherarchiv innerhalb des Fibre Channel-Bereichs oder SCSI-Bus-Bereichs sowohl des IBM Spectrum Protect-Servers als auch des NAS-Dateiservers befinden.
- Konfiguration 2: An den NAS-Dateiserver angeschlossenes SCSI-Speicherarchiv  
Bei dieser Konfiguration müssen die Greifarme des Speicherarchivs und die Laufwerke physisch über eine Direktverbindung an den NAS-Dateiserver angeschlossen werden. Pfade müssen von der NAS-Einheit zum Versetzen von Daten zum Speicherarchiv und zu den Laufwerken definiert werden. Es ist keine physische Verbindung zwischen dem IBM Spectrum Protect-Server und dem SCSI-Speicherarchiv erforderlich.
- Konfiguration 3: An den IBM Spectrum Protect-Server angeschlossenes 349x-Speicherarchiv  
Bei dieser Konfiguration schließen Sie das Bandarchiv wie für herkömmliche Operationen an das System an.
- Konfiguration 4: An den IBM Spectrum Protect-Server angeschlossenes ACSLS-Speicherarchiv  
Bei dieser Konfiguration schließen Sie das Bandarchiv wie für herkömmliche IBM Spectrum Protect-Operationen an das System an.

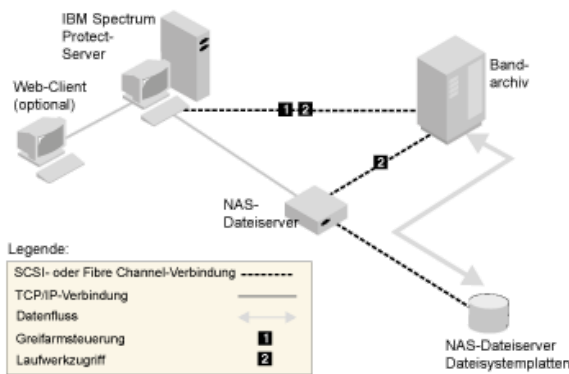
## Konfiguration 1: An den IBM Spectrum Protect-Server angeschlossenes SCSI-Speicherarchiv

Bei dieser Konfiguration muss das Bandarchiv über separate Ports für die Greifarmsteuerung und den Laufwerkzugriff verfügen. Außerdem muss sich das Speicherarchiv innerhalb des Fibre Channel-Bereichs oder SCSI-Bus-Bereichs sowohl des IBM Spectrum Protect-Servers als auch des NAS-Dateiservers befinden.

Bei dieser Konfiguration steuert der IBM Spectrum Protect-Server das SCSI-Speicherarchiv über eine direkte physische Verbindung zum Steueranschluss für die Greifarme des Speicherarchivs. Für NDMP-Operationen werden die Laufwerke im Speicherarchiv direkt an den NAS-Dateiserver angeschlossen; außerdem muss ein Pfad von der NAS-Einheit zum Versetzen von Daten zu jedem Laufwerk, das verwendet werden soll, definiert werden. Der NAS-Dateiserver überträgt auf Anforderung des IBM Spectrum Protect-Servers Daten zum Bandlaufwerk. Um die Laufwerke auch für IBM Spectrum Protect-Operationen verwenden zu können, verbinden Sie den IBM Spectrum Protect-Server mit den Bandlaufwerken und definieren Sie Pfade vom Server zu den Bandlaufwerken.

Diese Konfiguration unterstützt außerdem einen IBM Spectrum Protect-Speicheragenten, der für seine LAN-unabhängigen Operationen Zugriff auf die Laufwerke hat; der IBM Spectrum Protect-Server kann dabei auch ein Speicherarchivmanager sein.

Abbildung 1. Konfiguration 1: An den IBM Spectrum Protect-Server angeschlossenes SCSI-Speicherarchiv

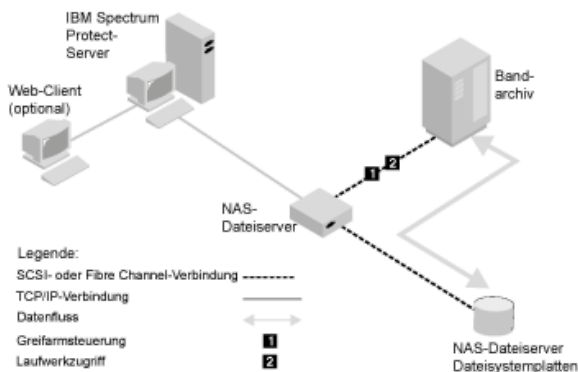


## Konfiguration 2: An den NAS-Dateiserver angeschlossenes SCSI-Speicherarchiv

Bei dieser Konfiguration müssen die Greifarme des Speicherarchivs und die Laufwerke physisch über eine Direktverbindung an den NAS-Dateiserver angeschlossen werden. Pfade müssen von der NAS-Einheit zum Versetzen von Daten zum Speicherarchiv und zu den Laufwerken definiert werden. Es ist keine physische Verbindung zwischen dem IBM Spectrum Protect-Server und dem SCSI-Speicherarchiv erforderlich.

Der IBM Spectrum Protect-Server steuert die Greifarme, indem er Speicherarchivbefehle über das Netz an den NAS-Dateiserver sendet. Der NAS-Dateiserver übergibt die Befehle an das Bandarchiv. Alle vom Speicherarchiv generierten Antworten werden an den NAS-Dateiserver gesendet und über das Netz zurück an den IBM Spectrum Protect-Server übergeben. Diese Konfiguration unterstützt einen IBM Spectrum Protect-Server und einen NAS-Dateiserver, die physisch voneinander getrennt sind. Der IBM Spectrum Protect-Server kann sich beispielsweise in einer anderen Stadt befinden als der NAS-Dateiserver und das Bandarchiv.

Abbildung 1. Konfiguration 2: An den NAS-Dateiserver angeschlossenes SCSI-Speicherarchiv



## Konfiguration 3: An den IBM Spectrum Protect-Server angeschlossenes 349x-Speicherarchiv

Bei dieser Konfiguration schließen Sie das Bandarchiv wie für herkömmliche Operationen an das System an.

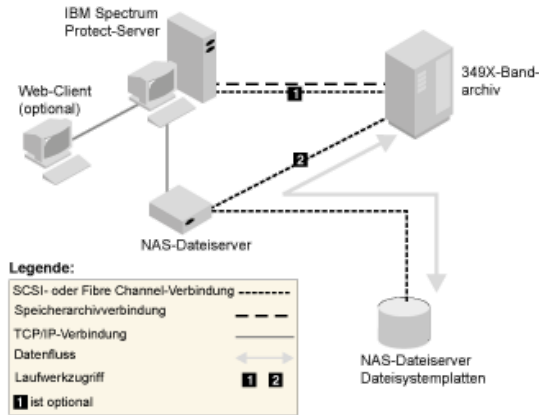
Bei dieser Konfiguration wird das 349X-Bandarchiv durch den IBM Spectrum Protect-Server gesteuert. Der IBM Spectrum Protect-Server steuert das Speicherarchiv, indem die Anforderung über TCP/IP an den 349X-Speicherarchivmanager übergeben wird.

Um NAS-Sicherungs- oder -Zurückschreibungsoperationen auszuführen, muss der NAS-Dateiserver auf ein oder mehrere Bandlaufwerke im 349X-Speicherarchiv zugreifen können. Alle für NAS-Operationen verwendeten Bandlaufwerke müssen physisch an den NAS-Dateiserver angeschlossen sein. Es müssen Pfade von der NAS-Einheit zum Versetzen von Daten zu den Laufwerken definiert werden. Der NAS-Dateiserver überträgt auf Anforderung des IBM Spectrum Protect-Servers Daten zum Bandlaufwerk. Für den Anschluss der Einheit an das Serversystem sind die Anweisungen des Herstellers zu befolgen.



Diese Konfiguration unterstützt einen IBM Spectrum Protect-Server und einen NAS-Dateiserver, die physisch voneinander getrennt sind. Der IBM Spectrum Protect-Server könnte sich beispielsweise in einer anderen Stadt befinden als der NAS-Dateiserver und das Bandarchiv.

Abbildung 1. Konfiguration 3: An den IBM Spectrum Protect-Server angeschlossenes 349x-Speicherarchiv



#### Zugehörige Informationen:

Einheiten für den Server anschließen

## Konfiguration 4: An den IBM Spectrum Protect-Server angeschlossenes ACSLS-Speicherarchiv

Bei dieser Konfiguration schließen Sie das Bandarchiv wie für herkömmliche IBM Spectrum Protect-Operationen an das System an.

Das ACSLS-Bandarchiv (ACSL = Automated Cartridge System Library Software) wird durch den IBM Spectrum Protect-Server gesteuert. Der IBM Spectrum Protect-Server steuert das Speicherarchiv, indem die Anforderung über TCP/IP an den ACSLS-Speicherarchivserver übergeben wird. Das ACSLS-Speicherarchiv unterstützt die gemeinsame Nutzung von Speicherarchiven und LAN-unabhängige Operationen.

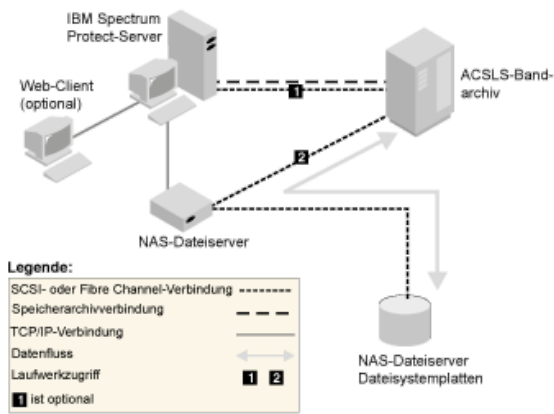
Windows-Betriebssystemeinschränkung: Um ACSLS-Funktionen verwenden zu können, muss StorageTek Library Attach-Software installiert sein. Weitere Informationen finden Sie in ACSLS-verwaltete Speicherarchive (Version 7.1.1).

Um NAS-Sicherungs- oder -Zurückschreibungsoperationen auszuführen, muss der NAS-Dateiserver auf ein oder mehrere Bandlaufwerke im ACSLS-Speicherarchiv zugreifen können. Alle für NAS-Operationen verwendeten Bandlaufwerke müssen physisch an den NAS-Dateiserver angeschlossen sein und alle Pfade von der NAS-Einheit zum Versetzen von Daten zu den Laufwerken müssen definiert werden. Der NAS-Dateiserver überträgt auf Anforderung des IBM Spectrum Protect-Servers Daten zum Bandlaufwerk. Für den Anschluss der Einheit an das Serversystem sind die Anweisungen des Herstellers zu befolgen.

Diese Konfiguration unterstützt einen IBM Spectrum Protect-Server und einen NAS-Dateiserver, die physisch voneinander getrennt sind. Der IBM Spectrum Protect-Server könnte sich beispielsweise in einer anderen Stadt befinden als der NAS-Dateiserver und das Bandarchiv.

Um die Laufwerke auch für IBM Spectrum Protect-Operationen verwenden zu können, müssen Sie den IBM Spectrum Protect-Server mit den Bandlaufwerken verbinden und Pfade vom IBM Spectrum Protect-Server zu den Bandlaufwerken definieren.

Abbildung 1. Konfiguration 4: An den IBM Spectrum Protect-Server angeschlossenes ACSLS-Speicherarchiv



### Zugehörige Informationen:

Einheiten für den Server anschließen

## NAS-Knoten im IBM Spectrum Protect-Server registrieren

Registrieren Sie den NAS-Dateiserver unter Angabe von TYPE=NAS als einen IBM Spectrum Protect-Knoten. Anhand dieses Knotennamens werden die Imagesicherungen für den NAS-Dateiserver protokolliert.

### Vorgehensweise

Geben Sie folgenden Beispielbefehl aus, um einen NAS-Dateiserver als Knoten mit dem Namen NASNODE1 mit dem Kennwort NASPWD1 in einer Maßnahmendomäne mit dem Namen NASDOMAIN zu registrieren:

```
register node nasnode1 naspwd1 domain=nasdomain type=nas
```

Wenn Sie eine Clientoptionsgruppe verwenden, geben Sie die Optionsgruppe beim Registrieren des Knotens an. Sie können prüfen, ob dieser Knoten registriert wurde, indem Sie folgenden Befehl ausgeben:

```
query node type=nas
```

Hinweis: Sie müssen TYPE=NAS angeben, damit nur NAS-Knoten angezeigt werden.

## Einheit zum Versetzen von Daten für einen NAS-Dateiserver definieren

Definieren Sie eine Einheit zum Versetzen von Daten für jeden NAS-Dateiserver unter Verwendung von NDMP-Operationen in Ihrer Umgebung. Der Name der Einheit zum Versetzen von Daten muss mit dem Knotennamen übereinstimmen, den Sie angegeben haben, als Sie den NAS-Knoten für den IBM Spectrum Protect-Server registriert haben.

### Informationen zu diesem Vorgang

IBM Spectrum Protect unterstützt zwei Arten von Einheiten zum Versetzen von Daten:

- Bei NDMP-Operationen handelt es sich bei den Einheiten zum Versetzen von Daten um NAS-Dateiserver. Die Definition für eine NAS-Einheit zum Versetzen von Daten enthält die Netzadresse, die Berechtigung sowie Datenformate, die für NDMP-Operationen erforderlich sind. Eine Einheit zum Versetzen von Daten aktiviert die Übertragung und stellt die Berechtigung für NDMP-Operationen zwischen dem IBM Spectrum Protect-Server und dem NAS-Dateiserver sicher.
- Bei der serverunabhängigen Datenversetzung handelt es sich bei den Einheiten zum Versetzen von Daten um Einheiten wie IBM® SAN Data Gateway, die Daten zwischen Platteinheiten und Bändeinheiten im SAN übertragen.

### Vorgehensweise

Um eine Einheit zum Versetzen von Daten zu definieren, verwenden Sie den Befehl DEFINE DATAMOVER.

### Beispiel

Definieren Sie beispielsweise eine Einheit zum Versetzen von Daten mit den folgenden Parametern:

- Der NAS-Knoten hat den Namen NASNODE1.

- Die Adresse der oberen Ebene ist eine IP-Adresse für den NAS-Dateiserver, und zwar entweder eine numerische Adresse oder ein Hostname.
- Die Adresse der unteren Ebene ist der IP-Port für NDMP-Sitzungen mit dem NAS-Dateiserver. Die Standardportnummer ist 10000.
- Die Benutzer-ID ist die für den NAS-Dateiserver definierte ID, die die Berechtigung für eine NDMP-Sitzung mit dem NAS-Dateiserver bereitstellt. In diesem Beispiel ist die Benutzer-ID die Verwaltungs-ID für den NetApp-Dateiserver.
- Der Kennwortparameter ist ein gültiges Kennwort für die Authentifizierung bei einer NDMP-Sitzung mit dem NAS-Dateiserver.
- Das Datenformat ist NETAPPDUMP. Dieses Datenformat wird vom NetApp-Dateiserver für Bandsicherungen verwendet. Dieses Datenformat muss mit dem Datenformat des Zielspeicherpools übereinstimmen.

Geben Sie den folgenden Befehl ein:

```
define datamover nasnode1 type=nas haddress=netapp2 laddress=10000 userid=root
password=admin dataformat=netappdump
```

#### Zugehörige Verweise:

DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren)

## Pfade für NDMP-Operationen definieren

---

Für NDMP-Operationen müssen Sie Pfade zu Laufwerken und Speicherarchiven erstellen.

- Pfade zu Laufwerken für NDMP-Operationen definieren  
Welche Methode Sie für das Erstellen von Pfaden zu Laufwerken auswählen, ist davon abhängig, ob der Zugriff auf die Laufwerke über einen NAS-Dateiserver und den IBM Spectrum Protect-Server oder ausschließlich über einen NAS-Dateiserver erfolgt.
- Pfade zu Speicherarchiven für NDMP-Operationen definieren  
Definieren Sie entweder vom IBM Spectrum Protect-Server oder vom NAS-Dateiserver einen Pfad zu dem SCSI-Speicherarchiv.

## Pfade zu Laufwerken für NDMP-Operationen definieren

---

Welche Methode Sie für das Erstellen von Pfaden zu Laufwerken auswählen, ist davon abhängig, ob der Zugriff auf die Laufwerke über einen NAS-Dateiserver und den IBM Spectrum Protect-Server oder ausschließlich über einen NAS-Dateiserver erfolgt.

- Pfade für an einen NAS-Dateiserver und an den IBM Spectrum Protect-Server angeschlossene Laufwerke definieren  
Wenn der Zugriff auf ein Bandlaufwerk über einen NAS-Dateiserver und den IBM Spectrum Protect-Server erfolgen muss, müssen Sie zwei Pfade erstellen. Ein Pfad ist zwischen dem Bandlaufwerk und dem NAS-Dateiserver vorhanden. Der andere Pfad ist zwischen dem Bandlaufwerk und dem IBM Spectrum Protect-Server vorhanden.
- Pfade für nur an NAS-Dateiserver angeschlossene Laufwerke definieren  
Wenn der Zugriff auf ein Bandlaufwerk ausschließlich über einen NAS-Dateiserver und nicht über den IBM Spectrum Protect-Server erfolgen muss, ist nur ein einziger Pfad zwischen dem Bandlaufwerk und dem NAS-Dateiserver erforderlich.
- Namen für an NAS-Dateiserver angeschlossene Einheiten abrufen  
Für Pfade von einer NAS-Einheit zum Versetzen von Daten ist der Wert des Parameters DEVICE im Befehl DEFINE PATH der Name, unter dem der NAS-Dateiserver ein Speicherarchiv oder ein Laufwerk kennt.

## Pfade für an einen NAS-Dateiserver und an den IBM Spectrum Protect-Server angeschlossene Laufwerke definieren

---

Wenn der Zugriff auf ein Bandlaufwerk über einen NAS-Dateiserver und den IBM Spectrum Protect-Server erfolgen muss, müssen Sie zwei Pfade erstellen. Ein Pfad ist zwischen dem Bandlaufwerk und dem NAS-Dateiserver vorhanden. Der andere Pfad ist zwischen dem Bandlaufwerk und dem IBM Spectrum Protect-Server vorhanden.

## Vorgehensweise

---

Führen Sie die folgenden Schritte aus:

1. Wenn das Laufwerk für den IBM Spectrum Protect-Server nicht definiert ist, erstellen Sie die Laufwerkdefinition. Um beispielsweise das Laufwerk NASDRIVE1 für das Speicherarchiv NASLIB zu definieren, geben Sie den folgenden Befehl aus:

```
define drive naslib nasdrive1 element=autodetect
```

Hinweis: Wenn das Laufwerk an den IBM Spectrum Protect-Server angeschlossen ist, wird die Elementadresse automatisch erkannt.

2. Ordnen Sie den NAS-Laufwerknamen der entsprechenden Laufwerkdefinition auf dem IBM Spectrum Protect-Server zu:
  - Geben Sie auf dem IBM Spectrum Protect-Server den Befehl QUERY DRIVE FORMAT=DETAILED aus, um den weltweiten Namen (WWN) und die Seriennummer für das Laufwerk abzurufen, das an den NAS-Dateiserver angeschlossen wird.

- Rufen Sie auf der NAS-Einheit den Bandeinheitennamen, die Seriennummer und den weltweiten Namen für das Laufwerk ab.

Wenn der weltweite Name oder die Seriennummer übereinstimmen, ist das Laufwerk auf dem NAS-Dateiserver mit dem Laufwerk auf dem IBM Spectrum Protect-Server identisch.

3. Definieren Sie unter Verwendung des Laufwerknamens jeweils einen Pfad vom NAS-Dateiserver und vom IBM Spectrum Protect-Server zu dem Laufwerk.

- Um beispielsweise einen Pfad zwischen einem Bandlaufwerk mit dem Einheitennamen rst01 und einem NetApp-Dateiserver zu definieren, geben Sie den folgenden Befehl aus:

```
define path nasnode1 nasdrive1 srctype=datamover desttype=drive
  library=naslib device=rst01
```

- Um einen Pfad zwischen dem Bandlaufwerk und dem IBM Spectrum Protect-Server zu definieren, geben Sie den folgenden Befehl aus:

#### AIX-Betriebssysteme

```
define path server1 nasdrive1 srctype=server desttype=drive
  library=naslib device=/dev/rmt0
```

#### Linux-Betriebssysteme

```
define path server1 nasdrive1 srctype=server desttype=drive
  library=naslib device=/dev/tsm SCSI/mt0
```

#### Windows-Betriebssysteme

```
define path server1 nasdrive1 srctype=server desttype=drive
  library=naslib device=mt3.0.0.2
```

## Pfade für nur an NAS-Dateiserver angeschlossene Laufwerke definieren




Wenn der Zugriff auf ein Bandlaufwerk ausschließlich über einen NAS-Dateiserver und nicht über den IBM Spectrum Protect-Server erfolgen muss, ist nur ein einziger Pfad zwischen dem Bandlaufwerk und dem NAS-Dateiserver erforderlich.

### Vorgehensweise

Führen Sie die folgenden Schritte aus:

1. Rufen Sie die SCSI-Elementadresse, den weltweiten Name (WWN, worldwide name) und die Seriennummer für das Laufwerk ab, das an den NAS-Dateiserver angeschlossen werden soll.  
Einschränkung: Wenn das SCSI-Laufwerk nur an einen NAS-Dateiserver angeschlossen ist, wird die Elementadresse nicht automatisch erkannt, sodass Sie die Adresse angeben müssen. Wenn ein Speicherarchiv über mehrere Laufwerke verfügt, müssen Sie eine Elementadresse für jedes Laufwerk angeben.

Um eine SCSI-Elementadresse abzurufen, rufen Sie die folgenden Websites für die Einheitenunterstützung auf:

-  AIX-Betriebssysteme  Windows-Betriebssysteme Supported devices for AIX and Windows
-  Linux-Betriebssysteme Supported devices for Linux

Die Elementnummernzuordnung und Zuordnungen weltweiter Namen für Einheiten werden auch von den Herstellern der Bandarchiveinheiten zur Verfügung gestellt.

2. Erstellen Sie Laufwerkdefinitionen, indem Sie die im vorherigen Schritt identifizierte Elementadresse angeben. Geben Sie die Elementadresse im Parameter ELEMENT des Befehls DEFINE DRIVE an. Um beispielsweise das Laufwerk NASDRIVE1 mit der Elementadresse 82 für das Speicherarchiv NASLIB zu definieren, geben Sie den folgenden Befehl aus:

```
define drive naslib nasdrive1 element=82
```

Achtung: Für ein Laufwerk, das an den NAS-Dateiserver angeschlossen ist, dürfen Sie nicht ASNEEDED als Wert für den Parameter CLEANFREQUENCY im Befehl DEFINE DRIVE angeben.

3. Rufen Sie den Einheitennamen, die Seriennummer und den weltweiten Name für das Laufwerk auf der NAS-Einheit ab.
4. Ordnen Sie mithilfe der in den Schritten 1 und 3 abgerufenen Informationen den Namen der NAS-Einheit der Elementadresse in der Laufwerkdefinition auf dem IBM Spectrum Protect-Server zu.
5. Definieren Sie einen Pfad zwischen dem Bandlaufwerk und dem NAS-Dateiserver. Um beispielsweise eine Pfad zwischen einem NetApp-Dateiserver und einem Bandlaufwerk mit dem Einheitennamen rst01 zu definieren, geben Sie den folgenden Befehl aus:

```
define path nasnode1 nasdrive1 srctype=datamover desttype=drive
  library=naslib device=rst01
```

## Namen für an NAS-Dateiserver angeschlossene Einheiten abrufen

Für Pfade von einer NAS-Einheit zum Versetzen von Daten ist der Wert des Parameters DEVICE im Befehl DEFINE PATH der Name, unter dem der NAS-Dateiserver ein Speicherarchiv oder ein Laufwerk kennt.

## Informationen zu diesem Vorgang

Sie können diese Einheitennamen, die auch als *Gerätedateinamen* bezeichnet werden, können durch Abfragen des NAS-Dateiservers abrufen. Informationen zum Abrufen der Namen von Einheiten, die mit einem NAS-Dateiserver verbunden sind, finden Sie in der Produktinformation zum Dateiserver.

## Vorgehensweise

- Um die Einheitennamen für Bandarchive auf einem Dateiserver unter NetApp Release ONTAP 10.0 GX oder höher abzurufen, stellen Sie mithilfe von Telnet die Verbindung zum Dateiserver her und geben Sie den Befehl SYSTEM HARDWARE TAPE LIBRARY SHOW aus. Um die Einheitennamen für Bandlaufwerke auf einem Dateiserver unter NetApp Release ONTAP 10.0 GX oder höher abzurufen, stellen Sie mithilfe von Telnet die Verbindung zum Dateiserver her und geben Sie den Befehl SYSTEM HARDWARE TAPE DRIVE SHOW aus. Ausführliche Informationen zu diesen Befehlen finden Sie in der Produktdokumentation des NetApp ONTAP GX-Dateiservers.
- Verwenden Sie für Releases vor NetApp Release ONTAP 10.0 GX weiterhin den Befehl SYSCONFIG. Um beispielsweise die Einheitennamen für Bandarchive anzuzeigen, stellen Sie mithilfe von Telnet die Verbindung zum Dateiserver her und geben Sie den folgenden Befehl aus:

```
sysconfig -m
```

Geben Sie folgenden Befehl aus, um die Einheitennamen für Bandlaufwerke anzuzeigen:

```
sysconfig -t
```

- Führen Sie für Laufwerke, die über Fibre Channel angeschlossen sind, und die Celerra-Einheit zum Versetzen von Daten die folgenden Schritte aus:
  1. Melden Sie sich bei der EMC Celerra-Steuerwerkstation mit einer Verwaltungs-ID an. Geben Sie den folgenden Befehl aus:

```
server_devconfig server_1 -l -s -n
```

Tipp: Mit der Option -l für diesen Befehl werden nur die Einheitsdaten aufgelistet, die in der Datenbank der Einheit zum Versetzen von Daten gespeichert wurden. Mit dem Befehl und der Option werden keine Änderungen an der Einheitenkonfiguration angezeigt, die nach der letzten Datenbankaktualisierung auf der Einheit zum Versetzen von Daten durchgeführt wurden. Ausführliche Informationen zum Abrufen der neuesten Einheitenkonfiguration für Ihre Einheit zum Versetzen von Daten enthält die EMC Celerra-Dokumentation.

Die Ausgabe für den Befehl server\_devconfig umfasst die Einheitennamen für die Einheiten, die an die Einheit zum Versetzen von Daten angeschlossen sind. Die Einheitennamen sind in der Spalte *addr* aufgeführt, z. B.:

```
server_1:
SCSI-Einheitentabelle
name      addr      type      info
tapel     c64t010  tape     IBM ULT3580-TD2 53Y2
ttapel    c96t010  tape     IBM ULT3580-TD2 53Y2
```

2. Ordnen Sie den Celerra-Einheitennamen dem weltweiten Namen (WWN, worldwide name) der Einheit zu:
  - a. Um den weltweiten Namen aufzulisten, melden Sie sich bei der EMC Celerra-Steuerwerkstation an und geben Sie den folgenden Befehl aus. Beachten Sie, dass Sie in diesem Befehl als erstes Zeichen einen Punkt (.) angeben müssen.

```
.server_config server_# -v "fcv bind show"
```

Die Ausgabe für diesen Befehl umfasst den weltweiten Namen (WWN), z. B.:

```
Chain 0064: WWN 500507630f418e29 HBA 2 N_PORT Bound
Chain 0096: WWN 500507630f418e18 HBA 2 N_PORT Bound
```

Tipp: Der Befehl .server\_config ist ein EMC Celerra-Befehl, der nicht dokumentiert ist. Weitere Informationen zur Verwendung dieses Befehls erhalten Sie von EMC.

- b. Identifizieren Sie die Bändeinheit, die in der Ausgabe des Befehls server\_devconfig aufgelistet war und denselben weltweiten Namen (WWN) hat mithilfe der Kettennummer, z. B.:

| Bandeinheitennamen | Kettennummer | WWN              |
|--------------------|--------------|------------------|
| c64t010            | 0064         | 500507630f418e29 |
| c96t010            | 0096         | 500507630f418e18 |

Das Verhalten von Celerra-Befehlen kann auf verschiedenen EMC Celerra-Systemen und Betriebssystemversionen variieren. Um ausführliche Informationen zu erhalten, lesen Sie in der EMC Celerra-Dokumentation nach oder wenden Sie sich an EMC.

## Pfade zu Speicherarchiven für NDMP-Operationen definieren

---

Definieren Sie entweder vom IBM Spectrum Protect-Server oder vom NAS-Dateiserver einen Pfad zu dem SCSI-Speicherarchiv.

### Vorgehensweise

---

1. Geben Sie für ein SCSI-Speicherarchiv, das mit IBM Spectrum Protect verbunden ist, den folgenden Beispielbefehl aus, um einen Pfad von dem Server mit dem Namen SERVER1 zu dem SCSI-Speicherarchiv mit dem Namen TSMLIB zu definieren:

#### AIX-Betriebssysteme

```
define path server1 tsmlib srctype=server desttype=library
device=/dev/lb1
```

#### Linux-Betriebssysteme

```
define path server1 tsmlib srctype=server desttype=library
device=/dev/tmscsi/lb1
```

#### Windows-Betriebssysteme

```
define path server1 tsmlib srctype=server desttype=library
device=lb0.0.0.2
```

2. Geben Sie für ein SCSI-Speicherarchiv, das mit einem NAS-Dateiserver verbunden ist, den folgenden Beispielbefehl aus, um einen Pfad zwischen einer NetApp-NAS-Einheit zum Versetzen von Daten mit dem Namen NASNODE1 und einem Speicherarchiv mit dem Namen NASLIB zu definieren:

```
define path nasnode1 naslib srctype=datamover desttype=library device=mc0
```

3. Definieren Sie für ein 349X-Speicherarchiv einen Pfad vom IBM Spectrum Protect-Server zum Speicherarchiv. Geben Sie beispielsweise den folgenden Befehl ein, um einen Pfad vom Server mit dem Namen SERVER1 zum 349X-Speicherarchiv mit dem Namen TSMLIB zu definieren:

#### AIX-Betriebssysteme

```
define path server1 tsmlib srctype=server desttype=library
device=/dev/lmcp0
```

#### Linux-Betriebssysteme Windows-Betriebssysteme

```
define path server1 tsmlib srctype=server desttype=library
device=library1
```

Tipp: Der Befehl DEFINE PATH ist für ein ACSLS-Speicherarchiv nicht erforderlich.

## NDMP-Operationen planen

---

Sie können Sicherungs- oder Zurückschreibungsoperationen für Images planen, die von NDMP-Operationen erstellt werden. Verwenden Sie Verwaltungszeitpläne, die den Verwaltungsbefehl BACKUP NODE oder RESTORE NODE verarbeiten.

### Vorgehensweise

---


Erstellen Sie einen Verwaltungszeitplan mit dem Befehl DEFINE SCHEDULE. Um beispielsweise einen Verwaltungszeitplan mit dem Namen NASSCHED zu erstellen, um alle Dateisysteme für den Knoten NASNODE1 zu sichern, geben Sie den folgenden Befehl ein:

```
define schedule nassched type=administrative cmd='backup node nasnode1' active=yes
starttime=20:00 period=1 perunits=days
```

Der Zeitplan ist aktiv und wird jeden Tag um 20 Uhr ausgeführt.

Einschränkung: Die Befehle BACKUP NODE und RESTORE NODE können nur für Knoten mit TYPE=NAS verwendet werden.

#### **Zugehörige Tasks:**

 Zeitplan für tägliche Operationen optimieren

#### **Zugehörige Verweise:**

BACKUP NODE (NAS-Knoten sichern)

RESTORE NODE (NAS-Knoten zurückschreiben)

DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)

## Virtuelle Dateibereiche definieren

---

Verwenden Sie die Definition eines virtuellen Dateibereichs, um NAS-Sicherungen auf Verzeichnisebene auszuführen. Um die Sicherungs- und Zurückschreibungszeiten für große Dateisysteme zu reduzieren, ordnen Sie einen Verzeichnispfad von einem NAS-Dateiserver zum Namen eines virtuellen Dateibereichs auf dem IBM Spectrum Protect-Server zu.

### Vorgehensweise

---

Um den Namen eines virtuellen Dateibereichs für den Verzeichnispfad auf der NAS-Einheit zu erstellen, geben Sie den Befehl DEFINE VIRTUALFSMAPPING aus:

```
define virtualfsmapping nas1 /mikesdir /vol/voll /mikes
```

Mit diesem Befehl wird der Name des virtuellen Dateibereichs /MIKESDIR auf dem Server definiert, der den Verzeichnispfad /VOL/VOL1/MIKES auf dem NAS-Dateiserver darstellt, der durch Knoten NAS1 dargestellt wird. Weitere Informationen finden Sie in Sicherung und Zurückschreibung auf Verzeichnisebene für NDMP-Operationen.

## Daten mit der Band-zu-Band-Kopierfunktion sichern

---

Wenn Sie die NDMP-Band-zu-Band-Kopierfunktion zum Sichern von Daten verwenden, kann der Speicherarchivtyp SCSI, 349X oder ACSLS (Automated Cartridge System Library Software) sein. Laufwerke können von den NAS-Einheiten und dem IBM Spectrum Protect-Server gemeinsam genutzt werden.

### Informationen zu diesem Vorgang

---

Wenn Sie die NDMP-Band-zu-Band-Kopierfunktion verwenden, könnte Ihr Konfigurationssetup Auswirkungen auf die Leistung bei der Back-End-Datenversetzung in IBM Spectrum Protect haben.

### Vorgehensweise

---

Um eine einzelne NAS-Einheit mit Pfaden zu vier Laufwerken in einem Speicherarchiv zu definieren, verwenden Sie den Befehl MOVE DATA, nachdem Sie Ihr Konfigurationssetup abgeschlossen haben. Damit werden Daten auf dem Datenträger VOL1 auf alle verfügbaren Datenträger in demselben Speicherpool wie VOL1 versetzt:

```
move data voll
```

## Daten mit der Band-zu-Band-Kopierfunktion versetzen

---

Um Daten unter Verwendung der NDMP-Band-zu-Band-Kopieroperation von einer vorherigen Bandtechnologie in eine neue Bandtechnologie zu versetzen, müssen Sie die Standardschritte in Ihrem Konfigurationssetup sowie weitere Schritte ausführen.

### Informationen zu diesem Vorgang

---

Wenn Sie die NDMP-Band-zu-Band-Kopierfunktion verwenden, könnte Ihr Konfigurationssetup Auswirkungen auf die Leistung bei der Back-End-Datenversetzung in IBM Spectrum Protect haben.

### Vorgehensweise

---

Führen Sie zusätzlich zu den Standardschritten in Ihrem Konfigurationssetup die folgenden Schritte aus:

1. Definieren Sie ein einzelnes Laufwerk in dem Speicherarchiv lib1, das über die vorherige Bandtechnologie verfügt:

```
define drive lib1 drv1 element=1035
```

2. Definieren Sie ein Laufwerk in dem Speicherarchiv lib2, das über die neue Bandtechnologie verfügt:

```
define drive lib2 drv1 element=1036
```

3. Definieren Sie Pfade vom NAS-Dateiserver zu jedem Laufwerk:

```
define path nas1 drv1 sourcetype=datamover desttype=drive library=lib1 device=rst11  
define path nas1 drv1 sourcetype=datamover desttype=drive library=lib2 device=rst21
```

4. Versetzen Sie Daten auf dem Datenträger voll in dem primären Speicherpool auf die Datenträger in einem anderen primären Speicherpool nasprimpool2:

# IBM Spectrum Protect für NDMP-Operationen in einer NetApp-Clusterumgebung konfigurieren

Sie können Daten von einem NetApp-Cluster auf einer direkt angeschlossenen Bandeinheit oder einem IBM Spectrum Protect-Server sichern, der die Daten in einem Speicherpool speichert. Sie können den gesamten Cluster auf einem einzigen IBM Spectrum Protect-Knoten oder Teile des Clusters auf mehreren Knoten sichern.

## Vorbereitende Schritte

Eine Übersicht über die NDMP-Funktionalität in IBM Spectrum Protect- und NetApp-Dateiservern finden Sie in der Technote 7046965. In dieser Technote sind auch die Systemvoraussetzungen aufgelistet.

## Informationen zu diesem Vorgang

Sie können Daten in einer NetApp-Clusterumgebung auf den folgenden Speichermedien sichern:

**Bandeinheit, die direkt an einen NAS-Dateiserver angeschlossen ist**

Sie können Daten auf einer Bandeinheit sichern, die direkt an einen NAS-Dateiserver angeschlossen ist. Dies ist die bevorzugte Methode. In der Regel erfolgt die Sicherung von Daten auf einer direkt angeschlossenen Bandeinheit schneller als die Sicherung von Daten in einem IBM Spectrum Protect-Speicherpool mithilfe einer Netzverbindung.

**Speicherpool in der lokalen IBM Spectrum Protect-Hierarchie**

Sie können Daten auf einem IBM Spectrum Protect-Server sichern, der die Daten in einem Speicherpool des Typs DISK, FILE oder Band speichert. Das Speichern von Daten in einem Speicherpool hat den Vorteil, dass Sie die Daten replizieren können, um den Datenschutz zu verbessern. Sie können vorhandene Speicherpools verwenden oder Speicherpools erstellen. Zwischen dem NAS-Dateiserver und dem IBM Spectrum Protect-Server muss eine Netzverbindung vorhanden sein. Die Netzverbindung muss über genügend Bandbreite für die Übertragung der NAS-Sicherungsdaten verfügen.

Tipp: Dieser Sicherungstyp wird manchmal auch als 'Sicherung vom Dateiserver auf den Server' bezeichnet.

Sie können eine der folgenden Sicherungsmethoden verwenden:

**Clustergesamtsicherung**

Wenn Sie diese Methode anwenden, ist ein einzelner IBM Spectrum Protect-Knoten Eigner der Sicherungsdaten des gesamten Clusters. Selbst wenn die Datenträger innerhalb des Clusters verschoben werden, werden Clustergesamtsicherungsoperationen fortgesetzt und Sie müssen Sicherungsoperationen nicht rekonfigurieren. Dies ist die bevorzugte Methode.

**Clusterteilsicherung**

Wenn Sie diese Methode anwenden, geben Sie eine NetApp Storage Virtual Machine (SVM) an, die den Bereich der Sicherungsoperation angibt. Die SVM ist ein virtueller Server, der Zugriff auf einen Teil eines Clusters bereitstellt. Sie können angeben, dass jede SVM in dem Cluster Daten auf einem anderen IBM Spectrum Protect-Knoten sichert. Diese Methode erfordert eine umfangreichere Konfiguration als die Clustergesamtsicherungsmethode sowie eine Netzverbindung für die Übertragung von Daten von der SVM auf den IBM Spectrum Protect-Knoten.

Einschränkung: Sie können diese Methode nicht verwenden, um Daten auf einer Bandeinheit zu sichern, da SVMs keinen direkten Zugriff auf Bandeinheiten haben.

## Vorgehensweise

1. Wählen Sie die Speichermedien auf der Basis der folgenden Fragen aus:

| Frage  | Speichermedien   |
|--|--|
| Ist es aufgrund Ihrer Geschäftsanforderungen erforderlich, Daten auf einer lokalen Bandeinheit zu sichern? | Lautet die Antwort 'Ja', verwenden Sie eine direkt angeschlossene Bandeinheit.<br><br>Lautet die Antwort 'Nein', verwenden Sie entweder eine direkt angeschlossene Bandeinheit oder einen lokalen IBM Spectrum Protect-Speicherpool. |
| Sind für Ihr Unternehmen Hochgeschwindigkeitssicherungsoperationen erforderlich?                           | Lautet die Antwort 'Ja', verwenden Sie eine direkt angeschlossene Bandeinheit.<br><br>Lautet die Antwort 'Nein', verwenden Sie entweder eine direkt angeschlossene Bandeinheit oder einen lokalen IBM Spectrum Protect-Speicherpool. |
| Verfügt Ihr Unternehmen über genügend Netzbandbreite für NAS-Sicherungsdaten?                              | Lautet die Antwort 'Ja', verwenden Sie entweder eine direkt angeschlossene Bandeinheit oder einen lokalen IBM Spectrum Protect-Speicherpool.<br><br>Lautet die Antwort 'Nein', verwenden Sie eine direkt angeschlossene Bandeinheit. |



| Frage   | Speichermedien  |
|---|---|
| Möchte Ihr Unternehmen mithilfe der Replikation den Datenschutz verbessern?                                 | Lautet die Antwort 'Ja', verwenden Sie einen lokalen IBM Spectrum Protect-Speicherpool.<br><br>Lautet die Antwort 'Nein', verwenden Sie entweder eine direkt angeschlossene Bandeinheit oder einen lokalen IBM Spectrum Protect-Speicherpool. |
| Befinden sich Ihre NAS-Dateiserver an fernen Standorten ohne Zugriff auf direkt angeschlossene Bandarchive? | Lautet die Antwort 'Ja', verwenden Sie einen lokalen IBM Spectrum Protect-Speicherpool.<br><br>Lautet die Antwort 'Nein', verwenden Sie entweder eine direkt angeschlossene Bandeinheit oder einen lokalen IBM Spectrum Protect-Speicherpool. |

2. Wählen Sie eine Sicherungsmethode auf der Basis der folgenden Fragen aus:

| Frage  | Sicherungsmethode   |
|--|---|
| Ist es aufgrund Ihrer Geschäftsanforderungen erforderlich, Daten auf einer direkt angeschlossenen Bandeinheit zu sichern?      | Lautet die Antwort 'Ja', verwenden Sie die Gesamtsicherungsmethode.<br><br>Lautet die Antwort 'Nein', verwenden Sie entweder die Gesamt- oder die Teilsicherungsmethode.  |
| Verfügt Ihr System über genügend Netzbandbreite, um mehrere SVMs ohne Auswirkungen auf die Netzleistung sichern zu können?     | Lautet die Antwort 'Ja', verwenden Sie entweder die Gesamt- oder die Teilsicherungsmethode.<br><br>Lautet die Antwort 'Nein', verwenden Sie die Gesamtsicherungsmethode. Die Teilsicherungsmethode kann sich unter Umständen negativ auf die Systemleistung auswirken.  |
| Sind die SVMs über mehrere Unternehmen verteilt? Werden beispielsweise SVMs durch Dritte wie Cloudplattformprovider gesteuert? | Lautet die Antwort 'Ja', verwenden Sie die Teilsicherungsmethode, da SVM-Eigner Sicherungsoperationen für einzelne SVMs steuern können. Wenn ein SVM-Eigner auch Eigner eines IBM Spectrum Protect-Servers ist, kann der Eigner Sicherungsoperationen von der SVM zu einem Serverknoten konfigurieren. Auf diese Art und Weise kann der Eigner den End-to-End-Prozess steuern.<br><br>Lautet die Antwort 'Nein', verwenden Sie entweder die Gesamt- oder die Teilsicherungsmethode. |

3. Konfigurieren Sie die Systemumgebung auf der Basis der ausgewählten Speichermedien und der ausgewählten Sicherungsmethode. Führen Sie die Anweisungen für die von Ihnen ausgewählte Methode aus:

- Clustergesamtsicherungen auf direkt angeschlossene Bandeinheiten konfigurieren
- Clustergesamtsicherungen mit einem IBM Spectrum Protect-Server als Ziel konfigurieren
- Clusterteilsicherungen mit einem IBM Spectrum Protect-Server als Ziel konfigurieren

Tipp: Wenn Sie IBM Spectrum Protect zum Sichern von NetApp-Clustern mithilfe von NDMP auf Knotenebene konfiguriert haben, ziehen Sie die Rekonfiguration von IBM Spectrum Protect für die Verwendung von NDMP Cluster Aware Backup (CAB) in Erwägung. Auf diese Art und Weise können Sie Sicherungsoperationen für NetApp-Cluster optimieren. Führen Sie die Anweisungen in IBM Spectrum Protect für die Optimierung von Clustersicherungen rekonfigurieren aus.

- Clustergesamtsicherungen auf direkt angeschlossene Bandeinheiten konfigurieren  
Sie können IBM Spectrum Protect für die Sicherung aller Datenträger in einem NetApp-Cluster auf eine direkt angeschlossene Bandeinheit konfigurieren.
- Clustergesamtsicherungen mit einem IBM Spectrum Protect-Server als Ziel konfigurieren  
Sie können IBM Spectrum Protect für die Sicherung aller Datenträger in einem NetApp-Cluster mit einem IBM Spectrum Protect-Server als Ziel konfigurieren, der die Daten in einem Speicherpool speichert. Selbst wenn Datenträger innerhalb des Clusters verschoben werden, werden Sicherungsoperationen fortgesetzt und es ist keine Rekonfiguration erforderlich.
- Clusterteilsicherungen mit einem IBM Spectrum Protect-Server als Ziel konfigurieren  
Sie können IBM Spectrum Protect für die Ausführung einer Teilsicherung eines NetApp-Clusters konfigurieren. Diese Methode ist geeignet, wenn mehrere Unternehmen Eigner von Daten in dem Cluster sind. Jedes Unternehmen kann Sicherungsoperationen für seine Daten verwalten.
- IBM Spectrum Protect für die Optimierung von Clustersicherungen rekonfigurieren  
Wenn Sie IBM Spectrum Protect zum Sichern von NetApp-Clustern mithilfe von NDMP auf Knotenebene konfiguriert haben, können Sie IBM Spectrum Protect für die Verwendung von NDMP Cluster Aware Backup (CAB) rekonfigurieren. Auf diese Art und Weise können Sie Sicherungsoperationen für NetApp-Cluster optimieren.

## Clustergesamtsicherungen auf direkt angeschlossene Bandeinheiten konfigurieren

Sie können IBM Spectrum Protect für die Sicherung aller Datenträger in einem NetApp-Cluster auf eine direkt angeschlossene Bänderinheit konfigurieren.

## Vorbereitende Schritte

---

Eine Übersicht über die NDMP-Funktionalität in IBM Spectrum Protect- und NetApp-Dateiservern finden Sie in der Technote 7046965. In dieser Technote sind auch die Systemvoraussetzungen aufgelistet.

Wenn das Betriebssystem NetApp Clustered Data ONTAP 8.2 oder höher oder 9.1 oder höher auf Ihrem NetApp-Dateiserver installiert ist, verwenden Sie die folgende Prozedur. Nach der Konfiguration Ihres NetApp-Dateiservers für den gemeinsamen Einsatz mit IBM Spectrum Protect können Sie die Erweiterung NetApp Cluster Aware Backup (CAB) zum Sichern aller Datenträger verwenden.

Wenn das Betriebssystem NetApp Clustered Data ONTAP 8.2 oder höher oder 9.1 oder höher nicht auf Ihrem NetApp-Dateiserver installiert ist, sichern Sie Daten anhand der Anweisungen in IBM Spectrum Protect für NDMP-Operationen in einer Umgebung ohne Clustering konfigurieren.

## Informationen zu diesem Vorgang

---

Die bevorzugte Methode ist das Sichern des gesamten Clusters unter Verwendung eines Knotens und einer Einheit zum Versetzen von Daten, die dem clusterweiten Netz zugeordnet sind. Auf diese Art und Weise wird sichergestellt, dass ein einzelner IBM Spectrum Protect-Knoten Eigner der Sicherungsdaten ist. Selbst wenn Datenträger innerhalb des Clusters verschoben werden, werden Sicherungsoperationen fortgesetzt und es ist keine Rekonfiguration erforderlich.

## Vorgehensweise

---

Um Clustergesamtsicherungsoperationen auf eine direkt angeschlossene Bänderinheit zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass IBM Spectrum Protect Extended Edition installiert und die Lizenz registriert ist. Wenn die Lizenz nicht registriert ist, geben Sie den folgenden IBM Spectrum Protect-Befehl aus:

```
register license file=tsmee.lic
```

2. Fordern Sie Clusteradministratorberechtigungen für den NetApp-Dateiserver an. Dieser Schritt ist für den Zugriff auf die Clusterkonsole erforderlich.
3. Aktivieren Sie auf dem NetApp-Dateiserver die Verwendung von NDMP, indem Sie die Anweisungen in der Veröffentlichung *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide* ausführen. Führen Sie die folgenden Schritte aus:
  - a. Aktivieren Sie auf Clusterebene NDMP-Sicherungsoperationen auf SVM-Ebene. Auf diese Art und Weise inaktivieren Sie auf dem NAS-Dateiserver NDMP-Sicherungsoperationen auf Knotenebene. Stellen Sie sicher, dass die Option `node-scoped-ndmp` auf dem NAS-Dateiserver auf OFF gesetzt ist.
  - b. Erstellen Sie eine Sicherungsbenutzer-ID für NDMP-Operationen.
  - c. Konfigurieren Sie eine Netzschnittstelle für NDMP-Steuerverbindungen auf Clusterebene.
4. Registrieren Sie den IBM Spectrum Protect-Knoten, der Eigner aller Sicherungsdaten für den Cluster werden soll. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl REGISTER NODE aus:

```
register node Knotenname Kennwort domain=NAS-Domäne type=nas
```

Dabei gibt *Knotenname* den Knotennamen, *Kennwort* das Knotenkennwort und *NAS-Domäne* die Domäne des Knotens an. Ordnen Sie den Knoten einer Domäne zu, die über eine Maßnahme zum Sichern von Daten in einem entsprechenden Speicherpool verfügt.

5. Bestimmen Sie die IP-Adresse der NetApp-Cluster-Managementschnittstelle auf dem NAS-Dateiserver. Die Schnittstelle stellt Zugriff auf den gesamten Cluster bereit. Geben Sie auf dem NAS-Dateiserver den folgenden Data ONTAP-Betriebssystembefehl aus:

```
network interface show -role cluster-mgmt
```

Die IP-Adresse, die in der Befehlsausgabe angezeigt wird, ist erforderlich, wenn Sie den Parameter HLADDRESS in Schritt 6 angeben.

6. Definieren Sie eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Knoten, der Eigner der Sicherungsdaten werden soll. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl DEFINE DATAMOVER in einer einzigen Zeile aus:

```
define datamover Name_der_Einheit_zum_Versetzen_von_Daten type=nascluster  
hladdress=Cluster-Managementschnittstelle lladdress=Port  
USER=Benutzername password=Kennwort dataformat=netappdump
```

Dabei ist *Cluster-Managementschnittstelle* der Wert aus Schritt 5 und *Name\_der\_Einheit\_zum\_Versetzen\_von\_Daten* der in Schritt 4 registrierte Knotenname. Informationen zur Angabe der anderen Parameter finden Sie in DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren).

Tipp: Nach dem Definieren der Einheit zum Versetzen von Daten werden weitere Einheiten zum Versetzen von Daten automatisch für jeden Knoten in dem Cluster definiert. Der Name der jeweiligen Einheit zum Versetzen von Daten stimmt mit dem Namen des physischen Knotens in dem Cluster überein. Diese Einheiten zum Versetzen von Daten werden beim Definieren von Pfaden zu Bandlaufwerken in Schritt 3 in Bandeinheiten für Clustergesamtsicherungen konfigurieren verwendet.

## Nächste Schritte

---

Um die Bandeinheit für die Clustergesamtsicherung zu konfigurieren, führen Sie die Anweisungen in Bandeinheiten für Clustergesamtsicherungen konfigurieren aus.

- Bandeinheiten für Clustergesamtsicherungen konfigurieren  
Wenn Sie planen, alle Datenträger in einem NetApp-Cluster auf einer direkt angeschlossenen Bandeinheit zu sichern, müssen Sie die Bandeinheit konfigurieren.

### Zugehörige Verweise:

REGISTER NODE (Knoten registrieren)

## Clustergesamtsicherungen mit einem IBM Spectrum Protect-Server als Ziel konfigurieren

---

Sie können IBM Spectrum Protect für die Sicherung aller Datenträger in einem NetApp-Cluster mit einem IBM Spectrum Protect-Server als Ziel konfigurieren, der die Daten in einem Speicherpool speichert. Selbst wenn Datenträger innerhalb des Clusters verschoben werden, werden Sicherungsoperationen fortgesetzt und es ist keine Rekonfiguration erforderlich.

## Vorbereitende Schritte

---

Eine Übersicht über die NDMP-Funktionalität in IBM Spectrum Protect- und NetApp-Dateiservern finden Sie in der Technote 7046965. In dieser Technote sind auch die Systemvoraussetzungen aufgelistet.

Wenn das Betriebssystem NetApp Clustered Data ONTAP 8.2 oder höher oder 9.1 oder höher auf Ihrem NetApp-Dateiserver installiert ist, verwenden Sie die folgende Prozedur. Nach der Konfiguration Ihres NetApp-Dateiservers für den gemeinsamen Einsatz mit IBM Spectrum Protect können Sie die Erweiterung NetApp Cluster Aware Backup (CAB) zum Sichern aller Datenträger in dem Cluster verwenden. Ein einzelner IBM Spectrum Protect-Knoten wird zum Eigner aller gesicherten Daten.

Wenn das Betriebssystem NetApp Clustered Data ONTAP 8.2 oder höher oder 9.1 oder höher nicht auf Ihrem NetApp-Dateiserver installiert ist, sichern Sie Daten anhand der Anweisungen in IBM Spectrum Protect für NDMP-Operationen in einer Umgebung ohne Clustering konfigurieren.

## Vorgehensweise

---

1. Stellen Sie sicher, dass IBM Spectrum Protect Extended Edition installiert und die Lizenz registriert ist. Wenn die Lizenz nicht registriert ist, geben Sie den folgenden IBM Spectrum Protect-Befehl aus:

```
register license file=tsmee.lic
```

2. Fordern Sie Clusteradministratorberechtigungen für den NetApp-Dateiserver an. Dieser Schritt ist für den Zugriff auf die Clusterkonsole erforderlich.
3. Aktivieren Sie die Verwendung von NDMP, indem Sie die Anweisungen in der Veröffentlichung *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide* ausführen. Führen Sie die folgenden Schritte aus:
  - a. Aktivieren Sie NetApp SVM, um NDMP-Sicherungsoperationen auf Clusterebene steuern zu können.
  - b. Erstellen Sie eine Sicherungsbutzer-ID für NDMP-Operationen.
  - c. Konfigurieren Sie eine Netzschnittstelle für NDMP-Steuerverbindungen auf Clusterebene.
4. Registrieren Sie den IBM Spectrum Protect-Knoten, der Eigner aller Sicherungsdaten für den Cluster werden soll. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl REGISTER NODE aus:

```
register node Knotenname Kennwort domain=NAS-Domäne type=nas
```

Dabei gibt *Knotenname* den Knotennamen, *Kennwort* das Knotenkennwort und *NAS-Domäne* die Domäne des Knotens an.

5. Bestimmen Sie die numerische IP-Adresse oder den Domänennamen für den Zugriff auf den NAS-Dateiserver. Die Schnittstelle stellt Zugriff auf den gesamten Cluster bereit. Geben Sie auf dem NAS-Dateiserver den folgenden Data ONTAP-Betriebssystembefehl aus:

```
network interface show -role cluster-mgmt
```

Die IP-Adresse in der Ausgabe ist erforderlich, wenn Sie einen Wert für den Parameter HLADDRESS in Schritt 6 angeben.

6. Definieren Sie eine Einheit zum Versetzen von Daten für den Knoten, indem Sie den Befehl DEFINE DATAMOVER unter Angabe von TYPE=NASCLUSTER ausgeben. Geben Sie auf dem IBM Spectrum Protect-Server den folgenden Befehl in einer einzigen Zeile aus:

```
define datamover Name_der_Einheit_zum_Versetzen_von_Daten type=nascluster  
hladdress=Cluster-Managementschnittstelle lladdress=Port  
USER=Benutzername password=Kennwort dataformat=netappdump
```

Dabei ist *Cluster-Managementschnittstelle* der Wert aus Schritt 5 und *Name\_der\_Einheit\_zum\_Versetzen\_von\_Daten* der in Schritt 4 registrierte Knotenname. Informationen zur Angabe der anderen Parameter finden Sie in DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren).

7. Konfigurieren Sie eine IBM Spectrum Protect-Maßnahme für die Verwaltung von NAS-Imagesicherungen. Führen Sie die Anweisungen in IBM Spectrum Protect-Maßnahme für NDMP-Operationen konfigurieren aus.
8. Aktualisieren Sie den in Schritt 4 registrierten Clusterknoten für die in Schritt 7 konfigurierte Domäne. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl UPDATE NODE aus:

```
update node Knotenname domain=Domänenname
```

9. Optional: Ermitteln Sie die Datenträger in dem Cluster und planen Sie Sicherungen für die Datenträger:
- a. Ermitteln Sie auf dem NAS-Dateiserver die Datenträger in dem Cluster, indem Sie den folgenden Data ONTAP-Befehl ausgeben:

```
volume show
```

- b. Planen Sie Sicherungsoperationen, indem Sie die Anweisungen in NDMP-Operationen planen ausführen.

## Nächste Schritte

---

Die folgenden Tasks sind optional:

- Um zu überprüfen, ob die Datenträger in dem NetApp-Cluster gesichert wurden, führen Sie die folgenden Schritte aus:
  1. Klicken Sie in der Menüleiste des Operations Center auf Clients.
  2. Klicken Sie doppelt auf einen NAS-Einheitenclient und klicken Sie auf Datenträger.
  3. Um zu bestimmen, wann die letzte Datenträgergesamtsicherung ausgeführt wurde, überprüfen Sie die Informationen in der Spalte 'Letzte Gesamtsicherung'. Um zu bestimmen, wann die letzte Differenzsicherung ausgeführt wurde, überprüfen Sie die Informationen in der Spalte 'Letzte Differenzsicherung'.
- Um Kopiespeicherpools für verbesserten Datenschutz zu konfigurieren, konfigurieren Sie die Band-zu-Band-Kopierfunktion zum Sichern von Daten. Anweisungen finden Sie in Daten mit der Band-zu-Band-Kopierfunktion sichern.

### Zugehörige Verweise:

REGISTER NODE (Knoten registrieren)

## Clusterteilsicherungen mit einem IBM Spectrum Protect-Server als Ziel konfigurieren

---

Sie können IBM Spectrum Protect für die Ausführung einer Teilsicherung eines NetApp-Clusters konfigurieren. Diese Methode ist geeignet, wenn mehrere Unternehmen Eigner von Daten in dem Cluster sind. Jedes Unternehmen kann Sicherungsoperationen für seine Daten verwalten.

## Vorbereitende Schritte

---

Eine Übersicht über die NDMP-Funktionalität in IBM Spectrum Protect- und NetApp-Dateiservern finden Sie in der Technote 7046965. In dieser Technote sind auch die Systemvoraussetzungen aufgelistet.

Wenn das Betriebssystem NetApp Clustered Data ONTAP 8.2 oder höher oder 9.1 oder höher auf Ihrem NetApp-Dateiserver installiert ist, verwenden Sie die folgende Prozedur. Nach der Konfiguration Ihres NetApp-Dateiservers für den gemeinsamen Einsatz mit IBM Spectrum Protect können Sie die Erweiterung NetApp Cluster Aware Backup (CAB) zum Sichern eines Teils eines Clusters verwenden. Wenn Sie eine Clusterteilsicherung konfigurieren, legen Sie den Bereich der Sicherung fest, indem Sie einen virtuellen Server, die NetApp Storage Virtual Machine (SVM), angeben. Die SVM stellt Zugriff auf einen Teil eines Clusters bereit.

Wenn das Betriebssystem NetApp Clustered Data ONTAP 8.2 oder höher oder 9.1 oder höher nicht auf Ihrem NetApp-Dateiserver installiert ist, sichern Sie Daten anhand der Anweisungen in IBM Spectrum Protect für NDMP-Operationen in einer Umgebung ohne Clustering konfigurieren.

## Vorgehensweise

---

1. Stellen Sie sicher, dass IBM Spectrum Protect Extended Edition installiert und die Lizenz registriert ist. Wenn die Lizenz nicht registriert ist, geben Sie den folgenden IBM Spectrum Protect-Befehl aus:

```
register license file=tsmee.lic
```

2. Fordern Sie Clusteradministratorberechtigungen für den NetApp-Dateiserver an. Dieser Schritt ist für den Zugriff auf die Clusterkonsole erforderlich.
3. Aktivieren Sie auf dem NetApp-Dateiserver die Verwendung von NDMP, indem Sie die Anweisungen in der Veröffentlichung *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide* ausführen. Führen Sie die folgenden Schritte aus:
  - a. Aktivieren Sie NetApp SVM, um NDMP-Sicherungsoperationen steuern zu können.
  - b. Erstellen Sie eine Sicherungsbenutzer-ID für NDMP-Operationen.
  - c. Konfigurieren Sie eine Netzchnittstelle für NDMP-Steuerverbindungen auf SVM-Ebene.
4. Registrieren Sie den IBM Spectrum Protect-Knoten, der Eigner der gesicherten Daten werden soll. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl REGISTER NODE aus:

```
register node Knotenname Kennwort domain=NAS-Domäne type=nas
```

Dabei gibt *Knotenname* den Knotennamen, *Kennwort* das Knotenkennwort und *NAS-Domäne* die Domäne des Knotens an.

5. Bestimmen Sie die numerische IP-Adresse oder den Domänennamen der Clusterschnittstelle, die von der SVM verwendet wird. Um den Wert zu bestimmen, geben Sie auf dem NAS-Dateiserver den folgenden ONTAP-Betriebssystembefehl aus:

```
network interface show -vserver Vserver-Name -role data
```

Dabei gibt *Vserver-Name* den Namen der SVM an. Dieser Wert ist in Schritt 6 erforderlich.

6. Definieren Sie eine zugehörige Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Knoten, indem Sie den Befehl DEFINE DATAMOVER unter Angabe von `TYPE=NASVSERVER` ausgeben. Geben Sie auf dem IBM Spectrum Protect-Server den folgenden Befehl in einer einzigen Zeile aus:

```
define datamover Name_der_Einheit_zum_Versetzen_von_Daten type=nasvserver  
laddress=SVM-Datenschnittstelle lladdress=Port  
USER=Benutzername password=Kennwort dataformat=netappdump
```

Dabei ist *SVM-Datenschnittstelle* der Wert aus Schritt 5 und *Name\_der\_Einheit\_zum\_Versetzen\_von\_Daten* der Name des in Schritt 4 registrierten Knotens.

Informationen zur Angabe der anderen Parameter finden Sie in DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren).

7. Konfigurieren Sie eine IBM Spectrum Protect-Maßnahme für die Verwaltung von NAS-Imagesicherungen. Führen Sie die Anweisungen in IBM Spectrum Protect-Maßnahme für NDMP-Operationen konfigurieren aus.
8. Aktualisieren Sie den in Schritt 4 registrierten Knoten für die in Schritt 7 konfigurierte Domäne. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl UPDATE NODE aus:

```
update node Knotenname domain=Domänename
```

9. Optional: Ermitteln Sie die Datenträger in dem Cluster und planen Sie Sicherungsoperationen. Führen Sie die folgenden Schritte aus:

- a. Ermitteln Sie auf dem NAS-Dateiserver die Datenträger in dem Cluster, indem Sie den folgenden Data ONTAP-Befehl ausgeben:

```
volume show -vserver Vserver-Name
```

Dabei gibt *Vserver-Name* den Namen der SVM an.

- b. Planen Sie Sicherungsoperationen, indem Sie die Anweisungen in NDMP-Operationen planen ausführen.

## Nächste Schritte

---

Um zu überprüfen, ob die Datenträger in dem NetApp-Cluster gesichert wurden, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Menüleiste des Operations Center auf Clients.
2. Klicken Sie doppelt auf einen NAS-Einheitenclient und klicken Sie auf Datenträger.
3. Um zu bestimmen, wann die letzte Datenträgergesamticherung ausgeführt wurde, überprüfen Sie die Informationen in der Spalte 'Letzte Gesamticherung'. Um zu bestimmen, wann die letzte Differenzicherung ausgeführt wurde, überprüfen Sie die Informationen in der Spalte 'Letzte Differenzicherung'.

### Zugehörige Verweise:

REGISTER NODE (Knoten registrieren)

# IBM Spectrum Protect für die Optimierung von Clustersicherungen rekonfigurieren

Wenn Sie IBM Spectrum Protect zum Sichern von NetApp-Clustern mithilfe von NDMP auf Knotenebene konfiguriert haben, können Sie IBM Spectrum Protect für die Verwendung von NDMP Cluster Aware Backup (CAB) rekonfigurieren. Auf diese Art und Weise können Sie Sicherungsoperationen für NetApp-Cluster optimieren.

## Vorbereitende Schritte

Eine Übersicht über die NDMP-Funktionalität in IBM Spectrum Protect- und NetApp-Dateiservern finden Sie in der Technote 7046965. In dieser Technote sind auch die Systemvoraussetzungen aufgelistet.

## Informationen zu diesem Vorgang

Wenn Sie IBM Spectrum Protect für die Verwendung von CAB rekonfigurieren, können Sie Sicherungsoperationen wie folgt optimieren:

- Sie können IBM Spectrum Protect für die Sicherung aller Datenträger in einem NetApp-Cluster auf eine direkt angeschlossene Banderinheit oder auf einen IBM Spectrum Protect-Server konfigurieren. In beiden Fällen ist ein einzelner IBM Spectrum Protect-Knoten Eigner der Daten. Selbst wenn Datenträger innerhalb des Clusters verschoben werden, werden Sicherungsoperationen fortgesetzt und es ist keine Rekonfiguration erforderlich.
- Sie können eine Teilsicherung eines NetApp-Clusters auf einen IBM Spectrum Protect-Server ausführen. Diese Methode ist geeignet, wenn mehrere Unternehmen Eigner von Daten in dem Cluster sind. Jedes Unternehmen kann Sicherungsoperationen für seine Daten verwalten. Sie legen den Bereich einer Teilsicherung fest, indem Sie eine NetApp Storage Virtual Machine (SVM) angeben, die Zugriff auf einen Teil eines Clusters bereitstellt.

Um IBM Spectrum Protect für die Verwendung von CAB zu rekonfigurieren, müssen Sie einen neuen IBM Spectrum Protect-Knoten und eine neue Einheit zum Versetzen von Daten definieren.

## Vorgehensweise

1. Stellen Sie sicher, dass NetApp Clustered Data ONTAP 8.2 oder höher oder 9.1 oder höher auf dem NetApp-Dateiserver installiert ist.
2. Aktivieren Sie die Verwendung von NDMP, indem Sie die Anweisungen in der Veröffentlichung *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide* ausführen. Führen Sie eine der folgenden Aktionen aus:

Für eine Clustergesamtsicherung

Führen Sie die folgenden Schritte aus:

- a. Aktivieren Sie auf Clusterebene NDMP-Sicherungsoperationen auf SVM-Ebene. Auf diese Art und Weise inaktivieren Sie auf dem NAS-Dateiserver NDMP-Sicherungsoperationen auf Knotenebene. Stellen Sie sicher, dass die Option `node-scoped-ndmp` auf dem NAS-Dateiserver auf OFF gesetzt ist.
- b. Erstellen Sie eine Sicherungsbutzer-ID für NDMP-Operationen.
- c. Konfigurieren Sie eine Netzchnittstelle für NDMP-Steuerverbindungen auf Clusterebene.

Für eine Clusterteilsicherung

Führen Sie die folgenden Schritte aus:

- a. Aktivieren Sie NDMP auf SVM-Ebene, um NDMP-Sicherungsoperationen steuern zu können.
- b. Erstellen Sie eine Sicherungsbutzer-ID für NDMP-Operationen.
- c. Konfigurieren Sie eine Netzchnittstelle für NDMP-Steuerverbindungen auf SVM-Ebene.

3. Registrieren Sie den IBM Spectrum Protect-Knoten, der Eigner der Sicherungsdaten werden soll. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl REGISTER NODE aus:

```
register node Knotenname Kennwort domain=NAS-Domäne type=nas
```

Dabei gibt *Knotenname* den Knotennamen, *Kennwort* das Knotenkennwort und *NAS-Domäne* die Domäne des Knotens an.

4. Wenn Sie planen, einen gesamten Cluster zu sichern, bestimmen Sie die IP-Adresse der NetApp-Cluster-Managementschnittstelle auf dem NAS-Dateiserver. Die Schnittstelle stellt Zugriff auf den gesamten Cluster bereit. Geben Sie auf dem NAS-Dateiserver den folgenden Data ONTAP-Betriebssystembefehl aus:

```
network interface show -role cluster-mgmt
```

Die IP-Adresse in der Ausgabe ist erforderlich, wenn Sie den Parameter HLADDRESS in Schritt 6 angeben.

5. Wenn Sie planen, einen Teil eines Clusters zu sichern, bestimmen Sie die numerische IP-Adresse oder den Domännennamen der Clusterschnittstelle, die von der SVM verwendet wird. Um den Wert zu bestimmen, geben Sie auf dem NAS-Dateiserver den folgenden Data ONTAP-Betriebssystembefehl aus:

```
network interface show -vserver Vserver-Name -role data
```

Dabei gibt *Vserver-Name* den Namen der SVM an. Der abgerufene Wert ist in Schritt 6 erforderlich.

6. Definieren Sie eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Knoten. Führen Sie eine der folgenden Aktionen aus:

Für eine Clustergesamtsicherung

Definieren Sie eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Knoten, der Eigner der Sicherungsdaten werden soll. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl DEFINE DATAMOVER in einer einzigen Zeile aus:

```
define datamover Name_der_Einheit_zum_Versetzen_von_Daten type=nascluster  
hladdress=Cluster-Managementschnittstelle lladdress=Port  
USER=Benutzername password=Kennwort dataformat=netappdump
```

Dabei ist *Cluster-Managementschnittstelle* der Wert aus Schritt 4 und *Name\_der\_Einheit\_zum\_Versetzen\_von\_Daten* der in Schritt 3 registrierte Knotenname.

Tipp: Nach dem Definieren der Einheit zum Versetzen von Daten werden weitere Einheiten zum Versetzen von Daten automatisch für jeden Knoten in dem Cluster definiert. Der Name der jeweiligen Einheit zum Versetzen von Daten stimmt mit dem Namen des physischen Knotens in dem Cluster überein. Diese Einheiten zum Versetzen von Daten werden beim Definieren von Pfaden zu Bandlaufwerken verwendet, die an den Cluster angeschlossen sind.

Für eine Clusterteilsicherung

Definieren Sie eine Einheit zum Versetzen von Daten für den Knoten, indem Sie den Befehl DEFINE DATAMOVER unter Angabe von *TYPE=NASVSERVER* ausgeben. Geben Sie auf dem IBM Spectrum Protect-Server den folgenden Befehl in einer einzigen Zeile aus:

```
define datamover Name_der_Einheit_zum_Versetzen_von_Daten type=nasvserver  
hladdress=SVM-Datenschnittstelle lladdress=Port  
USER=Benutzername password=Kennwort dataformat=netappdump
```

Dabei ist *SVM-Datenschnittstelle* der Wert aus Schritt 5 und *Name\_der\_Einheit\_zum\_Versetzen\_von\_Daten* der in Schritt 3 registrierte Knotenname.

Informationen zur Angabe der anderen Parameter im Befehl DEFINE DATAMOVER finden Sie in DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren).

7. Um Daten auf eine direkt angeschlossene Bandoeinheit zu sichern, ermitteln Sie für jedes Bandlaufwerk, das an den Cluster angeschlossen ist, den Einheitennamen und den physischen Knoten, an den das Laufwerk angeschlossen ist:

- a. Geben Sie auf dem NAS-Dateiserver den folgenden Data ONTAP-Befehl aus:

```
storage tape show-tape-drive
```

- b. Prüfen Sie die Ausgabe, um die Seriennummer des Bandlaufwerks und den Knoten des Clusters, an den das Laufwerk angeschlossen ist, zu finden. Dieselbe Zeilengruppe umfasst den Einheitennamen, beispielsweise *st1*, *st2* oder *st3*.

8. Um eine Clustergesamtsicherung auf eine direkt angeschlossene Bandoeinheit zu konfigurieren, führen Sie die Anweisungen in Bandoeinheiten für Clustergesamtsicherungen konfigurieren aus.
9. Um eine Clustergesamt- oder Clusterteilsicherung auf einen IBM Spectrum Protect-Server zu konfigurieren, konfigurieren Sie eine Maßnahme für die Verwaltung von NAS-Imagesicherungen. Führen Sie die Anweisungen in IBM Spectrum Protect-Maßnahme für NDMP-Operationen konfigurieren aus.
10. Inaktivieren Sie geplante Sicherungsoperationen für alle Knoten, die zuvor zum Sichern des NetApp-Clusters verwendet wurden.
11. Ermitteln Sie die Datenträger in dem Cluster und planen Sie wahlweise Sicherungsoperationen für die Datenträger. Führen Sie eine der folgenden Aktionen aus:

Für eine Clustergesamtsicherung

- a. Ermitteln Sie auf dem NAS-Dateiserver die Datenträger in dem Cluster, indem Sie den folgenden Data ONTAP-Befehl verwenden:

```
volume show
```

- b. Führen Sie eine Gesamtsicherung des gesamten Clusters aus.

- c. Optional: Um Sicherungsoperationen zu planen, führen Sie die Anweisungen in NDMP-Operationen planen aus.

Für eine Clusterteilsicherung

- a. Ermitteln Sie auf dem NAS-Dateiserver die Datenträger in dem Cluster, indem Sie den folgenden Data ONTAP-Befehl verwenden:

```
volume show -vserver Vserver-Name
```

Dabei gibt *Vserver-Name* den Namen der SVM an.

- b. Führen Sie eine Gesamtsicherung für einen Teil des Clusters aus.

- c. Optional: Um Sicherungsoperationen zu planen, führen Sie die Anweisungen in NDMP-Operationen planen aus.

## Nächste Schritte

---

Um zu überprüfen, ob die Datenträger in dem NetApp-Cluster gesichert wurden, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Menüleiste des Operations Center auf Clients.
2. Klicken Sie doppelt auf einen NAS-Einheitenclient und klicken Sie auf Datenträger.
3. Um zu bestimmen, wann die letzte Datenträgergesamticherung ausgeführt wurde, überprüfen Sie die Informationen in der Spalte 'Letzte Gesamtsicherung'. Um zu bestimmen, wann die letzte Differenzsicherung ausgeführt wurde, überprüfen Sie die Informationen in der Spalte 'Letzte Differenzsicherung'.

**Zugehörige Verweise:**

DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren)

DEFINE PATH (Pfad definieren, wenn Ziel ein Laufwerk ist)

REGISTER NODE (Knoten registrieren)

## NAS-Dateiserver mithilfe von NDMP sichern und zurückschreiben

---

Nach der Konfiguration von IBM Spectrum Protect für NDMP-Operationen können Sie mit der Verwendung von NDMP beginnen.

### Vorgehensweise

---

Verwenden Sie entweder eine Clientschnittstelle oder eine Verwaltungsschnittstelle, um eine Dateisystemimagesicherung auszuführen. Um beispielsweise die Schnittstelle des Windows-Clients für Sichern/Archivieren zu verwenden, um ein Dateisystem mit dem Namen /vol/vol1 auf einem NAS-Dateiserver mit dem Namen NAS1 zu verwenden, geben Sie den folgenden Befehl aus:

```
dsmc backup nas -nasnodename=nas1 {/vol/vol1}
```

Weitere Informationen zu dem Befehl finden Sie in Sicherungsimage.

Tipp: Jedes Mal, wenn Sie die Clientschnittstelle verwenden, werden Sie aufgefordert, sich als IBM Spectrum Protect-Administrator zu authentifizieren, bevor die Operation beginnen kann. Die Administrator-ID muss mindestens über Clienteignerberechtigung für den NAS-Knoten verfügen.

Sie können dieselbe Sicherungsoperation auch mit einer Serverschnittstelle ausführen. Sichern Sie beispielsweise über den Verwaltungsbefehlszeilenclient das Dateisystem mit dem Namen /vol/vol1 auf einem NAS-Dateiserver mit dem Namen NAS1, indem Sie den folgenden Befehl ausgeben:

```
backup node nas1 /vol/vol1
```

Einschränkung: Die Befehle BACKUP NAS und BACKUP NODE schließen keine Momentaufnahmen ein. Informationen zum Sichern von Momentaufnahmen finden Sie in Mit Momentaufnahmen sichern und zurückschreiben.

Sie können das Image mit jeder der beiden Schnittstellen zurückschreiben. Sicherungen sind, unabhängig davon, ob sie mit einer Clientschnittstelle oder einer Serverschnittstelle gesichert werden, identisch. Angenommen, das in den vorherigen Beispielen gesicherte Image soll zurückgeschrieben werden. In diesem Beispiel wird das Dateisystem mit dem Namen /vol/vol1 in /vol/vol2 zurückgeschrieben. Schreiben Sie das Dateisystem mit dem folgenden Befehl, der von einer Schnittstelle des Windows-Clients für Sichern/Archivieren ausgegeben wird, zurück:

```
dsmc restore nas -nasnodename=nas1 {/vol/vol1} {/vol/vol2}
```

Sie können das Dateisystem wahlweise mithilfe einer Serverschnittstelle zurückschreiben. Um beispielsweise das Dateisystem mit dem Namen /vol/vol1 in das Dateisystem /vol/vol2 für einen NAS-Dateiserver mit dem Namen NAS1 zurückzuschreiben, geben Sie den folgenden Befehl ein:

```
restore node nas1 /vol/vol1 /vol/vol2
```

Sie können Daten von einem NAS-Anbietersystem auf ein anderes NAS-Anbietersystem zurückschreiben, wenn Sie das NDMPDUMP-Datenformat verwenden. Sie müssen jedoch entweder die Kompatibilität zwischen den Systemen überprüfen oder einen separaten Speicherpool für jeden NAS-Anbieter verwalten.

- NAS-Dateiserver: Sicherungen auf einem einzelnen IBM Spectrum Protect-Server  
Wenn mehrere NAS-Dateiserver an verschiedenen Standorten vorhanden sind, möchten Sie die Sicherungsdaten möglicherweise eher an einen einzelnen IBM Spectrum Protect-Server senden, anstatt ein Bandarchiv an jede NAS-Einheit anzuschließen.
- NDMP-Dateiserver auf einem IBM Spectrum Protect-Server sichern  
Sie können Daten auf einem einzelnen IBM Spectrum Protect-Server sichern, anstatt ein Bandarchiv an jede NAS-Einheit anzuschließen.

## NAS-Dateiserver: Sicherungen auf einem einzelnen IBM Spectrum Protect-Server

---



Wenn mehrere NAS-Dateiserver an verschiedenen Standorten vorhanden sind, möchten Sie die Sicherungsdaten möglicherweise eher an einen einzelnen IBM Spectrum Protect-Server senden, anstatt ein Bandarchiv an jede NAS-Einheit anzuschließen.

Wenn Sie NAS-Sicherungsdaten in der Speicherhierarchie des IBM Spectrum Protect-Servers speichern, können Sie IBM Spectrum Protect-Back-End-Datenverwaltungsfunktionen anwenden. Auf diese Art und Weise können Sie die Vorteile der Umlagerung, Konsolidierung, Wiederherstellung nach einem Katastrophenfall und anderer Funktionen nutzen.

Um eine NAS-Einheit in einem nativen IBM Spectrum Protect-Speicherpool zu sichern, definieren Sie den Zielspeicherpool in der Kopiergruppe so, dass er auf den gewünschten nativen Speicherpool verweist. Der Zielspeicherpool stellt die Informationen zu dem Speicherarchiv und den Laufwerken zur Verfügung, die für die Sicherung und Zurückschreibung verwendet werden. Sie müssen sicherstellen, dass genügend Speicherbereich in Ihrem Zielspeicherpool verfügbar ist, um die NAS-Daten zu speichern, die auf sequenziellen Einheiten, Platten- oder Dateieinheiten gesichert werden können. Das Definieren einer separaten Einheitenklasse ist nicht erforderlich.

Wenn Sie ein Inhaltsverzeichnis erstellen, muss eine Verwaltungsklasse mit dem Parameter TOCDESTINATION in den Befehlen DEFINE und UPDATE COPYGROUP angegeben werden. Wenn Sie einen NAS-Dateiserver in nativen IBM Spectrum Protect-Pools sichern, kann TOCDESTINATION mit dem Ziel der Daten, die unter Verwendung von NDMP gesichert werden, identisch sein.

Firewallaspekte sind strikter als bei der Übertragung zwischen Dateiserver und angeschlossenem Speicherarchiv, da die Übertragung entweder vom IBM Spectrum Protect-Server oder vom NAS-Dateiserver eingeleitet werden kann. NDMP-Bandserver werden als Threads innerhalb des IBM Spectrum Protect-Servers ausgeführt und der Bandserver akzeptiert Verbindungen an Port 10001. Diese Portnummer kann mit der folgenden Option in der IBM Spectrum Protect-Serveroptionsdatei geändert werden: NDMPPORTRANGE untere\_Portnummer, obere\_Portnummer.

Während NDMP-Sicherungsoperationen vom Dateiserver auf den Server können Sie mit der Option NDMPREFDATAINTERFACE angeben, welche Netzchnittstelle der IBM Spectrum Protect-Server verwendet, um Sicherungsdaten zu empfangen. Der Wert für diese Option ist ein Hostname oder eine IPv4-Adresse, die einer der aktiven Netzchnittstellen des Systems zugeordnet ist, auf dem der IBM Spectrum Protect-Server ausgeführt wird. Diese Schnittstelle muss IPv4-fähig sein.

Bevor Sie diese Option verwenden, überprüfen Sie, ob Ihre NAS-Einheit NDMP-Operationen unterstützt, die eine andere Netzchnittstelle für NDMP-Steuer- und NDMP-Datenverbindungen verwenden. NDMP-Steuerverbindungen werden von IBM Spectrum Protect zur Authentifizierung mit einem NDMP-Server und zur Überwachung einer NDMP-Operation verwendet, wohingegen NDMP-Datenverbindungen für die Übertragung und den Empfang von Sicherungsdaten während NDMP-Operationen verwendet werden. Sie müssen dennoch Ihre NAS-Einheit konfigurieren, damit Sicherungs- und Zurückschreibungsdaten an die entsprechende Netzchnittstelle weitergeleitet werden.

Wenn die Option NDMPREFDATAINTERFACE aktiviert ist, wirkt sie sich auf alle nachfolgenden NDMP-Operationen zwischen Dateiserver und Server aus. Sie hat aber keine Auswirkungen auf NDMP-Steuerverbindungen, da diese die Standardnetzchnittstelle des Systems verwenden. Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server stoppen und erneut starten zu müssen.

NetApp-Dateiserver stellen eine NDMP-Option (ndmpd.preferred\_interface) zur Verfügung, um die für NDMP-Datenverbindungen verwendete Schnittstelle zu ändern. Weitere Informationen enthält die Dokumentation zu Ihrer NAS-Einheit.

Anweisungen zur Ausführung von NDMP-Sicherungsoperationen vom Dateiserver auf den Server finden Sie in NDMP-Dateiserver auf einem IBM Spectrum Protect-Server sichern.

Informationen zu Serveroptionen finden Sie in Serveroptionen.

## NDMP-Dateiserver auf einem IBM Spectrum Protect-Server sichern

---

Sie können Daten auf einem einzelnen IBM Spectrum Protect-Server sichern, anstatt ein Bandarchiv an jede NAS-Einheit anzuschließen.

### Vorgehensweise

---

Um einen Server in einem NAS-Dateisystem zu sichern, führen Sie die folgenden Schritte aus:

1. Wählen Sie einen vorhandenen Speicherpool aus oder konfigurieren Sie einen Speicherpool für NAS-Daten, indem Sie den folgenden Befehl ausgeben:

```
define stgpool naspool disk
```

2. Definieren Sie Datenträger, die dem Speicherpool hinzugefügt werden sollen. Definieren Sie beispielsweise einen Datenträger mit dem Namen naspool\_volAB:

```
define volume naspool /usr/storage/naspool_volAB formatsize=100
```

3. Setzen Sie das Kopienziel auf den zuvor definierten Speicherpool und aktivieren Sie die zugehörige Maßnahmengruppe.

```
update copygroup standard standard standard destination=naspool
  tocdestination=naspool
activate policyset standard standard
```

Das Ziel für NAS-Daten wird durch das Ziel in der Kopiergruppe bestimmt. Bei der Schätzung der Speichergröße für NAS-Differenzsicherungen wird die Belegung des Dateibereichs verwendet - derselbe Wert, der für eine Gesamtsicherung verwendet wird. Sie können diese Größenschätzung als einen der Aspekte bei der Auswahl eines Speicherpools verwenden. Eines der Attribute eines Speicherpools ist der Wert für MAXSIZE, mit dem angegeben wird, dass Daten an den nächsten Speicherpool gesendet werden, wenn der Wert für MAXSIZE durch die geschätzte Größe überschritten wird. Da NAS-Differenzsicherungen in native IBM Spectrum Protect-Speicherpools die Belegungsgröße des Basisdateibereichs als geschätzte Speichergröße verwenden, werden Differenzsicherungen in demselben Speicherpool wie die Gesamtsicherung gespeichert. Abhängig von den Kollokationseinstellungen können Differenzsicherungen auf denselben Datenträgern wie die Gesamtsicherung gespeichert werden.

4. Definieren Sie einen Knoten und eine Einheit zum Versetzen von Daten für die NAS-Einheit. Das Datenformat gibt an, dass die von dieser NAS-Einheit erstellten Sicherungsbilder ein Dump-Typ des Sicherungsbildes in einem NetApp-spezifischen Format sind.

```
register node nas1 nas1 type=nas domain=standard
define datamover nas1 type=nas hla=nas1 user=root
password=***** dataformat=netappdump
```

Die NAS-Einheit kann jetzt in einem IBM Spectrum Protect-Serverspeicherpool gesichert werden. Pfade zu lokalen Laufwerken können definiert werden, das von der Verwaltungsklasse angegebene Ziel bestimmt jedoch die Zielposition für diese Sicherungsoperation.

5. Sichern Sie die NAS-Einheit in den IBM Spectrum Protect-Speicherpool, indem Sie den folgenden Befehl ausgeben:

```
backup node nas1 /vol/vol0
```

6. Schreiben Sie eine NAS-Einheit aus dem IBM Spectrum Protect-Speicherpool zurück, indem Sie den folgenden Befehl ausgeben:

```
restore node nas1 /vol/vol0
```

## Sicherung und Zurückschreibung auf Dateiebene für NDMP-Operationen

Wenn Sie Daten mit NDMP sichern, können Sie angeben, dass der IBM Spectrum Protect-Server Informationen auf Dateiebene erfasst und in einem Inhaltsverzeichnis (TOC) speichert.

Wenn Sie diese Option während der Sicherung angeben, können Sie später das Inhaltsverzeichnis (TOC) des Sicherungsbildes anzeigen. Mithilfe des Web-Clients für Sichern/Archivieren können Sie einzelne Dateien oder Verzeichnisse auswählen, um diese direkt aus den generierten Sicherungsbildern zurückzuschreiben.

Die Erfassung von Informationen auf Dateiebene erfordert zusätzliche Verarbeitungszeit, Netzressourcen, Speicherpoolbereich, temporären Datenbankbereich und möglicherweise zusätzliche Speichereinheiteninteraktion. Anweisungen zum Konfigurieren von Speichereinheiten finden Sie in Speichereinheiten konfigurieren. Gegebenenfalls müssen Sie der IBM Spectrum Protect-Serverdatenbank mehr Speicherbereich zuordnen. Sie müssen die Maßnahme so konfigurieren, dass der IBM Spectrum Protect-Server das Inhaltsverzeichnis (TOC) in einem anderen Speicherpool als das Sicherungsbild speichert. Das Inhaltsverzeichnis (TOC) wird wie jedes andere Objekt in diesem Speicherpool behandelt.

Sie können auch eine Sicherung mit NDMP ausführen, ohne Zurückschreibungsinformationen auf Dateiebene zu erfassen.

Um die Erstellung eines Inhaltsverzeichnisses (TOC) für eine Sicherung mit NDMP zu ermöglichen, müssen Sie das Attribut TOCDESTINATION in der Sicherungskopiergruppe für die Verwaltungsklasse definieren, an die dieses Sicherungsbild gebunden ist. Sie können keinen Kopierspeicherpool oder Pool für aktive Daten als Ziel angeben. Der von Ihnen angegebene Speicherpool für das Ziel des Inhaltsverzeichnisses (TOCDESTINATION) muss das Datenformat NATIVE oder NONBLOCK haben und darf daher nicht der für das Sicherungsbild verwendete Bandspeicherpool sein.

Wenn Informationen auf Dateiebene erfasst werden sollen, geben Sie den Parameter TOC im Serverbefehl BACKUP NODE an. Wenn Sie Ihre Sicherung mithilfe des Clients einleiten, können Sie die Option TOC in der Clientoptionsdatei, in der Clientoptionsgruppe oder in der Clientbefehlszeile angeben. Sie können NO, PREFERRED oder YES angeben. Wenn Sie PREFERRED oder YES angeben, speichert der IBM Spectrum Protect-Server Dateiinformationen für eine einzelne NDMP-gesteuerte Sicherung in einem Inhaltsverzeichnis (TOC). Das Inhaltsverzeichnis (TOC) wird in einen Speicherpool gestellt. Danach kann der IBM Spectrum Protect-Server auf das Inhaltsverzeichnis (TOC) zugreifen, sodass Datei- und Verzeichnisinformationen vom Server oder Client abgefragt werden können. Die Verwendung des Parameters TOC ermöglicht es, ein Inhaltsverzeichnis (TOC) für einige Images zu generieren und für andere nicht, ohne dass verschiedene Verwaltungsklassen für die Images erforderlich sind.

Weitere Informationen zum Befehl BACKUP NODE finden Sie in BACKUP NODE (NAS-Knoten sichern).

Verwenden Sie Speicherpools mit wahlfreiem Zugriff (Einheitenklasse DISK) als Ziel für das Inhaltsverzeichnis (TOC), um Mountverzögerungen zu vermeiden und ausreichenden Speicherbereich zu gewährleisten. Bei Speicherpools mit sequenziellem Zugriff ist keine Kennzeichnung oder andere Datenträgervorbereitung erforderlich, wenn Arbeitsdatenträger zulässig sind.

Weitere Informationen finden Sie in Inhaltsverzeichnisse verwalten.

- Schnittstellen für Zurückschreibungsoperationen auf Dateiebene  
Wenn Sie einzelne Dateien und Verzeichnisse zurückschreiben, haben Sie die Möglichkeit, eine von zwei Schnittstellen zu verwenden, um die Zurückschreibung einzuleiten: den Web-Client für Sichern/Archivieren oder die Serverschnittstelle.
- Zeichen des internationalen Zeichensatzes für NetApp-Dateiserver  
Alle Systeme, die Daten auf einem bestimmten Datenträger des NAS-Dateiservers erstellen oder auf diese zugreifen, müssen dafür eine Methode verwenden, die mit der Spracheinstellung des Datenträgers kompatibel ist.
- Zurückschreibungsoperationen auf Dateiebene aus einem Sicherungsimagen auf Verzeichnisebene  
Zurückschreibungsoperationen auf Dateiebene werden für Sicherungsimagen auf Verzeichnisebene unterstützt.

## Schnittstellen für Zurückschreibungsoperationen auf Dateiebene

---

Wenn Sie einzelne Dateien und Verzeichnisse zurückschreiben, haben Sie die Möglichkeit, eine von zwei Schnittstellen zu verwenden, um die Zurückschreibung einzuleiten: den Web-Client für Sichern/Archivieren oder die Serverschnittstelle.

Zurückschreibungsoperationen mithilfe des Web-Clients für Sichern/Archivieren

Für den Web-Client für Sichern/Archivieren muss ein Inhaltsverzeichnis (TOC) vorhanden sein, um Dateien und Verzeichnisse zurückschreiben zu können. Der Web-Client muss sich auf einem Windows-System befinden. Der IBM Spectrum Protect-Server greift auf das Inhaltsverzeichnis (TOC) im Speicherpool zu und lädt TOC-Informationen in eine temporäre Datenbanktabelle. Dann können Sie mithilfe des Web-Clients für Sichern/Archivieren Verzeichnisse und Dateien in einem oder mehreren Dateisystemimages überprüfen und einzelne Dateien oder Verzeichnisse zum direkten Zurückschreiben aus den generierten Sicherungsimagen auswählen.

Zurückschreibungsoperationen mithilfe der Serverschnittstelle

- Wenn ein Inhaltsverzeichnis (TOC) vorhanden ist, verwenden Sie den Befehl `QUERY NASBACKUP`, um Informationen zu den von NDMP generierten Sicherungsimagen aufzurufen und anzuzeigen, welche Images über ein entsprechendes Inhaltsverzeichnis (TOC) verfügen. Verwenden Sie dann den Befehl `RESTORE NODE` mit dem Parameter `FILELIST`.
- Wenn kein Inhaltsverzeichnis (TOC) erstellt wurde, kann der Inhalt des Sicherungsimagen nicht angezeigt werden. Sie können einzelne Dateien und/oder Verzeichnisse zurückschreiben, wenn Sie den Namen der Datei bzw. des Verzeichnisses kennen, und wenn Sie wissen, in welchem Image sich die Sicherung befindet. Verwenden Sie den Befehl `RESTORE NODE` mit dem Parameter `FILELIST`.

## Zeichen des internationalen Zeichensatzes für NetApp-Dateiserver

---

Alle Systeme, die Daten auf einem bestimmten Datenträger des NAS-Dateiservers erstellen oder auf diese zugreifen, müssen dafür eine Methode verwenden, die mit der Spracheinstellung des Datenträgers kompatibel ist.

Sie müssen Data ONTAP 6.4.1 oder höher (falls verfügbar) auf Ihrem NetApp-NAS-Dateiserver installieren, um vollständige Unterstützung für Zeichen des internationalen Zeichensatzes in Datei- und Verzeichnisnamen zu erhalten.

Wenn Ihre Version von Data ONTAP älter als 6.4.1 ist, benötigen Sie eine der beiden folgenden Konfigurationen, um Informationen auf Dateiebene erfassen und zurückschreiben zu können. Bei anderen Konfigurationen als den beiden aufgeführten sind die Ergebnisse unvorhersehbar. Der IBM Spectrum Protect-Server gibt eine Warnung (ANR4946W) während Sicherungsoperationen aus. Die Nachricht gibt an, dass die Zeichencodierung der NDMP-Dateiprotokollnachrichten unbekannt ist und UTF-8 angenommen wird, um ein Inhaltsverzeichnis zu erstellen. Diese Nachricht kann nur in den beiden folgenden Konfigurationen ohne Bedenken ignoriert werden.

- Ihre Daten enthalten Verzeichnis- und Dateinamen, die nur aus Zeichen des englischen Zeichensatzes (7-Bit ASCII) bestehen.
- Ihre Daten enthalten Verzeichnis- und Dateinamen, die aus Zeichen bestehen, die nicht zum englischen Zeichensatz gehören, und als Datenträgersprache ist die UTF-8-Version der entsprechenden Ländereinstellung definiert (beispielsweise `de.UTF-8` für Deutsch).

Wenn Ihre Version von Data ONTAP 6.4.1 oder höher ist, benötigen Sie eine der drei folgenden Konfigurationen, um Informationen auf Dateiebene erfassen und zurückschreiben zu können. Bei anderen Konfigurationen als den drei aufgeführten sind die Ergebnisse unvorhersehbar.

- Ihre Daten enthalten Verzeichnis- und Dateinamen, die nur aus Zeichen des englischen Zeichensatzes (7-Bit ASCII) bestehen, und die Datenträgersprache ist entweder nicht definiert oder mit einem der folgenden Werte definiert:
  - `C (POSIX)`
  - `en`
  - `en_US`
  - `en.UTF-8`
  - `en_US.UTF-8`
- Ihre Daten enthalten Verzeichnis- und Dateinamen, die aus Zeichen bestehen, die nicht zum englischen Zeichensatz gehören, und als Datenträgersprache ist die entsprechende Ländereinstellung definiert (beispielsweise `de.UTF-8` oder `de` für Deutsch).

Tipp: Die Verwendung der UTF-8-Version der Spracheinstellung des Datenträgers ist in Bezug auf die IBM Spectrum Protect-Serververarbeitung und den Speicherbereich des Inhaltsverzeichnisses effizienter.

- Sie verwenden CIFS nur, um Ihre Daten zu erstellen und auf sie zuzugreifen.

## Zurückschreibungsoperationen auf Dateiebene aus einem Sicherungsbild auf Verzeichnisebene

---

Zurückschreibungsoperationen auf Dateiebene werden für Sicherungsbilder auf Verzeichnisebene unterstützt.

Wie bei einer NAS-Dateisystemsicherung wird während einer Sicherung auf Verzeichnisebene ein Inhaltsverzeichnis erstellt und Sie können die Dateien in dem Image mit dem Web-Client durchsuchen. Standardmäßig werden die Dateien an die ursprüngliche Position zurückschrieben. Während einer Zurückschreibung auf Dateiebene aus einer Sicherung auf Verzeichnisebene können Sie jedoch entweder ein anderes Dateisystem oder einen anderen virtuellen Dateibereichsnamen als Ziel auswählen.

Für ein Inhaltsverzeichnis (TOC) eines Sicherungsbildes auf Verzeichnisebene beziehen sich die Pfadnamen für alle Dateien auf das Verzeichnis, das in der Definition des virtuellen Dateibereichs angegeben wurde, und nicht auf das Stammverzeichnis des Dateisystems.

## Sicherungs- und Zurückschreibungsoperationen auf Verzeichnisebene

---

Wenn Sie über ein großes NAS-Dateisystem verfügen, werden durch das Einleiten einer Sicherung auf Verzeichnisebene Sicherungs- und Zurückschreibungszeiten reduziert und größere Flexibilität beim Konfigurieren von NAS-Sicherungen bereitgestellt. Durch das Definieren virtueller Dateibereiche kann eine Dateisystemsicherung auf mehrere NDMP-Sicherungsoperationen und auf mehrere Bandlaufwerke verteilt werden. Sie können auch verschiedene Sicherungszeitpläne verwenden, um Unterverzeichnisstrukturen eines Dateisystems zu sichern.

Der Name des virtuellen Dateibereichs darf nicht mit einem Dateisystem auf dem NAS-Knoten übereinstimmen. Wird auf der NAS-Einheit ein Dateisystem erstellt, das denselben Namen wie ein virtuelles Dateisystem hat, tritt eine Namensunverträglichkeit auf dem IBM Spectrum Protect-Server auf, wenn der neue Dateibereich gesichert wird. Anweisungen zur Ausgabe von Befehlen zur Zuordnung virtueller Dateibereiche finden Sie in DEFINE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs definieren).  
Einschränkung: Zuordnungen virtueller Dateibereiche werden nur für NAS-Knoten unterstützt.

- Sicherung und Zurückschreibung auf Verzeichnisebene für NDMP-Operationen  
Mit dem Befehl DEFINE VIRTUALFSMAPPING wird ein Verzeichnispfad eines NAS-Dateiservers dem Namen eines virtuellen Dateibereichs auf dem IBM Spectrum Protect-Server zugeordnet. Nachdem eine Zuordnung definiert wurde, können Sie NAS-Operationen, wie beispielsweise BACKUP NODE und RESTORE NODE, unter Verwendung der Namen der virtuellen Dateibereiche so ausführen, als würde es sich um tatsächliche NAS-Dateibereiche handeln.
- Mit Momentaufnahmen sichern und zurückschreiben  
NDMP-Sicherungsoperationen auf Verzeichnisebene ermöglichen es Ihnen, benutzererstellte Momentaufnahmen eines NAS-Dateisystems zu sichern. Diese Momentaufnahmen werden dann als Unterverzeichnisse gespeichert. Die Momentaufnahmen können zu beliebiger Zeit erstellt werden, und die Sicherung auf Band kann bis zu einem geeigneten Zeitpunkt verzögert werden.

## Sicherung und Zurückschreibung auf Verzeichnisebene für NDMP-Operationen

---

Mit dem Befehl DEFINE VIRTUALFSMAPPING wird ein Verzeichnispfad eines NAS-Dateiservers dem Namen eines virtuellen Dateibereichs auf dem IBM Spectrum Protect-Server zugeordnet. Nachdem eine Zuordnung definiert wurde, können Sie NAS-Operationen, wie beispielsweise BACKUP NODE und RESTORE NODE, unter Verwendung der Namen der virtuellen Dateibereiche so ausführen, als würde es sich um tatsächliche NAS-Dateibereiche handeln.

Um eine Sicherung des Verzeichnisses zu starten, geben Sie den Befehl BACKUP NODE mit dem Namen des virtuellen Dateibereichs anstelle eines Dateibereichsnamens aus. Um die Unterverzeichnisstruktur des Verzeichnisses an die ursprüngliche Position zurückzuschreiben, führen Sie den Befehl RESTORE NODE aus und geben Sie den Namen des virtuellen Dateibereichs an.

Definitionen für den virtuellen Dateibereich können ebenfalls als Ziel in einem Befehl RESTORE NODE angegeben werden. Auf diese Art und Weise können Sie Sicherungsbilder (Dateisystem oder Verzeichnis) in ein Verzeichnis in einem beliebigen Dateisystem der NAS-Einheit zurückschreiben.

Mit dem Web-Client können Sie Dateien für die Zurückschreibung aus einem Sicherungsbild auf Verzeichnisebene auswählen, da der IBM Spectrum Protect-Client die Namen der virtuellen Dateibereiche als NAS-Dateibereiche behandelt.

## Mit Momentaufnahmen sichern und zurückschreiben

---

NDMP-Sicherungsoperationen auf Verzeichnisebene ermöglichen es Ihnen, benutzererstellte Momentaufnahmen eines NAS-Dateisystems zu sichern. Diese Momentaufnahmen werden dann als Unterverzeichnisse gespeichert. Die Momentaufnahmen können zu beliebiger Zeit erstellt werden, und die Sicherung auf Band kann bis zu einem geeigneten Zeitpunkt verzögert werden.

## Vorgehensweise

---

Um beispielsweise eine Momentaufnahme, die für ein NetApp-Dateisystem erstellt wird, zu sichern, führen Sie die folgenden Schritte aus:

1. Geben Sie an der Konsole für die NAS-Einheit den Befehl zum Erstellen der Momentaufnahme aus. SNAP CREATE lautet der Befehl für eine NetApp-Einheit.

```
snap create vol2 february17
```

In diesem Beispiel wird eine Momentaufnahme mit dem Namen FEBRUARY 17 des Dateisystems /vol/vol2 erstellt. Die physische Position für die Momentaufnahmedaten befindet sich in dem Verzeichnis /vol/vol2/.snapshot/february17. Die Speicherposition für die Momentaufnahmedaten ist von der Implementierung durch den NAS-Anbieter abhängig. Für NetApp kann der Befehl SNAP LIST verwendet werden, um alle Momentaufnahmen für ein Dateisystem anzuzeigen.

2. Erstellen Sie eine Definition für die Zuordnung eines virtuellen Dateibereichs auf dem IBM Spectrum Protect-Server für die im vorherigen Schritt erstellten Momentaufnahmedaten.

```
define virtualfsmapping nas1 /feb17snapshot /vol/vol2 /.snapshot/february17
```

In diesem Beispiel wird die Definition /feb17snapshot für die Zuordnung eines virtuellen Dateibereichs erstellt.

3. Sichern Sie die Zuordnung des virtuellen Dateibereichs.

```
backup node nas1 /feb17snapshot mode=full toc=yes
```

4. Nachdem die Sicherung erstellt wurde, können Sie entweder das gesamte Momentaufnahmeimage oder eine einzelne Datei zurückschreiben. Vor dem Zurückschreiben der Daten können Sie einen Namen für die Zuordnung des virtuellen Dateibereichs für das Zielverzeichnis erstellen. Sie können einen beliebigen Dateisystemnamen als Ziel auswählen. Die Zielposition in diesem Beispiel ist das Verzeichnis /feb17snaprestore im Dateisystem /vol/vol1.

```
define virtualfsmapping nas1 /feb17snaprestore /vol/vol1 /feb17snaprestore
```

5. Schreiben Sie das Momentaufnahmesicherungsimage zurück.

```
restore node nas1 /feb17snapshot /feb17snaprestore
```

In diesem Beispiel wird eine Kopie des Dateisystems /vol/vol2 in das Verzeichnis /vol/vol1/feb17snaprestore in demselben Zustand wie bei der Erstellung der Momentaufnahme im ersten Schritt zurückgeschrieben.

## Sicherungs- und Zurückschreibungsoperationen mit der NetApp-Funktion 'SnapMirror to Tape'

---

Sie können große NetApp-Dateisysteme mithilfe der NetApp-Funktion 'SnapMirror to Tape' (die auch als 'SMTape' bekannt ist) sichern. Durch die Verwendung einer Datenkopie auf Blockebene für die Sicherung ist die Methode 'SnapMirror to Tape' schneller als eine traditionelle NDMP-Gesamtsicherung und kann verwendet werden, wenn NDMP-Gesamtsicherungen nicht geeignet sind.

Verwenden Sie die NDMP-Funktion 'SnapMirror to Tape' als Option zur Wiederherstellung nach einem Katastrophenfall für das Kopieren großer NetApp-Dateisysteme in Zusatzspeicher. Verwenden Sie für die meisten NetApp-Dateisysteme die standardmäßige NDMP-Gesamt- oder Differenzsicherungsmethode.

Die Angabe eines Parameters in den Befehlen BACKUP NODE und RESTORE NODE ermöglicht Ihnen das Sichern und Zurückschreiben von Dateisystemen mithilfe der Funktion 'SnapMirror to Tape'. In Bezug auf die Verwendungsmöglichkeiten von SnapMirror-Images gibt es verschiedene Einschränkungen. Beachten Sie die folgenden Richtlinien, bevor Sie die Funktion als Sicherungsmethode verwenden:

- Wenn NetApp ONTAP 8.2 oder höher installiert wurde, müssen Sie eine Einheit des Typs NASCLUSTER oder NASVSERVER zum Versetzen von Daten für 'SnapMirror to Tape'-Operationen definieren.
- Eine Sicherungs- oder Zurückschreibungsoperation mit 'SnapMirror to Tape' kann nicht vom IBM Spectrum Protect Operations Center, Web-Client oder Befehlszeilenclient eingeleitet werden.
- Differenzsicherungen von SnapMirror-Images können nicht ausgeführt werden.
- Eine Sicherung auf Verzeichnisebene mithilfe der Funktion 'SnapMirror to Tape' kann nicht ausgeführt werden. Demzufolge erlaubt IBM Spectrum Protect keine Sicherungsoperationen mit 'SnapMirror to Tape' für einen virtuellen Serverdateibereich.
- Eine NDMP-Zurückschreibungsoperation auf Dateiebene aus 'SnapMirror to Tape'-Images kann nicht ausgeführt werden. Daher wird bei Imagesicherungen mit 'SnapMirror to Tape' nie ein Inhaltsverzeichnis erstellt.
- Zu Beginn einer Kopieroperation mit 'SnapMirror to Tape' generiert der Dateiserver eine Momentaufnahme des Dateisystems. NetApp stellt eine NDMP-Umgebungsvariable zur Verfügung, um zu steuern, ob diese Momentaufnahme am Ende der 'SnapMirror

to Tape'-Operation entfernt wird. Diese Variable wird von IBM Spectrum Protect immer so gesetzt, dass die Momentaufnahme entfernt wird.

- Nachdem ein 'SnapMirror to Tape'-Image abgerufen und in ein NetApp-Dateisystem kopiert wurde, bleibt das Zieldateisystem als SnapMirror-Partner konfiguriert. NetApp stellt eine NDMP-Umgebungsvariable zur Verfügung, um zu steuern, ob diese SnapMirror-Beziehung abgebrochen werden soll. IBM Spectrum Protect bricht immer die SnapMirror-Beziehung während des Abrufs ab. Nach Abschluss der Zurückschreibungsoperation befindet sich das Zieldateisystem in demselben Status wie das ursprüngliche Dateisystem zum Zeitpunkt der Sicherung.

Weitere Informationen zur Funktion 'SnapMirror to Tape' finden Sie in BACKUP NODE (NAS-Knoten sichern) und RESTORE NODE (NAS-Knoten zurückschreiben).

## NDMP-Sicherungsoperationen mithilfe von in Celerra-Dateiserver integrierten Prüfpunkten

---

Wenn der IBM Spectrum Protect-Server eine NDMP-Sicherungsoperation auf einer Celerra-Einheit zum Versetzen von Daten einleitet, kann die Sicherung eines umfangreichen Dateisystems mehrere Stunden dauern. Ohne integrierte Celerra-Prüfpunkte werden alle auf dem Dateisystem vorgenommenen Änderungen in das Sicherungsimago geschrieben.

Demzufolge enthält das Sicherungsimago Änderungen, die während der gesamten Sicherungsoperation an dem Dateisystem vorgenommen wurden. Das Sicherungsimago ist kein echtes Zeitpunktimago des Dateisystems.

Wenn Sie NDMP-Sicherungsoperationen für Celerra-Dateiserver ausführen, führen Sie ein Upgrade für das Betriebssystem auf Ihrer Einheit zum Versetzen von Daten auf Celerra-Dateiserver Version T5.5.25.1 oder höher durch. Diese Betriebssystemversion ermöglicht die Aktivierung der integrierten Prüfpunkte für alle NDMP-Sicherungsoperationen von der Celerra-Steuerworkstation aus. Durch die Aktivierung dieses Features stellen Sie sicher, dass die Sicherungsdaten echte Zeitpunktimagos des Dateisystems darstellen, das gesichert wird.

Anweisungen zum Aktivieren von integrierten Prüfpunkten während aller NDMP-Sicherungsoperationen enthält die Dokumentation zum Celerra-Dateiserver.

Wenn das Betriebssystem auf Ihrem Celerra-Dateiserver eine frühere Version als T5.5.25.1 hat und Sie NDMP zum Sichern von Celerra-Einheiten zum Versetzen von Daten verwenden, generieren Sie manuell eine Momentaufnahme des Dateisystems mithilfe der Celerra-Befehlszeilenfunktion für Prüfpunkte. Leiten Sie anschließend eine NDMP-Sicherungsoperation für das Prüfpunktdateisystem anstelle einer NDMP-Sicherungsoperation für das ursprüngliche Dateisystem ein.

Anweisungen zum Erstellen und Planen von Prüfpunkten von der Celerra-Steuerworkstation enthält die Dokumentation zum Celerra-Dateiserver.

## NAS-Knoten replizieren

---

Sie können einen NAS-Knoten, der NDMP für Sicherungsoperationen verwendet, replizieren. Machen Sie sich, bevor Sie die Replikationsoperation konfigurieren, mit den geltenden Einschränkungen vertraut.

### Informationen zu diesem Vorgang

---

Einschränkungen:

- Die Sicherungsdaten müssen sich in einem Speicherpool mit dem Datenformat NATIVE befinden. Sicherungsdaten in Speicherpools mit den folgenden Datenformaten können nicht repliziert werden:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP
- Eine Differenzsicherung kann nur repliziert werden, wenn die zugehörige Gesamtsicherung repliziert wurde.

### Vorgehensweise

---

1. Aktivieren Sie den NAS-Knoten für die Replikation, indem Sie den Befehl UPDATE NODE ausgeben:

```
update node Knotenname replstate=enabled
```

Dabei gibt *Knotenname* den Namen des NAS-Knotens an.

2. Replizieren Sie den Knoten, indem Sie den Befehl REPLICATE NODE ausgeben:

```
replicate node Knotenname
```

Dabei gibt *Knotenname* den Namen des NAS-Knotens an.

- Um sicherzustellen, dass die replizierten Daten zurückgeschrieben werden können, definieren Sie eine Einheit zum Versetzen von Daten auf dem Zielsystem für den Knoten, indem Sie den Befehl DEFINE DATAMOVER ausgeben:

```
define datamover Knotenname type=nas hladdress=Adresse_der_höheren_Ebene  
lladdress=Adresse_der_unteren_Ebene  
userid=Benutzer-ID password=Benutzerkennwort dataformat=netappdump
```

Erläuterungen:

*Knotenname*

Gibt den Namen des NAS-Knotens an.

*Adresse\_der\_höheren\_Ebene*

Gibt entweder die numerische IP-Adresse oder den Domännennamen für den Zugriff auf den NAS-Dateiserver an.

*Adresse\_der\_unteren\_Ebene*

Gibt die TCP-Portnummer für den Zugriff auf die NAS-Einheit für NDMP-Sitzungen an.

*Benutzer-ID*

Gibt die ID eines Benutzers an, der zum Einleiten einer NDMP-Sitzung mit dem NAS-Dateiserver berechtigt ist.

*Benutzerkennwort*

Gibt das Kennwort des Benutzers an, der zum Einleiten einer NDMP-Sitzung mit dem NAS-Dateiserver berechtigt ist.

## Ergebnisse

---

Das Format der Sicherungsdaten ändert sich während des Replikationsprozesses nicht. Wenn Sicherungsdaten repliziert werden, wird auch das zugehörige Inhaltsverzeichnis repliziert.

## Datenschutz mithilfe des lizenzierten NetApp-Features SnapLock

---

Sie können das lizenzierte NetApp-Feature SnapLock verwenden, um die strengen gesetzlichen Bestimmungen für archivierte Daten einzuhalten. Wenn Sie das Feature SnapLock aktivieren, können Sie mithilfe von IBM Spectrum Protect ein Datum für das Ende des Aufbewahrungszeitraums für Dateien festlegen und eine Datei im WORM-Status (WORM = Write Once Read Many) festschreiben.

Daten, die mit einem Datum für das Ende des Aufbewahrungszeitraums gespeichert werden, können erst aus dem Dateisystem gelöscht werden, wenn der Aufbewahrungszeitraum abgelaufen ist. Das Feature SnapLock kann nur von IBM Spectrum Protect-Servern verwendet werden, wenn für die Server der Aufbewahrungsschutz für Daten aktiviert ist.

Daten, die auf Servern mit aktiviertem Aufbewahrungsschutz für Daten archiviert und auf NetApp-NAS-Dateiservern gespeichert werden, werden als IBM Spectrum Protect-FILE-Datenträger gespeichert. Am Ende einer Schreibtransaktion wird ein Datum für das Ende des Aufbewahrungszeitraums für den FILE-Datenträger über die SnapLock-Schnittstelle definiert. Dieses Datum wird mithilfe der Parameter RETVER und RETMIN der Archivierungskopiengruppe berechnet, die beim Archivieren der Daten verwendet wird. Indem dem FILE-Datenträger ein Datum für das Ende des Aufbewahrungszeitraums zugeordnet wird, wird verhindert, dass die Daten des FILE-Datenträgers gelöscht oder überschrieben werden, bevor der Aufbewahrungszeitraum abläuft. Diese FILE-Datenträger werden als WORM-FILE-Datenträger bezeichnet. Nachdem ein Datum für das Ende des Aufbewahrungszeitraums festgelegt wurde, kann der WORM-FILE-Datenträger erst gelöscht werden, nachdem das Datum für das Ende des Aufbewahrungszeitraums überschritten wurde. IBM Spectrum Protect for Data Retention stellt zusammen mit der WORM-FILE-Datenträgerkonsolidierung den Schutz der Daten während ihres Lebenszyklus sicher.

Speicherpools können entweder nach Schwellenwert oder nach Datenaufbewahrungszeitraum verwaltet werden. Der Speicherpoolparameter RECLAMATIONTYPE gibt an, dass ein Speicherpool auf der Basis eines Datenaufbewahrungszeitraums verwaltet wird. Wird ein traditioneller Speicherpool mit dem Parameter FORMAT=DETAILED abgefragt, wird diese Ausgabe angezeigt:

```
Konsolidierungstyp: THRESHOLD
```

Wenn ein IBM Spectrum Protect-Server mit Aufbewahrungsschutz für Daten über IBM Spectrum Protect for Data Retention aktiviert ist und der Server Zugriff auf einen NetApp-Dateiserver mit dem lizenzierten Feature SnapLock hat, können Sie einen Speicherpool definieren, für den der Parameter RECLAMATIONTYPE auf SNAPLOCK gesetzt ist. Dies bedeutet, dass Daten, die auf Datenträgern in diesem Speicherpool erstellt werden, anhand des Datums für das Ende des Aufbewahrungszeitraums verwaltet werden. Wenn ein SnapLock-Speicherpool mit dem Parameter FORMAT=DETAILED abgefragt wird, gibt die Ausgabe an, dass die Speicherpools anhand des Datenaufbewahrungszeitraums verwaltet werden:

```
Konsolidierungstyp: SNAPLOCK
```

Weitere Informationen zum SnapLock-Dateiserver enthält die NetApp-Dokumentation *Data ONTAP Archive and Compliance Management Guide for 7-Mode*.

Achtung: Verwenden Sie dieses Feature nicht zum Schützen von Daten mit einem Aufbewahrungszeitraum von weniger als drei Monaten.

- **Wiederherstellung und das Feature SnapLock**  
Um sicherzustellen, dass Daten immer geschützt werden, setzen Sie den NetApp-Standardaufbewahrungszeitraum auf 30 Tage, damit er mit dem Standardkonsolidierungszeitraum des WORM-FILE-Datenträgers übereinstimmt. IBM Spectrum Protect konsolidiert alle verbleibenden Daten auf einem WORM-FILE-Datenträger unmittelbar vor dem Ablauf des Aufbewahrungszeitraums.
- **Aufbewahrungszeiträume**  
IBM Spectrum Protect-Maßnahmen steuern den Aufbewahrungszeitraum für den WORM-FILE-Datenträger. Die Aufbewahrungsdauer einiger Dateien kann unter Umständen den Aufbewahrungszeitraum für den WORM-FILE-Datenträger, auf dem sie gespeichert sind, überschreiten. Möglicherweise müssen Sie einige Dateien auf einen anderen Datenträger versetzen, um sicherzustellen, dass die Dateien auf WORM-Datenträgern gespeichert werden.
- **Konfiguration des Features SnapLock für die ereignisgesteuerte Aufbewahrung**  
Auf SnapLock-Datenträgern gespeicherte Daten, die durch IBM Spectrum Protect for Data Retention und ereignisgesteuerte Aufbewahrung verwaltet werden, können zu exzessiver Konsolidierung führen, was Leistungseinbußen auf dem Server zur Folge hat.
- **Unterbrechungsfreier Datenschutz mit dem SnapLock-Feature**  
Wenn Daten auf einem Datenträger mit aktiviertem SnapLock-Feature gespeichert sind und die Daten auf einen Datenträger, auf dem das SnapLock-Feature nicht aktiviert ist, versetzt oder kopiert werden, verlieren die Daten den einzigartigen Hardwareschutz, der durch NetApp-WORM-Datenträger zur Verfügung gestellt wird.
- **SnapLock-Datenträger als IBM Spectrum Protect-WORM-FILE-Datenträger konfigurieren**  
Um die strengen Anforderungen für archivierte Daten zu erfüllen, aktivieren Sie das NetApp-Feature SnapLock.

## Wiederherstellung und das Feature SnapLock

---

Um sicherzustellen, dass Daten immer geschützt werden, setzen Sie den NetApp-Standardaufbewahrungszeitraum auf 30 Tage, damit er mit dem Standardkonsolidierungszeitraum des WORM-FILE-Datenträgers übereinstimmt. IBM Spectrum Protect konsolidiert alle verbleibenden Daten auf einem WORM-FILE-Datenträger unmittelbar vor dem Ablauf des Aufbewahrungszeitraums.

Mit der Konsolidierung eines WORM-FILE-Datenträgers auf einem anderen WORM-FILE-Datenträger vor dem Ablauf des Aufbewahrungszeitraums wird sichergestellt, dass Daten immer durch das Feature SnapLock geschützt werden.

Da dieser Schutz auf der IBM Spectrum Protect-Datenträgerebene stattfindet, können die Daten auf den Datenträgern durch IBM Spectrum Protect-Maßnahmen verwaltet werden, unabhängig davon, wo die Daten gespeichert werden. Daten, die auf WORM-FILE-Datenträgern gespeichert werden, werden sowohl durch den Aufbewahrungsschutz von Daten als auch durch den Aufbewahrungszeitraum geschützt, der mit der physischen Datei auf dem SnapLock-Datenträger gespeichert wird. Wenn ein IBM Spectrum Protect-Administrator einen Befehl zum Löschen der Daten ausgibt, schlägt der Befehl fehl. Wenn ein Benutzer versucht, die Datei mithilfe einer Reihe von Netzdateisystemaufrufen zu löschen, verhindert das Feature SnapLock das Löschen der Daten.

Während der Konsolidierungsverarbeitung wird eine Warnung ausgegeben, wenn der IBM Spectrum Protect-Server keine Daten von einem SnapLock-Datenträger, der verfällt, auf einen neuen SnapLock-Datenträger versetzen kann.

## Aufbewahrungszeiträume

---

IBM Spectrum Protect-Maßnahmen steuern den Aufbewahrungszeitraum für den WORM-FILE-Datenträger. Die Aufbewahrungsdauer einiger Dateien kann unter Umständen den Aufbewahrungszeitraum für den WORM-FILE-Datenträger, auf dem sie gespeichert sind, überschreiten. Möglicherweise müssen Sie einige Dateien auf einen anderen Datenträger versetzen, um sicherzustellen, dass die Dateien auf WORM-Datenträgern gespeichert werden.

Einige Objekte auf dem Datenträger müssen möglicherweise länger als andere Objekte auf dem Datenträger aufbewahrt werden, da:

- Die Objekte an Verwaltungsklassen mit unterschiedlichen Aufbewahrungszeiträumen gebunden sind.
- Die Objekte aufgrund des Status 'Löschen unzulässig' nicht entfernt werden können.
- Die Objekte auf das Eintreten eines Ereignisses vor dem Verfall warten.
- Der Aufbewahrungszeitraum für eine Kopiergruppe verlängert wird und damit ein längerer Aufbewahrungszeitraum als der Aufbewahrungszeitraum erforderlich wird, der im Feature SnapLock beim Festschreiben des WORM-FILE-Datenträgers angegeben wurde.

Um einen WORM-FILE-Datenträger nach Aufbewahrungszeitraum zu verwalten, müssen Sie den Befehl DEFINE STGPOOL unter Angabe von RECLAMATIONTYPE=SNAPLOCK ausgeben. Auf diese Art und Weise definieren Sie einen Speicherpool als SnapLock-Speicherpool. Anschließend können Sie den Parameter RECLAMATIONTYPE nicht mit dem Wert THRESHOLD aktualisieren. Wenn Sie einen SnapLock-Speicherpool definieren, prüft das System, ob die angegebenen Verzeichnisse in der Einheitenklasse SnapLock-WORM-Datenträger sind. Wenn eine Dateiklasse definiert wird und Speicherpools mit dem Konsolidierungstyp SNAPLOCK erstellt werden, müssen alle Datenträger WORM-Datenträger sein; andernfalls schlägt die Operation fehl. Wenn eine Einheitenklasse aktualisiert wird, um zusätzliche Verzeichnisse zu enthalten, und wenn der Einheitenklasse SnapLock-Speicherpools zugeordnet werden, erfolgt dieselbe Prüfung, um sicherzustellen, dass alle Verzeichnisse SnapLock-WORM-Datenträger sind.



Für das NetApp-Feature SnapLock sind drei Aufbewahrungszeiträume verfügbar. Die Aufbewahrungszeiträume müssen korrekt konfiguriert werden, damit der IBM Spectrum Protect-Server WORM-Daten, die auf SnapLock-Datenträgern gespeichert werden, ordnungsgemäß verwalten kann. Der IBM Spectrum Protect-Server legt den Aufbewahrungszeitraum für Daten, die auf NetApp SnapLock-Datenträgern gespeichert werden, auf der Basis der Werte in der Kopiengruppe für die Daten fest, die archiviert werden. Der NetApp-Dateiserver darf nicht mit der Fähigkeit des IBM Spectrum Protect-Servers den Aufbewahrungszeitraum festlegen zu können, im Konflikt stehen. Die bevorzugte Methode ist die Konfiguration der folgenden Einstellungen für Aufbewahrungszeiträume im NetApp-Dateiserver:

- Minimaler Aufbewahrungszeitraum. Definieren Sie den höheren Wert: entweder 30 Tage oder die minimale Anzahl Tage, die von einer beliebigen Kopiengruppe (unter Verwendung eines NetApp SnapLock-Dateiservers für WORM-FILE-Speicher) für den Aufbewahrungszeitraum für Daten angegeben wird. Bei der Kopiengruppe handelt es sich um die Kopiengruppe, die zum Speichern von Daten auf NetApp SnapLock-Datenträgern verwendet wird.
- Maximaler Aufbewahrungszeitraum. Übernehmen Sie den Standardwert von 30 Jahren. Dieser Aufbewahrungszeitraum ermöglicht es dem IBM Spectrum Protect-Server, den tatsächlichen Datenträgeraufbewahrungszeitraum auf der Basis der Einstellungen in der Archivierungskopiengruppe festzulegen.
- Standardaufbewahrungszeitraum. Legen Sie diesen Zeitraum mit 30 Tagen fest. Wenn Sie diesen Wert und den maximalen Aufbewahrungszeitraum nicht festlegen, wird der Aufbewahrungszeitraum jedes Datenträgers auf 30 Jahre gesetzt. In diesem Fall kann der IBM Spectrum Protect-Server den Verfall und die Wiederverwendung von NetApp SnapLock-Datenträgern nicht steuern. Dies hat zur Folge, dass für die Dauer von 30 Jahren kein Datenträger wiederverwendet werden kann.

Wenn die NetApp SnapLock-Aufbewahrungszeiträume festgelegt werden, kann IBM Spectrum Protect die Daten in SnapLock-Speicherpools mit maximaler Effizienz verwalten. Für jeden Datenträger in einem SnapLock-Speicherpool wird ein IBM Spectrum Protect-Konsolidierungszeitraum erstellt. Der IBM Spectrum Protect-Konsolidierungszeitraum hat ein Startdatum (BEGIN RECLAIM PERIOD) und ein Enddatum (END RECLAIM PERIOD). Sie können diese Datumsangaben anzeigen, indem Sie den Befehl `QUERY VOLUME` unter Angabe des Parameters `FORMAT=DETAILED` für einen SnapLock-Datenträger ausgeben. Die Ausgabe ähnelt der in dem folgenden Beispiel:

```
Anfang des Konsolidierungszeitraums: 05.09.2017
Ende des Konsolidierungszeitraums: 06.10.2017
```

Wenn IBM Spectrum Protect Dateien auf einem SnapLock-Datenträger archiviert, verfolgt der Server das späteste Verfallsdatum dieser Dateien und der Wert für BEGIN RECLAIM PERIOD wird auf dieses späteste Verfallsdatum gesetzt. Wenn dem SnapLock-Datenträger weitere Dateien hinzugefügt werden, wird das Startdatum auf dieses spätere Datum gesetzt, wenn eine Datei mit einem späteren Verfallsdatum als das einer derzeit auf dem Datenträger gespeicherten Datei vorhanden ist. Das Startdatum wird für jede Datei auf diesem Datenträger auf das letzte Verfallsdatum gesetzt. Es wird davon ausgegangen, dass alle Dateien auf diesem Datenträger entweder bereits verfallen sind oder an diesem Tag verfallen. Am folgenden Tag sind keine gültigen Daten mehr auf diesem Datenträger vorhanden.

Das Ende des Konsolidierungszeitraums (END RECLAIM PERIOD) wird auf das Datum einen Monat nach dem Anfang des Konsolidierungszeitraums (BEGIN RECLAIM PERIOD) gesetzt. Das Datum für das Ende des Aufbewahrungszeitraums, das auf dem NetApp-Dateiserver für diesen Datenträger festgelegt ist, wird auf das Datum für END RECLAIM PERIOD gesetzt. Der NetApp-Dateiserver verhindert das Löschen dieses Datenträgers, bis das Datum für END RECLAIM PERIOD erreicht wird. Dieses Datum liegt ungefähr einen Monat nach dem Verfall der Daten auf dem IBM Spectrum Protect-Server. Wenn der IBM Spectrum Protect-Server ein Datum für END RECLAIM PERIOD für einen Datenträger berechnet und das Datum nach dem aktuellen Datum für END RECLAIM PERIOD liegt, wird das Datum auf dem NetApp-Dateiserver für diesen Datenträger auf das spätere Datum zurückgesetzt. Indem das Datum auf ein späteres Datum zurückgesetzt wird, wird sichergestellt, dass der IBM Spectrum Protect-WORM-FILE-Datenträger erst gelöscht wird, nachdem alle Daten auf dem Datenträger verfallen sind oder die Daten auf einen anderen SnapLock-Datenträger versetzt wurden.

Der IBM Spectrum Protect-Konsolidierungszeitraum ist der Zeitraum zwischen dem Anfangsdatum und dem Enddatum. Während des Konsolidierungszeitraums löscht der IBM Spectrum Protect-Server Datenträger, auf denen alle Daten verfallen sind, oder versetzt Dateien, die nicht verfallen sind und sich auf SnapLock-Datenträgern befinden, die verfallen, auf neue SnapLock-Datenträger mit neuen Datumsangaben. Dieser Monat ist entscheidend dafür, wie der Server die Daten auf WORM-FILE-Datenträgern sicher und effizient verwaltet. Daten auf einem SnapLock-Datenträger verfallen normalerweise, wenn das Anfangsdatum erreicht wird; außerdem muss der Datenträger leer sein. Wenn das Enddatum erreicht wird, kann der Datenträger gefahrlos aus dem IBM Spectrum Protect-Bestand und auf dem SnapLock-Dateiserver gelöscht werden.

Einige Ereignisse können jedoch zur Folge haben, dass sich gültige Daten auf einem SnapLock-Datenträger befinden:

- Die Verfallsverarbeitung auf dem IBM Spectrum Protect-Server für diesen Datenträger wurde möglicherweise verzögert oder ist nicht abgeschlossen.
- Die Aufbewahrungsparameter in der Kopiengruppe oder in den zugeordneten Verwaltungsklassen wurden möglicherweise für eine Datei nach deren Archivierung geändert und diese Datei wird für einige Zeit nicht verfallen.
- Einer oder mehreren Dateien auf dem Datenträger wurde möglicherweise der Status 'Löschen unzulässig' zugeordnet.
- Die Konsolidierungsverarbeitung ist entweder inaktiviert oder während der Konsolidierungsverarbeitung treten beim Versetzen von Daten auf neue SnapLock-Datenträger in einem SnapLock-Speicherpool Fehler auf.
- Eine Datei wartet auf das Eintreten eines Ereignisses, bevor der IBM Spectrum Protect-Server den Verfall der Datei starten kann.

Wenn das Anfangsdatum erreicht wird und Dateien auf einem SnapLock-Datenträger vorhanden sind, die nicht verfallen sind, müssen die Dateien auf einen neuen SnapLock-Datenträger mit einem neuen Anfangs- und Enddatum versetzt werden. Wenn sich die Verfallsverarbeitung auf dem IBM Spectrum Protect-Server jedoch verzögert und diese Dateien verfallen, wenn die Verfallsverarbeitung auf dem IBM Spectrum Protect-Server ausgeführt wird, ist es ineffizient, diese Dateien auf einen neuen SnapLock-Datenträger zu versetzen. Um sicherzustellen, dass keine unnötige Datenversetzung für Dateien stattfindet, die verfallen werden, wird das Versetzen von Dateien auf SnapLock-Datenträger, die verfallen, um einige Tage nach dem Datum für BEGIN RECLAIM PERIOD verzögert. Da die Daten auf dem SnapLock-Dateiserver bis zum Datum für END RECLAIM PERIOD geschützt sind, sind die Daten durch die Verzögerung dieser Versetzung nicht gefährdet. Damit kann die IBM Spectrum Protect-Verfallsverarbeitung beendet werden. Wenn nach dieser Anzahl Tage gültige Daten auf einem SnapLock-Datenträger, der verfällt, vorhanden sind, werden die Daten auf einen neuen SnapLock-Datenträger versetzt und die Daten bleiben demzufolge geschützt.

Seit dem ersten Archivieren der Daten wurden möglicherweise Änderungen an den Aufbewahrungsparametern für diese Daten vorgenommen (beispielsweise Änderungen an den Verwaltungsklassen- oder Kopienpoolparametern) oder diese Daten haben möglicherweise den Status 'Löschen unzulässig'. Die Daten auf diesem Datenträger werden jedoch von SnapLock nur bis zum Datum für END RECLAIM PERIOD geschützt. Daten, die nicht verfallen sind, werden während des IBM Spectrum Protect-Konsolidierungszeitraums auf neue SnapLock-Datenträger versetzt. Wenn beim Versetzen von Daten auf einen neuen SnapLock-Datenträger Fehler auftreten, wird eine Warnung ausgegeben, die angibt, dass die Daten bald nicht mehr geschützt sind. Wenn der Fehler bestehen bleibt, geben Sie einen Befehl MOVE DATA für den betreffenden Datenträger aus.

Achtung: Inaktivieren Sie die Konsolidierungsverarbeitung für einen SnapLock-Speicherpool nicht. Nach der Inaktivierung der Verarbeitung hat der IBM Spectrum Protect-Server keine Möglichkeit, Warnungen auszugeben, die angeben, dass die Daten bald nicht mehr geschützt sind. Diese Situation kann auch auftreten, wenn Konsolidierung und Umlagerung für den gesamten Server inaktiviert werden (wenn beispielsweise NOMIGRRECL in der Serveroptionsdatei definiert wird). Stellen Sie sicher, dass Ihre Daten geschützt sind, wenn Sie SnapLock-Speicherpools verwalten.

## Konfiguration des Features SnapLock für die ereignisgesteuerte Aufbewahrung

---

Auf SnapLock-Datenträgern gespeicherte Daten, die durch IBM Spectrum Protect for Data Retention und ereignisgesteuerte Aufbewahrung verwaltet werden, können zu exzessiver Konsolidierung führen, was Leistungseinbußen auf dem Server zur Folge hat.

Wenn Daten durch die ereignisgesteuerte Aufbewahrung verwaltet werden, setzt IBM Spectrum Protect anfänglich den Aufbewahrungszeitraum auf den größeren der beiden Werte für RETVER und RETMIN für die Archivierungskopiengruppe. Wenn der Konsolidierungszeitraum für den Datenträger beginnt und Daten, die auf dem Datenträger verbleiben, versetzt werden, wird der Aufbewahrungszeitraum für den Zieldatenträger auf den verbleibenden Aufbewahrungszeitraum der Daten gesetzt, der normalerweise 0 ist. Für den neuen Datenträger beginnt dann der Konsolidierungszeitraum kurz nachdem der Datenträger die Daten empfängt, was die Konsolidierung von Datenträgern zur Folge hat, die gerade erstellt wurden.

Sie können diese Situation durch Verwendung der Serveroption RETENTIONEXTENSION vermeiden. Mit dieser Option kann der Server das Ende des Aufbewahrungszeitraums eines SnapLock-Datenträgers festlegen oder erweitern. Sie können einen Wert im Bereich von 30 bis 9999 Tagen angeben. Der Standardwert ist 365 Tage.

Wenn Sie Datenträger in einem SnapLock-Speicherpool für die Konsolidierung auswählen, prüft der Server, ob sich der Datenträger innerhalb des Konsolidierungszeitraums befindet:

- Wenn sich der Datenträger nicht innerhalb des Konsolidierungszeitraums befindet, wird keine Aktion ausgeführt. Der Datenträger wird nicht konsolidiert und das Ende des Aufbewahrungszeitraums bleibt unverändert.
- Wenn sich der Datenträger innerhalb des Konsolidierungszeitraums befindet, prüft der Server, ob der Prozentsatz des konsolidierbaren Speicherbereichs auf dem Datenträger größer als der Konsolidierungsschwellenwert des Speicherpools oder größer als der Prozentsatz für den Schwellenwert ist, der im Parameter THRESHOLD eines Befehls RECLAIM STGPOOL übergeben wurde:
  - Wenn der konsolidierbare Speicherbereich größer als der Schwellenwert ist, konsolidiert der Server den Datenträger und setzt das Ende des Aufbewahrungszeitraums des Zieldatenträgers auf den größeren der folgenden Werte:
    - Der verbleibende Aufbewahrungszeitraum der Daten plus 30 Tage für den Konsolidierungszeitraum.
    - Der Wert für RETENTIONEXTENSION plus 30 Tage für den Konsolidierungszeitraum.
  - Wenn der konsolidierbare Speicherbereich nicht größer als der Schwellenwert ist, ändert der Server den Wert für das Ende des Aufbewahrungszeitraums des Datenträgers gemäß dem in der Option RETENTIONEXTENSION angegebenen Wert. Der neue Aufbewahrungszeitraum wird berechnet, indem die angegebene Anzahl Tage zum aktuellen Datum addiert wird.

In den folgenden Beispielen befindet sich der SnapLock-Datenträger VolumeA in einem Speicherpool, dessen Konsolidierungsschwellenwert auf 60 % gesetzt ist. Die Serveroption RETENTIONEXTENSION ist auf 365 Tage gesetzt. Der Aufbewahrungszeitraum für VolumeA liegt innerhalb des Konsolidierungszeitraums. Die folgenden Situationen zeigen die Auswirkungen auf den Aufbewahrungszeitraum:

- Der konsolidierbare Speicherbereich auf VolumeA liegt unter 60 %. Das Ende des Aufbewahrungszeitraums von VolumeA wird um 365 Tage verlängert.
- Der konsolidierbare Speicherbereich auf VolumeA ist größer als 60 % und der verbleibende Aufbewahrungszeitraum der Daten beträgt mehr als 365 Tage. VolumeA wird konsolidiert und das Ende des Aufbewahrungszeitraums des Zieldatenträgers wird auf der Basis des verbleibenden Aufbewahrungszeitraums der Daten plus 30 Tage für den Konsolidierungszeitraum gesetzt.
- Der konsolidierbare Speicherbereich auf VolumeA ist größer als 60 % und der Aufbewahrungszeitraum der Daten beträgt weniger als 365 Tage. VolumeA wird konsolidiert und das Ende des Aufbewahrungszeitraums für VolumeA wird auf 365 Tage, den Wert für RETENTIONEXTENTION, plus 30 Tage für den Konsolidierungszeitraum gesetzt.

## Unterbrechungsfreier Datenschutz mit dem SnapLock-Feature

---

Wenn Daten auf einem Datenträger mit aktiviertem SnapLock-Feature gespeichert sind und die Daten auf einen Datenträger, auf dem das SnapLock-Feature nicht aktiviert ist, versetzt oder kopiert werden, verlieren die Daten den einzigartigen Hardwareschutz, der durch NetApp-WORM-Datenträger zur Verfügung gestellt wird.

Der IBM Spectrum Protect-Server erlaubt diesen Typ der Versetzung. Wenn die Daten jedoch von einem WORM-FILE-Datenträger auf einen anderen Typ von Datenträger versetzt werden, sind die Daten möglicherweise nicht mehr vor unbeabsichtigtem oder böswilligem Löschen geschützt. Wenn sich diese Daten zur Erfüllung von Datenaufbewahrungs- und Datenschutzerfordernungen aus rechtlichen Gründen auf WORM-Datenträgern befinden und auf andere Datenträger versetzt werden, erfüllen die Daten möglicherweise nicht mehr diese Anforderungen. Sie müssen Ihre Speicherpools so konfigurieren, dass dieser Typ von Daten in Speicherpools aufbewahrt wird, die während des gesamten Datenaufbewahrungszeitraums aus SnapLock-WORM-Datenträgern bestehen.

## SnapLock-Datenträger als IBM Spectrum Protect-WORM-FILE-Datenträger konfigurieren

---

Um die strengen Anforderungen für archivierte Daten zu erfüllen, aktivieren Sie das NetApp-Feature SnapLock.

### Informationen zu diesem Vorgang

---

Wenn Sie Konfigurationen, die SnapLock-Speicherpools einbeziehen, definieren oder aktualisieren, müssen Sie sicherstellen, dass die Option RECLAMATIONTYPE=SNAPLOCK für die Speicherpools, die für die Parameter NEXTSTGPOOL, RECLAIMSTGPOOL und COPYSTGPOOLS ausgewählt wurden, angegeben ist.

Indem Sie die Speicherpools auf diese Art und Weise konfigurieren, kann sichergestellt werden, dass Ihre Daten ordnungsgemäß geschützt sind. Wenn Sie einen nächsten Speicherpool, einen Konsolidierungsspeicherpool, einen Kopierspeicherpool oder einen Pool für aktive Daten definieren, ohne die Option RECLAMATIONTYPE=SNAPLOCK auszuwählen, ist der Speicherpool nicht geschützt. Der Befehl wird zwar erfolgreich ausgeführt, es wird jedoch eine Warnung ausgegeben.

### Vorgehensweise

---

Um einen SnapLock-Datenträger für die Verwendung als IBM Spectrum Protect-WORM-FILE-Datenträger zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Installieren und konfigurieren Sie SnapLock auf dem NetApp-Dateiserver. Stellen Sie sicher, dass Sie den minimalen, den maximalen und den Standardaufbewahrungszeitraum konfigurieren. Anweisungen finden Sie in der NetApp-Dokumentation.
2. Installieren und konfigurieren Sie einen IBM Spectrum Protect-Server.
3. Aktivieren Sie den Aufbewahrungsschutz für Archivierungsdaten, indem Sie den Befehl SET ARCHIVERETENTIONPROTECTION ausgeben:
 

```
set archiveretentionprotection on
```
4. Konfigurieren Sie die Maßnahme mithilfe des Befehls DEFINE COPYGROUP. Wählen Sie für RETVER und RETMIN in der Archivierungskopiengruppe Werte aus, die Ihre Anforderungen zum Schützen dieser Daten im WORM-Speicher erfüllen. Wenn für RETVER oder RETMIN keine Werte angegeben werden, werden die Werte der Standardverwaltungsklasse verwendet.
5. Konfigurieren Sie Speicher mithilfe des Befehls DEFINE DEVCLASS.
  - Verwenden Sie die Einheitenklasse FILE.
  - Geben Sie den Parameter DIRECTORY an, um auf das Verzeichnis oder die Verzeichnisse auf den SnapLock-Datenträgern zu verweisen.
6. Definieren Sie einen Speicherpool unter Verwendung der Einheitenklasse, die in Schritt 5 definiert wurde, indem Sie den Befehl DEFINE STGPOOL unter Angabe des Parameters RECLAMATIONTYPE=SNAPLOCK ausgeben.
7. Aktualisieren Sie die Kopiengruppe so, dass sie auf den Speicherpool verweist, indem Sie den Befehl UPDATE COPYGROUP ausgeben.
8. Verwenden Sie die IBM Spectrum Protect-API zum Archivieren Ihrer Objekte im SnapLock-Speicherpool. Dieses Feature ist in IBM Spectrum Protect-Standardclients für Sichern/Archivieren nicht verfügbar.

# Daten in Verzeichniscontainerspeicherpools reparieren und wiederherstellen

---

Sie können beschädigte Datenbereiche in Verzeichniscontainerspeicherpools reparieren und verloren gegangene Daten nach einem Katastrophenfall wiederherstellen.

Datenbereiche gehören zu einer Datei, die während des Dateneduplizierungsprozesses erstellt wird. Bereiche werden mit anderen Dateibereichen verglichen, um doppelte Daten zu identifizieren. Wenn in Ihren Verzeichniscontainerspeicherpools beschädigte Dateien oder Verzeichnisse vorhanden sind, können Sie deduplizierte Datenbereiche mithilfe des Zielreplikationsservers, des Quellenreplikationsservers oder mithilfe von Banddatenträgern in Containerkopierspeicherpools reparieren.

- Speicherpools mithilfe eines Zielreplikationsservers reparieren  
Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Quellenreplikationsserver beschädigt sind, können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Quellenreplikationsserver mithilfe eines Zielreplikationsservers reparieren.
- Speicherpools mithilfe von Datenträgern in Containerkopierspeicherpools reparieren  
Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Quellenserver beschädigt sind, können Sie Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Quellenserver reparieren, indem Sie die deduplizierten Datenbereiche von Banddatenträgern in Containerkopierspeicherpools vor Ort oder an einem anderen Standort abrufen.
- Speicherpools in einer Umgebung mithilfe eines Replikationsservers und mithilfe von Datenträgern in Containerkopierspeicherpools reparieren  
Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Quellenserver beschädigt sind, können Sie Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Quellenreplikationsserver reparieren, indem Sie die deduplizierten Datenbereiche vom Zielreplikationsserver oder von Banddatenträgern in Containerkopierspeicherpools abrufen.
- Speicherpools auf einem Zielreplikationsserver reparieren  
Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Zielreplikationsserver beschädigt sind, können Sie Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Zielreplikationsserver reparieren, indem Sie die deduplizierten Datenbereiche vom Quellenreplikationsserver abrufen.
- Speicherpools nach einem Katastrophenfall reparieren  
Nach einem Katastrophenfall können Sie Verzeichniscontainerspeicherpools reparieren und die zugehörigen verloren gegangenen Daten wiederherstellen.
- Beschädigten Banddatenträger im Containerkopierspeicherpool ersetzen  
Wenn ein Banddatenträger, der eine Kopie deduplizierter Datenbereiche in einem Containerkopierspeicherpool speichert, beschädigt wird, können Sie den Datenträger ersetzen.

## **Zugehörige Konzepte:**

Strategien zum Schutz vor Katastrophen

## **Zugehörige Tasks:**

Datenschutzlösungen

Wiederherstellung nach einem Datenverlust oder Systemausfall

## Speicherpools mithilfe eines Zielreplikationsservers reparieren

---

Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Quellenreplikationsserver beschädigt sind, können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Quellenreplikationsserver mithilfe eines Zielreplikationsservers reparieren.

## Vorbereitende Schritte

---

Evaluieren Sie Ihre Speicherumgebung, um festzustellen, ob Ausfälle, Netzprobleme oder Hardwarefehler zu einer Beschädigung an Daten führen oder zur Folge haben, dass die Daten beschädigt zu sein scheinen. Wenn Probleme in Ihrer Umgebung zu einer Beschädigung an Daten führen, ermitteln und beheben Sie die Probleme.

Stellen Sie sicher, dass in dem Verzeichniscontainerspeicherpool genügend Speicherbereich für die wiederhergestellten Daten verfügbar ist. Der Parameter `PREVIEW=YES` im Befehl `REPAIR STGPOOL` gibt an, welches Datenvolumen repariert wird. Wenn nicht genügend Speicherbereich vorhanden ist, stellen Sie mithilfe des Befehls `DEFINE STGPOOLDIRECTORY` Speicherbereich bereit.

## Informationen zu diesem Vorgang

---

Verwenden Sie die folgende Prozedur, um die folgenden Typen von Beschädigungen zu reparieren:

- Geringfügige Beschädigung, die durch das versehentliche Löschen von Dateien oder Verzeichnissen, überschriebene Dateien, versehentliche Änderungen an Dateiberechtigungen oder Plattenfehler aufgrund von Hardwareproblemen verursacht werden.

- Moderate Beschädigung, die durch Plattenfehler oder Datenträgermountfehler verursacht wird. Dieser Typ von Beschädigung hat den Verlust einer oder mehrerer Verzeichnisse zur Folge, aber nicht den Verlust des gesamten Speicherpools.

Beschädigte deduplizierte Speicherbereiche werden mit Bereichen repariert, die auf dem Zielreplikationsserver geschützt wurden.

Einschränkung: Sie können den Befehl REPAIR STGPOOL für einen angegebenen Speicherpool nur ausgeben, wenn die Daten mit dem Befehl PROTECT STGPOOL bereits in einen anderen Speicherpool auf einem Zielreplikationsserver kopiert wurden.

Wenn Sie einen Verzeichniscontainerspeicherpool mithilfe eines Replikationsservers reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Zielreplikationsserver ist nicht verfügbar.
- Der Zielspeicherpool ist beschädigt.
- Es tritt ein Netzausfall auf.

## Vorgehensweise

---

1. Wenn Sie eine geringfügige Beschädigung vermuten, geben Sie den Befehl AUDIT CONTAINER für den Containerspeicherpool auf Verzeichnisebene aus, um Inkonsistenzen zwischen der Datenbank und dem Verzeichniscontainerspeicherpool zu identifizieren. Indem Sie beschädigte Datenbereiche im Verzeichniscontainerspeicherpool identifizieren, können Sie die zu reparierenden Datenbereiche bestimmen. Um Zeit und Ressourcen einzusparen, prüfen Sie nur Container, bei denen Sie eine Beschädigung vermuten. Wenn Sie vermuten, dass Ihr Verzeichniscontainerspeicherpool eine schwerwiegendere Beschädigung aufweist, geben Sie den Befehl AUDIT CONTAINER auf Speicherpoolebene aus.

Um beispielsweise ein Verzeichnis, n:\pooldir, in einem Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1 stgpooldirectory=n:\pooldir
```

Um einen Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1
```

Die Ausführung des Prüfprozesses kann mehrere Stunden dauern.

2. Um einen Verzeichniscontainerspeicherpool zu reparieren, geben Sie den Befehl REPAIR STGPOOL unter Angabe des Parameters SRCLOCATION=REPLSERVER aus. Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 mithilfe eines Replikationsservers zu reparieren, geben Sie den folgenden Befehl aus:

```
repair stgpool stgpool1 srclocation=replserver
```

Wenn Sie den Befehl REPAIR STGPOOL ausgeben, werden die beschädigten Bereiche unmittelbar nach der Reparatur von dem Datenträger gelöscht. Die beschädigten Bereiche werden nicht gemäß dem im Parameter REUSEDelay angegebenen Wert beibehalten.

3. Identifizieren Sie alle weiteren beschädigten Bereiche, indem Sie den Befehl QUERY DAMAGED ausgeben.
4. Wenn eine Beschädigung erkannt wird und deduplizierte Speicherbereiche nicht mithilfe des Replikationsservers repariert werden können, ist eine Reparatur dennoch möglich. In einigen Fällen sendet der Clientknoten Daten im Rahmen einer Sicherungsoperation erneut und die beschädigten Bereiche werden repariert. Warten Sie für die Dauer von zwei Sicherungszyklen, um die Ausführung von Clientsicherungsoperationen zu ermöglichen. Führen Sie im Anschluss an zwei Sicherungszyklen die folgenden Schritte aus:

- a. Um zu prüfen, ob die Beschädigung repariert wurde, geben Sie den Befehl QUERY DAMAGED erneut aus.
- b. Wenn ein vollständiges Speicherpoolverzeichnis beschädigt ist, erstellen Sie ein neues Speicherpoolersatzverzeichnis mithilfe des Befehls DEFINE STGPOOLDIRECTORY.
- c. Um Objekte zu entfernen, die sich auf beschädigte Daten beziehen, geben Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=REMOVEDAMAGED aus.  
Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL1 zu prüfen und beschädigte Objekte zu entfernen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1 action=removedamaged
```

- d. Wahlweise können Sie den Befehl DELETE STGPOOLDIRECTORY ausgeben, um das leere Speicherpoolverzeichnis, das Sie in Schritt 4.b durch ein neues Verzeichnis ersetzt hatten, zu löschen.

## Nächste Schritte

---

Wenn Sie im Laufe der Zeit immer wieder beschädigte Daten erkennen, geben Sie den Befehl AUDIT CONTAINER für den Verzeichniscontainerspeicherpool aus, um festzustellen, ob eine umfangreichere Beschädigung vorliegt. Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1
```

### Zugehörige Verweise:

AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)  
DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)  
QUERY DAMAGED (Beschädigte Speicherpooldaten abfragen)  
PROTECT STGPOOL (Speicherpooldaten schützen)  
REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)  
DEFINE STGPOOLDIRECTORY (Speicherpoolverzeichnis definieren)  
DELETE STGPOOLDIRECTORY (Speicherpoolverzeichnis löschen)

## Speicherpools mithilfe von Datenträgern in Containerkopierspeicherpools reparieren

---

Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Quellenserver beschädigt sind, können Sie Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Quellenserver reparieren, indem Sie die deduplizierten Datenbereiche von Banddatenträgern in Containerkopierspeicherpools vor Ort oder an einem anderen Standort abrufen.

### Vorbereitende Schritte

---

Evaluieren Sie Ihre Speicherumgebung, um festzustellen, ob Ausfälle, Netzprobleme oder Hardwarefehler zu einer Beschädigung an Daten führen oder zur Folge haben, dass die Daten beschädigt zu sein scheinen. Wenn Probleme in Ihrer Umgebung zu einer Beschädigung an Daten führen, ermitteln und beheben Sie die Probleme.

Stellen Sie sicher, dass in dem Verzeichniscontainerspeicherpool genügend Speicherbereich für die wiederhergestellten Daten verfügbar ist. Der Parameter PREVIEW=YES im Befehl REPAIR STGPOOL gibt an, welches Datenvolumen repariert wird. Wenn nicht genügend Speicherbereich vorhanden ist, stellen Sie mithilfe des Befehls DEFINE STGPOOLDIRECTORY Speicherbereich bereit.

### Informationen zu diesem Vorgang

---

Verwenden Sie die folgende Prozedur, um die folgenden Typen von Beschädigungen zu reparieren:

- Geringfügige Beschädigung, die durch das versehentliche Löschen von Dateien oder Verzeichnissen, überschriebene Dateien, versehentliche Änderungen an Dateiberechtigungen oder Plattenfehler aufgrund von Hardwareproblemen verursacht werden.
- Moderate Beschädigung, die durch Plattenfehler oder Datenträgermountfehler verursacht wird. Dieser Typ von Beschädigung hat den Verlust einer oder mehrerer Verzeichnisse zur Folge, aber nicht den Verlust des gesamten Speicherpools.

Beschädigte deduplizierte Speicherbereiche werden mit Bereichen repariert, die in Containerkopierspeicherpools geschützt wurden. Einschränkung: Sie können den Befehl REPAIR STGPOOL für einen angegebenen Speicherpool nur ausgeben, wenn die Daten mit dem Befehl PROTECT STGPOOL bereits in Containerkopierspeicherpools kopiert wurden.

Wenn Sie einen Verzeichniscontainerspeicherpool mithilfe von Containerkopierspeicherpools reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Containerkopierspeicherpool ist nicht verfügbar.
- Der Containerkopierspeicherpool ist beschädigt.
- Die Datenträger in Containerkopierspeicherpools sind nicht verfügbar oder beschädigt.

### Vorgehensweise

---

1. Wenn Sie eine geringfügige Beschädigung vermuten, geben Sie den Befehl AUDIT CONTAINER für den Containerspeicherpool auf Verzeichnisebene aus, um Inkonsistenzen zwischen der Datenbank und dem Verzeichniscontainerspeicherpool zu identifizieren. Indem Sie beschädigte Datenbereiche im Verzeichniscontainerspeicherpool identifizieren, können Sie die zu reparierenden Datenbereiche bestimmen. Um Zeit und Ressourcen einzusparen, prüfen Sie nur Container, bei denen Sie eine Beschädigung vermuten. Wenn Sie vermuten, dass Ihr Containerspeicherpool eine schwerwiegendere Beschädigung aufweist, geben Sie den Befehl AUDIT CONTAINER auf Speicherpoolebene aus. Um beispielsweise ein Verzeichnis, n:\pooldir, in einem Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1 stgpooldirectory=n:\pooldir
```

Um einen Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1
```

Die Ausführung des Prüfprozesses kann mehrere Stunden dauern.

Während der Reparaturoperation fordert der Server von Ihnen die erforderlichen Datenträger an. In Schritt 3 werden die Datenträger wieder vor Ort gebracht und in das Speicherarchiv zurückgestellt. Die erforderlichen Datenträger müssen vor Ort

gebracht und in das Speicherarchiv zurückgestellt werden.

- Um eine Voranzeige der Reparaturoperation aufzurufen und die Liste der für die Reparaturoperation erforderlichen Banddatenträger zu generieren, geben Sie den Befehl REPAIR STGPOOL unter Angabe der Parameter SRCLOCATION=LOCAL und PREVIEW=YES aus.

Um beispielsweise für einen Speicherpool mit dem Namen STGPOOL1 eine Voranzeige der Reparaturoperation mithilfe von Containerkopierspeicherpools aufzurufen, geben Sie den folgenden Befehl aus:

```
repair stgpool stgpool1 srclocation=local preview=yes
```

Die Ausführung des Voranzeigeprozesses kann einige Zeit in Anspruch nehmen.

- Wenn sich einige der erforderlichen Datenträger an einen anderen Standort befinden, führen Sie die folgenden Schritte aus:
  - Bestimmen Sie mithilfe der Liste der Voranzeigeoperation, welche Datenträger vor Ort gebracht werden müssen.
  - Wenn sich die Datenträger wieder vor Ort befinden, stellen Sie diese in das Speicherarchiv zurück, indem Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters STATUS=PRIVATE ausgeben.
  - Aktualisieren Sie den Status der Datenträger, indem Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters ACCESS=READWRITE ausgeben.

Detaillierte Anweisungen zur Funktion Disaster Recovery Manager (DRM) finden Sie in Disaster Recovery Manager für Bandumgebungen verwenden (Version 7.1.1).

- Stellen Sie auf der Basis der Informationen, die während der Voranzeigeoperation abgerufen wurden, sicher, dass der Speicherpool über genügend Speicherbereich für die wiederhergestellten Daten verfügt. Wenn nicht genügend Speicherbereich vorhanden ist, stellen Sie mithilfe des Befehls DEFINE STGPOOLDIRECTORY Speicherbereich bereit.
- Um den Verzeichniscontainerspeicherpool zu reparieren, geben Sie den Befehl REPAIR STGPOOL unter Angabe des Parameters SRCLOCATION=LOCAL aus.

Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 mithilfe eines Containerkopierspeicherpools zu reparieren, geben Sie den folgenden Befehl aus:

```
repair stgpool stgpool1 srclocation=local
```

Wenn Sie den Befehl REPAIR STGPOOL ausgeben, werden die beschädigten Bereiche unmittelbar nach der Reparatur von dem Datenträger gelöscht. Die beschädigten Bereiche werden nicht gemäß dem im Parameter REUSEDELAY angegebenen Wert beibehalten.

- Identifizieren Sie alle weiteren beschädigten Bereiche, indem Sie den Befehl QUERY DAMAGED ausgeben.
- Wenn eine Beschädigung erkannt wird und deduplizierte Speicherbereiche nicht mithilfe der Containerkopierspeicherpools repariert werden können, ist eine Reparatur dennoch möglich. In einigen Fällen sendet der Clientknoten Daten im Rahmen einer Sicherungsoperation erneut und die beschädigten Bereiche werden repariert. Warten Sie für die Dauer von zwei Sicherungszyklen, um die Ausführung von Clientsicherungsoperationen zu ermöglichen. Führen Sie im Anschluss an zwei Sicherungszyklen die folgenden Schritte aus:
  - Um zu prüfen, ob die Beschädigung repariert wurde, geben Sie den Befehl QUERY DAMAGED erneut aus.
  - Wenn ein vollständiges Speicherpoolverzeichnis beschädigt ist, erstellen Sie ein neues Speicherpoolersatzverzeichnis mithilfe des Befehls DEFINE STGPOOLDIRECTORY.
  - Um Objekte zu entfernen, die sich auf beschädigte Daten beziehen, geben Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=REMOVEDAMAGED aus.  
Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL1 zu prüfen und beschädigte Objekte zu entfernen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1 action=removedamaged
```

- Wahlweise können Sie den Befehl DELETE STGPOOLDIRECTORY ausgeben, um das leere Speicherpoolverzeichnis, das Sie in Schritt 7.b durch ein neues Verzeichnis ersetzt hatten, zu löschen.

- Wenn ein vollständiges Speicherpoolverzeichnis repariert wurde, löschen Sie das ursprüngliche Verzeichnis, das leer ist und durch ein neues Verzeichnis ersetzt wurde. Löschen Sie das ursprüngliche Verzeichnis, indem Sie den Befehl DELETE STGPOOLDIRECTORY ausgeben.

## Nächste Schritte

---

Wenn Sie im Laufe der Zeit immer wieder beschädigte Daten erkennen, geben Sie den Befehl AUDIT CONTAINER für den Verzeichniscontainerspeicherpool aus, um festzustellen, ob eine umfangreichere Beschädigung vorliegt. Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1
```

### Zugehörige Verweise:

AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)

DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)

QUERY DAMAGED (Beschädigte Speicherpooldaten abfragen)

PROTECT STGPOOL (Speicherpooldaten schützen)  
REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)  
DEFINE STGPOOLDIRECTORY (Speicherpoolverzeichnis definieren)  
DELETE STGPOOLDIRECTORY (Speicherpoolverzeichnis löschen)

## Speicherpools in einer Umgebung mithilfe eines Replikationsservers und mithilfe von Datenträgern in Containerkopierspeicherpools reparieren

---

Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Quellenserver beschädigt sind, können Sie Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Quellenreplikationsserver reparieren, indem Sie die deduplizierten Datenbereiche vom Zielreplikationsserver oder von Banddatenträgern in Containerkopierspeicherpools abrufen.

### Vorbereitende Schritte

---

Evaluieren Sie Ihre Speicherumgebung, um festzustellen, ob Ausfälle, Netzprobleme oder Hardwarefehler zu einer Beschädigung an Daten führen oder zur Folge haben, dass die Daten beschädigt zu sein scheinen. Wenn Probleme in Ihrer Umgebung zu einer Beschädigung an Daten führen, ermitteln und beheben Sie die Probleme.

Stellen Sie sicher, dass in dem Verzeichniscontainerspeicherpool genügend Speicherbereich für die wiederhergestellten Daten verfügbar ist. Der Parameter `PREVIEW=YES` im Befehl `REPAIR STGPOOL` gibt an, welches Datenvolumen repariert wird. Wenn nicht genügend Speicherbereich vorhanden ist, stellen Sie mithilfe des Befehls `DEFINE STGPOOLDIRECTORY` Speicherbereich bereit.

### Informationen zu diesem Vorgang

---

Verwenden Sie die folgende Prozedur, um die folgenden Typen von Beschädigungen zu reparieren:

- Geringfügige Beschädigung, die durch das versehentliche Löschen von Dateien oder Verzeichnissen, überschriebene Dateien, versehentliche Änderungen an Dateiberechtigungen oder Plattenfehler aufgrund von Hardwareproblemen verursacht werden.
- Moderate Beschädigung, die durch Plattenfehler oder Datenträgermountfehler verursacht wird. Dieser Typ von Beschädigung hat den Verlust einer oder mehrerer Verzeichnisse zur Folge, aber nicht den Verlust des gesamten Speicherpools.

Beschädigte deduplizierte Speicherbereiche werden mit Bereichen repariert, die auf dem Zielreplikationsserver oder in Containerkopierspeicherpools auf einem Quellenserver geschützt wurden.

Einschränkung: Sie können den Befehl `REPAIR STGPOOL` für einen angegebenen Speicherpool nur ausgeben, wenn die Daten mit dem Befehl `PROTECT STGPOOL` bereits in einen anderen Speicherpool auf einem Zielreplikationsserver oder in Containerkopierspeicherpools kopiert wurden.

Wenn Sie einen Verzeichniscontainerspeicherpool mithilfe eines Zielreplikationsservers reparieren, schlägt der Befehl `REPAIR STGPOOL` fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Zielreplikationsserver ist nicht verfügbar.
- Der Zielspeicherpool ist beschädigt.
- Es tritt ein Netzausfall auf.

Wenn Sie einen Verzeichniscontainerspeicherpool mithilfe von Containerkopierspeicherpools reparieren, schlägt der Befehl `REPAIR STGPOOL` fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Containerkopierspeicherpool ist nicht verfügbar.
- Der Containerkopierspeicherpool ist beschädigt.
- Die Datenträger in Containerkopierspeicherpools sind nicht verfügbar oder beschädigt.

### Vorgehensweise

---

1. Versuchen Sie, den Speicherpool mithilfe des Zielreplikationsservers zu reparieren, indem Sie die Schritte in Speicherpools mithilfe eines Zielreplikationsservers reparieren ausführen.
2. Wenn die beschädigten Bereiche nicht mithilfe des Zielreplikationsservers repariert werden können, reparieren Sie die beschädigten Bereiche mithilfe von Containerkopierspeicherpools, indem Sie die Schritte in Speicherpools mithilfe von Datenträgern in Containerkopierspeicherpools reparieren ausführen.
3. Wenn Sie beschädigte Bereiche mithilfe von Containerkopierspeicherpools repariert hatten, geben Sie den Befehl `PROTECT STGPOOL` unter Angabe des Parameters `TYPE=REPLSERVER` für die Speicherpools auf dem Quellenreplikationsserver aus.

### Nächste Schritte

---

Wenn Sie im Laufe der Zeit immer wieder beschädigte Daten erkennen, geben Sie den Befehl `AUDIT CONTAINER` für den Verzeichniscontainerspeicherpool aus, um festzustellen, ob eine umfangreichere Beschädigung vorliegt. Um beispielsweise einen



Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1
```

**Zugehörige Verweise:**

AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)  
DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)  
QUERY DAMAGED (Beschädigte Speicherpooldaten abfragen)  
PROTECT STGPOOL (Speicherpooldaten schützen)  
REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)  
DEFINE STGPOOLDIRECTORY (Speicherpoolverzeichnis definieren)  
DELETE STGPOOLDIRECTORY (Speicherpoolverzeichnis löschen)

## Speicherpools auf einem Zielreplikationsserver reparieren

---

Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Zielreplikationsserver beschädigt sind, können Sie Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Zielreplikationsserver reparieren, indem Sie die deduplizierten Datenbereiche vom Quellenreplikationsserver abrufen.

### Vorbereitende Schritte

---

Evaluieren Sie Ihre Speicherumgebung, um festzustellen, ob Ausfälle, Netzprobleme oder Hardwarefehler zu einer Beschädigung an Daten führen oder zur Folge haben, dass die Daten beschädigt zu sein scheinen. Wenn Probleme in Ihrer Umgebung zu einer Beschädigung an Daten führen, ermitteln und beheben Sie die Probleme.

### Informationen zu diesem Vorgang

---

Verwenden Sie die folgende Prozedur, um die folgenden Typen von Beschädigungen zu reparieren:

- Geringfügige Beschädigung, die durch das versehentliche Löschen von Dateien oder Verzeichnissen, überschriebene Dateien, versehentliche Änderungen an Dateiberechtigungen oder Plattenfehler aufgrund von Hardwareproblemen verursacht werden.
- Moderate Beschädigung, die durch Plattenfehler oder Datenträgermountfehler verursacht wird. Dieser Typ von Beschädigung hat den Verlust einer oder mehrerer Verzeichnisse zur Folge, aber nicht den Verlust des gesamten Speicherpools.

Im Rahmen der Ausführung des Befehls PROTECT STGPOOL werden beschädigte Speicherbereiche im Zielspeicherpool repariert. Eine Reparatur ist nur möglich, wenn die Speicherbereiche auf dem Zielspeicher bereits als beschädigt markiert sind. Beispielsweise kann vor der Ausgabe des Befehls PROTECT STGPOOL mit einem Befehl AUDIT CONTAINER eine Beschädigung im Zielspeicherpool identifiziert werden.

### Vorgehensweise

---

1. Schützen Sie Datenbereiche in einem Verzeichniscontainerspeicherpool auf einem Quellenserver, indem Sie den Befehl PROTECT STGPOOL ausgeben.

Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen POOL1 zu schützen, geben Sie den folgenden Befehl aus:

```
protect stgpool pool1
```

Warten Sie, bis der Prozess zum Schützen beendet ist.

2. Um die beschädigten Datenbereiche in dem Verzeichniscontainerspeicherpool auf dem Zielserver zu identifizieren, geben Sie den Befehl AUDIT CONTAINER aus.

Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1
```

3. Reparieren Sie beschädigte Bereiche in dem Zielspeicherpool, indem Sie den Befehl PROTECT STGPOOL auf dem Quellenserver erneut ausgeben. Die beschädigten Bereiche im Zielspeicherpool werden als beschädigt markiert und repariert.
4. Stellen Sie sicher, dass keine weiteren beschädigten Bereiche vorhanden sind, indem Sie den Befehl QUERY DAMAGED ausgeben.

**Zugehörige Verweise:**

AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)  
DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)  
QUERY DAMAGED (Beschädigte Speicherpooldaten abfragen)  
PROTECT STGPOOL (Speicherpooldaten schützen)  
REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)  
DEFINE STGPOOLDIRECTORY (Speicherpoolverzeichnis definieren)

## Speicherpools nach einem Katastrophenfall reparieren

---

Nach einem Katastrophenfall können Sie Verzeichniscontainerspeicherpools reparieren und die zugehörigen verloren gegangenen Daten wiederherstellen.

Wenn ein Katastrophenfall eintritt und Ihr primärer Standort nicht mehr verfügbar ist, können Sie Ihre Verzeichniscontainerspeicherpools reparieren, indem Sie diese an Ihrem Wiederherstellungsstandort auf einen neuen Zielsever zurückschreiben.

- Speicherpools mithilfe von Datenträgern in Containerkopierspeicherpools nach einem Katastrophenfall reparieren  
Bei einem Katastrophenfall auf einem Quellenserver können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool mithilfe von ausgelagerten Banddatenträgern in Containerkopierspeicherpools reparieren. Der Verzeichniscontainerspeicherpool wird auf einem Zielsever am Wiederherstellungsstandort repariert.
- Speicherpools mithilfe eines Zielreplikationsservers nach einem Katastrophenfall reparieren  
Bei einem Katastrophenfall auf einem Quellenreplikationsserver können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool mithilfe eines Zielreplikationsservers reparieren. Der Verzeichniscontainerspeicherpool wird auf einem Zielsever am Wiederherstellungsstandort repariert.
- Speicherpools in einer Umgebung mithilfe eines Replikationsservers und mithilfe von Datenträgern in Containerkopierspeicherpools nach einem Katastrophenfall reparieren  
Bei einem Katastrophenfall auf einem Quellenserver können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool mithilfe eines Zielreplikationsservers oder mithilfe von ausgelagerten Banddatenträgern in Containerkopierspeicherpools reparieren. Der Verzeichniscontainerspeicherpool wird auf einem Zielsever am Wiederherstellungsstandort repariert.

### Zugehörige Verweise:

Bestimmen, ob Containerkopierspeicherpools für den Schutz vor Katastrophen verwendet werden können

## Speicherpools mithilfe von Datenträgern in Containerkopierspeicherpools nach einem Katastrophenfall reparieren

---

Bei einem Katastrophenfall auf einem Quellenserver können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool mithilfe von ausgelagerten Banddatenträgern in Containerkopierspeicherpools reparieren. Der Verzeichniscontainerspeicherpool wird auf einem Zielsever am Wiederherstellungsstandort repariert.

### Informationen zu diesem Vorgang

---

Verwenden Sie die folgende Prozedur, um die folgenden Typen schwerwiegender Beschädigungen zu reparieren:

- Vollständiger Verlust aller Containerspeicherpools auf dem Quellenserver
- Vollständiger Verlust des primären Standorts

Für dieses Wiederherstellungsszenario gelten die folgenden Voraussetzungen:

- Sie hatten den Befehl PROTECT STGPOOL verwendet, um Daten von einem Quellenserver in Containerkopierspeicherpools an einem anderen Standort zu sichern. Sie hatten die ausgelagerten Banddatenträger abgerufen, sodass diese am Wiederherstellungsstandort vorhanden sind.
- Sie hatten nicht den Befehl PROTECT STGPOOL verwendet, um Daten auf einen Zielreplikationsserver zu sichern.
- Sie hatten die IBM Spectrum Protect-Blueprints verwendet, um den IBM Spectrum Protect-Quellenserver zu konfigurieren; außerdem hatten Sie die Blueprint-Konfigurationsscripts verwendet, um die Umgebung zurückzuschreiben, indem am Wiederherstellungsstandort ein neuer Zielsever konfiguriert wurde. Mit den Scripts wurden Sicherungsversionen der IBM Spectrum Protect-Datenbank, der Serveroptionsdatei (dsmserv.opt), der Protokolldatei für Datenträger (volhist.out) und der Einheitenkonfigurationsdatei (devconfig.out) an ihre ursprünglichen Positionen auf dem Wiederherstellungsserver kopiert. Nach der Ausführung der Scripts werden die neu erstellten, leeren Verzeichnisse auf dem Wiederherstellungsserver angezeigt.

Wenn Sie versuchen, einen Verzeichniscontainerspeicherpool mithilfe von Containerkopierspeicherpools zu reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Containerkopierspeicherpool ist nicht verfügbar.
- Der Containerkopierspeicherpool ist beschädigt.
- Die Datenträger in Containerkopierspeicherpools sind nicht verfügbar oder beschädigt.

### Vorgehensweise

---

1. Markieren Sie alle Datenbereiche in dem Containerspeicherpool als beschädigt, indem Sie den Befehl `AUDIT CONTAINER` unter Angabe des Parameters `ACTION=MARKDAMAGED` für den Containerspeicherpool auf Speicherpoolebene ausgeben. Um beispielsweise einen Speicherpool mit dem Namen `STGPOOL1` zu prüfen und als beschädigt zu markieren, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1 action=markdamaged
```

2. Wenn Sie den Verzeichniscontainerspeicherpool sowohl mit Containerkopierspeicherpools vor Ort als auch mit Containerkopierspeicherpools an einem anderen Standort geschützt hatten, geben Sie den Befehl `UPDATE STGPOOL` unter Angabe des Parameters `ACCESS=UNAVAILABLE` für die Kopie des Containerkopierspeicherpools vor Ort aus.
3. Wenn sich die ausgelagerten Datenträger in Containerkopierspeicherpools wieder vor Ort befinden, stellen Sie diese in das Speicherarchiv zurück, indem Sie den Befehl `CHECKIN LIBVOLUME` unter Angabe des Parameters `STATUS=PRIVATE` ausgeben.
4. Aktualisieren Sie den Status der Datenträger, indem Sie den Befehl `UPDATE STGPOOL` unter Angabe des Parameters `ACCESS=READWRITE` ausgeben.
5. Reparieren Sie den Speicherpool, indem Sie den Befehl `REPAIR STGPOOL` unter Angabe des Parameters `SRCLOCATION=LOCAL` ausgeben. Um beispielsweise einen Speicherpool mit dem Namen `STGPOOL1` mithilfe von Containerkopierspeicherpools an einem anderen Standort zu reparieren, geben Sie den folgenden Befehl aus:

```
repair stgpool stgpool1 srclocation=local
```

Wenn Sie den Befehl `REPAIR STGPOOL` ausgeben, werden die beschädigten Bereiche unmittelbar nach der Reparatur von dem Datenträger gelöscht. Die beschädigten Bereiche werden nicht gemäß dem im Parameter `REUSEDELAY` angegebenen Wert beibehalten.

6. Stellen Sie sicher, dass keine weiteren beschädigten Bereiche vorhanden sind, indem Sie den Befehl `QUERY DAMAGED` ausgeben.
7. Wiederholen Sie diese Prozedur, um alle Ihre Speicherpools zu reparieren.

## Speicherpools mithilfe eines Zielreplikationsservers nach einem Katastrophenfall reparieren

---

Bei einem Katastrophenfall auf einem Quellenreplikationsserver können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool mithilfe eines Zielreplikationsservers reparieren. Der Verzeichniscontainerspeicherpool wird auf einem Zielsystem am Wiederherstellungsstandort repariert.

### Informationen zu diesem Vorgang

---

Verwenden Sie die folgende Prozedur, um die folgenden Typen schwerwiegender Beschädigungen zu reparieren:

- Vollständiger Verlust aller Containerspeicherpools auf dem Quellenreplikationsserver
- Vollständiger Verlust des primären Standorts

Für dieses Wiederherstellungsszenario gelten die folgenden Voraussetzungen:

- Sie hatten den Befehl `PROTECT STGPOOL` verwendet, um Daten von einem Quellenreplikationsserver auf einen Zielreplikationsserver zu sichern. Der Zielreplikationsserver wird an Ihrem Wiederherstellungsstandort ausgeführt.
- Sie hatten nicht den Befehl `PROTECT STGPOOL` verwendet, um Daten in Containerkopierspeicherpools an einem anderen Standort zu sichern.
- Sie hatten die IBM Spectrum Protect-Blueprints verwendet, um den IBM Spectrum Protect-Quellenserver zu konfigurieren; außerdem hatten Sie die Blueprint-Konfigurationsskripts verwendet, um die Umgebung zurückzuschreiben, indem am Wiederherstellungsstandort ein neuer Zielsystem konfiguriert wurde. Mit den Skripten wurden Sicherungsversionen der IBM Spectrum Protect-Datenbank, der Serveroptionsdatei (`dsmserv.opt`), der Protokolldatei für Datenträger (`volhist.out`) und der Einheitenkonfigurationsdatei (`devconfig.out`) an ihre ursprünglichen Positionen auf dem Wiederherstellungsserver kopiert. Nach der Ausführung der Skripts werden die neu erstellten, leeren Verzeichnisse auf dem Wiederherstellungsserver angezeigt.

Wenn Sie versuchen, einen Verzeichniscontainerspeicherpool mithilfe eines Zielreplikationsservers zu reparieren, schlägt der Befehl `REPAIR STGPOOL` fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Zielreplikationsserver ist nicht verfügbar.
- Der Zielspeicherpool ist beschädigt.
- Es tritt ein Netzausfall auf.

### Vorgehensweise

---

1. Markieren Sie alle Datenbereiche in dem Containerspeicherpool als beschädigt, indem Sie den Befehl `AUDIT CONTAINER` unter Angabe des Parameters `ACTION=MARKDAMAGED` für den Containerspeicherpool auf Speicherpoolebene ausgeben.

Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 zu prüfen und als beschädigt zu markieren, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1 action=markdamaged
```

2. Reparieren Sie den Speicherpool, indem Sie den Befehl REPAIR STGPOOL unter Angabe des Parameters SRCLOCATION=REPLSERVER ausgeben.

Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 mithilfe eines Zielreplikationsservers zu reparieren, geben Sie den folgenden Befehl aus:

```
repair stgpool stgpool1 srclocation=replserver
```

Wenn Sie den Befehl REPAIR STGPOOL ausgeben, werden die beschädigten Bereiche unmittelbar nach der Reparatur von dem Datenträger gelöscht. Die beschädigten Bereiche werden nicht gemäß dem im Parameter REUSEDELAY angegebenen Wert beibehalten.

3. Wenn Sie nicht die Blueprint-Konfigurationsskripts für die Konfiguration Ihres Zielreplikationsservers verwendet hatten, stimmt die Dateistruktur auf dem Zielreplikationsserver möglicherweise nicht mit den in der Datenbank gespeicherten Informationen überein. Entfernen Sie wahlweise die Speicherpoolverzeichnisse, die auf dem Zielreplikationsserver nicht vorhanden sind, indem Sie den Befehl DELETE STGPOOLDIRECTORY ausgeben.
4. Stellen Sie sicher, dass keine weiteren beschädigten Bereiche vorhanden sind, indem Sie den Befehl QUERY DAMAGED ausgeben.
5. Wenn eine Beschädigung erkannt wird und deduplizierte Speicherbereiche nicht mithilfe des Replikationsservers repariert werden können, ist eine Reparatur dennoch möglich. In einigen Fällen sendet der Clientknoten Daten im Rahmen einer Sicherungsoperation erneut und die beschädigten Bereiche werden repariert. Warten Sie für die Dauer von zwei Sicherungszyklen, um die Ausführung von Clientsicherungsoperationen zu ermöglichen. Führen Sie im Anschluss an zwei Sicherungszyklen die folgenden Schritte aus:
  - a. Um zu prüfen, ob die Beschädigung repariert wurde, geben Sie den Befehl QUERY DAMAGED erneut aus.
  - b. Um Objekte zu entfernen, die sich auf beschädigte Daten beziehen, geben Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=REMOVEDAMAGED aus.  
Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL1 zu prüfen und beschädigte Objekte zu entfernen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1 action=removedamaged
```

6. Wiederholen Sie diese Prozedur, um alle Ihre Speicherpools zu reparieren.

#### Zugehörige Verweise:

QUERY DAMAGED (Beschädigte Speicherpooldaten abfragen)

## Speicherpools in einer Umgebung mithilfe eines Replikationsservers und mithilfe von Datenträgern in Containerkopierspeicherpools nach einem Katastrophenfall reparieren

---

Bei einem Katastrophenfall auf einem Quellenserver können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool mithilfe eines Zielreplikationsservers oder mithilfe von ausgelagerten Banddatenträgern in Containerkopierspeicherpools reparieren. Der Verzeichniscontainerspeicherpool wird auf einem Zielsystem am Wiederherstellungsstandort repariert.

### Informationen zu diesem Vorgang

---

Verwenden Sie die folgende Prozedur, um die folgenden Typen schwerwiegender Beschädigungen zu reparieren:

- Vollständiger Verlust aller Containerspeicherpools auf dem Quellenserver
- Vollständiger Verlust des primären Standorts

Für dieses Wiederherstellungsszenario gelten die folgenden Voraussetzungen:

- Sie hatten den Befehl PROTECT STGPOOL verwendet, um Daten von einem Quellenreplikationsserver auf einen Zielreplikationsserver zu sichern. Der Zielreplikationsserver wird an Ihrem Wiederherstellungsstandort ausgeführt.
- Sie hatten den Befehl PROTECT STGPOOL verwendet, um Daten in Containerkopierspeicherpools an einem anderen Standort zu sichern.
- Sie hatten die IBM Spectrum Protect-Blueprints verwendet, um den IBM Spectrum Protect-Quellenserver zu konfigurieren; außerdem hatten Sie die Blueprint-Konfigurationsskripts verwendet, um die Umgebung zurückzuschreiben, indem am Wiederherstellungsstandort ein neuer Zielsystem konfiguriert wurde. Mit den Skripten wurden Sicherungsversionen der IBM Spectrum Protect-Datenbank, der Serveroptionsdatei (dsmserv.opt), der Protokolldatei für Datenträger (volhist.out) und der Einheitenkonfigurationsdatei (devconfig.out) an ihre ursprünglichen Positionen auf dem Wiederherstellungsserver kopiert. Nach der Ausführung der Skripts werden die neu erstellten, leeren Verzeichnisse auf dem Wiederherstellungsserver angezeigt.

Wenn Sie versuchen, einen Verzeichniscontainerspeicherpool mithilfe eines Zielreplikationsservers zu reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Zielreplikationsserver ist nicht verfügbar.
- Der Zielspeicherpool ist beschädigt.
- Es tritt ein Netzausfall auf.

Wenn Sie einen Verzeichniscontainerspeicherpool mithilfe von Containerkopienpools reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Containerkopienpeicherpool ist nicht verfügbar.
- Der Containerkopienpeicherpool ist beschädigt.
- Die Datenträger in Containerkopienpeicherpools sind nicht verfügbar oder beschädigt.

## Vorgehensweise

---

1. Markieren Sie alle Datenbereiche in dem Containerspeicherpool als beschädigt, indem Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=MARKDAMAGED für den Containerspeicherpool auf Speicherpoolebene ausgeben. Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 zu prüfen und als beschädigt zu markieren, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1 action=markdamaged
```

2. Wenn Sie den Verzeichniscontainerspeicherpool sowohl mit Containerkopienpeicherpools vor Ort als auch mit Containerkopienpeicherpools an einem anderen Standort geschützt hatten, geben Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters ACCESS=UNAVAILABLE für die Kopie des Containerkopienpeicherpools vor Ort aus.
3. Wenn sich die ausgelagerten Datenträger in Containerkopienpeicherpools wieder vor Ort befinden, stellen Sie diese in das Speicherarchiv zurück, indem Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters STATUS=PRIVATE ausgeben. Wenn die Banddatenträger jetzt vor Ort transportiert werden, sind Sie für die Reparatur beschädigter Bereiche mithilfe der Banddatenträger in Containerkopienpeicherpools vorbereitet, falls die beschädigten Bereiche nicht mithilfe des Zielreplikationsservers repariert werden können.
4. Aktualisieren Sie den Status der Datenträger, indem Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters ACCESS=READWRITE ausgeben.
5. Reparieren Sie den Speicherpool, indem Sie den Befehl REPAIR STGPOOL unter Angabe des Parameters SRCLOCATION=REPLSERVER ausgeben. Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 mithilfe eines Zielreplikationsservers zu reparieren, geben Sie den folgenden Befehl aus:

```
repair stgpool stgpool1 srclocation=replserver
```

Wenn Sie den Befehl REPAIR STGPOOL ausgeben, werden die beschädigten Bereiche unmittelbar nach der Reparatur von dem Datenträger gelöscht. Die beschädigten Bereiche werden nicht gemäß dem im Parameter REUSEDELAY angegebenen Wert beibehalten.

6. Wenn Sie nicht die Blueprint-Konfigurationsscripts für die Konfiguration Ihres Zielreplikationsservers verwendet hatten, stimmt die Dateistruktur auf dem Zielreplikationsserver möglicherweise nicht mit den in der Datenbank gespeicherten Informationen überein. Entfernen Sie wahlweise die Speicherpoolverzeichnisse, die auf dem Zielreplikationsserver nicht vorhanden sind. Geben Sie den Befehl DELETE STGPOOLDIRECTORY aus, um Verzeichnisse zu löschen, die auf dem Zielreplikationsserver nicht vorhanden sind.
7. Stellen Sie sicher, dass keine weiteren beschädigten Bereiche vorhanden sind, indem Sie den Befehl QUERY DAMAGED ausgeben.
8. Wenn die beschädigten Bereiche nicht mithilfe des Zielreplikationsservers repariert werden können, können Sie die beschädigten Bereiche mithilfe von ausgelagerten Containerkopienpeicherpools reparieren. Anweisungen finden Sie in Speicherpools mithilfe von Datenträgern in Containerkopienpeicherpools nach einem Katastrophenfall reparieren.
9. Stellen Sie sicher, dass keine weiteren beschädigten Bereiche vorhanden sind, indem Sie den Befehl QUERY DAMAGED erneut ausgeben.
10. Wenn eine Beschädigung erkannt wird und deduplizierte Speicherbereiche nicht mithilfe des Replikationsservers repariert werden können, ist eine Reparatur dennoch möglich. In einigen Fällen sendet der Clientknoten Daten im Rahmen einer Sicherungsoperation erneut und die beschädigten Bereiche werden repariert. Warten Sie für die Dauer von zwei Sicherungszyklen, um die Ausführung von Clientsicherungen zu ermöglichen. Führen Sie im Anschluss an zwei Sicherungszyklen die folgenden Schritte aus:
  - a. Um zu prüfen, ob die Beschädigung repariert wurde, geben Sie den Befehl QUERY DAMAGED erneut aus.
  - b. Um Objekte zu entfernen, die sich auf beschädigte Daten beziehen, geben Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=REMOVEDAMAGED aus. Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL1 zu prüfen und beschädigte Objekte zu entfernen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1 action=removedamaged
```

11. Wiederholen Sie diese Prozedur, um alle Ihre Speicherpools zu reparieren.

## Beschädigten Banddatenträger im Containerkopierspeicherpool ersetzen

---

Wenn ein Banddatenträger, der eine Kopie deduplizierter Datenbereiche in einem Containerkopierspeicherpool speichert, beschädigt wird, können Sie den Datenträger ersetzen.

### Vorgehensweise

---

1. Löschen Sie den beschädigten Banddatenträger, indem Sie den Befehl DELETE VOLUME unter Angabe des Parameters DISCARDDATA=YES ausgeben.

Um beispielsweise einen Datenträger mit dem Namen VOLUME1 zu löschen, geben Sie den folgenden Befehl aus:

```
delete volume volume1 discarddata=yes
```

2. Schützen Sie Datenbereiche im Verzeichniscontainerspeicherpool, indem Sie die Daten auf vorhandene Datenträger im Containerkopierspeicherpool kopieren. Geben Sie auf dem Quellenserver den Befehl PROTECT STGPOOL aus.

Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen POOL1 zu schützen, geben Sie den folgenden Befehl aus:

```
protect stgpool pool1 type=local
```

#### Zugehörige Verweise:

PROTECT STGPOOL (Speicherpooldaten schützen)

DELETE VOLUME (Speicherpooldatenträger löschen)

## Serverbefehle, -optionen und -dienstprogramme

---

Verwenden Sie Befehle, um den Server zu verwalten und zu konfigurieren, Optionen, um den Server anzupassen, und Dienstprogramme, um spezielle Tasks auszuführen, wenn der Server nicht aktiv ist.

- Server von der Befehlszeile aus verwalten  
IBM Spectrum Protect stellt mehrere verschiedene Befehlszeilenschnittstellen für die Verwaltung von IBM Spectrum Protect-Servern zur Verfügung.
- Verwaltungsbefehle  
Verwaltungsbefehle sind zum Verwalten und Konfigurieren des Servers verfügbar.
- Serveroptionen  
Bei der Installation stellt IBM Spectrum Protect eine Serveroptionsdatei zur Verfügung, die eine Reihe von Standardoptionen zum Starten des Servers enthält.
- Serverdienstprogramme  
Verwenden Sie Serverdienstprogramme, um spezielle Tasks auf dem Server auszuführen, während der Server nicht aktiv ist.
- Rückkehrcodes für die Verwendung in IBM Spectrum Protect-Scripts  
Sie können IBM Spectrum Protect-Scripts schreiben, die Rückkehrcodes verwenden, um den Fortschritt der Scriptverarbeitung zu bestimmen. Die Rückkehrcodes können eine von drei Wertigkeiten haben: OK, WARNING, ERROR.
- Einheitendienstprogramme  
Für Tasks, die sich auf das Konfigurieren von Speichereinheiten für den IBM Spectrum Protect-Server beziehen, können Einheitendienstprogramme verwendet werden.
- Server-Scripts und Makros für die Automatisierung  
Allgemeine Verwaltungstasks können durch das Erstellen von IBM Spectrum Protect-Server-Scripts oder Makros des Verwaltungsclients automatisiert werden. Server-Scripts werden in der Serverdatenbank gespeichert; ihre Ausführung kann mithilfe eines Befehls für Verwaltungszeitpläne geplant werden. Makros des Verwaltungsclients werden als Dateien auf dem Verwaltungsclient gespeichert.

## Server von der Befehlszeile aus verwalten

---

IBM Spectrum Protect stellt mehrere verschiedene Befehlszeilenschnittstellen für die Verwaltung von IBM Spectrum Protect-Servern zur Verfügung.

### Informationen zu diesem Vorgang

---

Die folgenden Befehlszeilenschnittstellen sind verfügbar:

Verwaltungsbefehlszeilenclient

Der Verwaltungsbefehlszeilenclient ist ein Programm, das auf einem Dateiserver, einer Workstation oder einem Großrechner ausgeführt werden kann. Er wird im Rahmen des IBM Spectrum Protect-Serverinstallationsprozesses installiert. Auf den Verwaltungsklient kann über Remotezugriff zugegriffen werden.

Auf dem Verwaltungsklient können Sie alle Serverbefehle ausgeben.

#### Serverkonsole

Die Serverkonsole ist ein Befehlszeilenfenster auf dem System, auf dem der Server installiert ist. Daher müssen Sie sich am physischen Standort des Serversystems befinden, um die Serverkonsole zu verwenden.

Im Vergleich zum Verwaltungsklient ist die Funktionalität der Serverkonsole begrenzt. Sie können bestimmte Befehle nicht an der Serverkonsole ausgeben und Sie können Befehle nicht an andere Server weiterleiten. Außerdem können Sie nicht angeben, dass bestimmte Befehle verarbeitet werden, bevor andere Befehle ausgegeben werden können. Diese Einschränkung kann jedoch nützlich sein, wenn Sie beispielsweise zwei Befehle in schneller Aufeinanderfolge ausführen möchten.

#### Operations Center-Befehlszeile

Sie können über das Operations Center auf die IBM Spectrum Protect-Befehlszeile zugreifen. Möglicherweise möchten Sie diese Befehlszeile verwenden, um Serverbefehle für die Ausführung bestimmter IBM Spectrum Protect-Tasks auszugeben, die im Operations Center nicht unterstützt werden.

Mit Server-Scripts können allgemeine Verwaltungstasks automatisiert werden. Ein Makro ist eine Datei, die IBM Spectrum Protect-Verwaltungsbefehle enthält. Wenn Sie den Befehl MACRO ausgeben, verarbeitet der Server alle Befehle in der Makrodatei in Folge, einschließlich der Befehle, die in allen verschachtelten Makros enthalten sind.

- **Befehle mit dem Verwaltungsklient ausgeben**  
Der Verwaltungsbefehlszeilenclient ist ein Programm, das auf einem Dateiserver, einer Workstation oder einem Großrechner ausgeführt werden kann.
- **Befehle im Operations Center ausgeben**  
In der Operations Center-Befehlszeilenschnittstelle können Sie Befehle ausgeben, um IBM Spectrum Protect-Server zu verwalten, die als Hub-Server oder Peripherieserver konfiguriert sind.
- **Befehle von der Serverkonsole ausgeben**  
IBM Spectrum Protect stellt eine Benutzer-ID mit dem Namen SERVER\_CONSOLE zur Verfügung, mit der Sie Befehle ausgeben und den Server von der Serverkonsole aus verwalten können, nachdem IBM Spectrum Protect installiert wurde. Bei der Installation wird SERVER\_CONSOLE automatisch als Administrator registriert und erhält die Systemberechtigung.
- **Verwaltungsbefehle eingeben**  
Befehle bestehen aus Befehlsnamen und normalerweise aus Parametern und Variablen. Syntaxdiagramme zeigen die Regeln, die bei der Eingabe von Befehlen zu befolgen sind.
- **Befehlsverarbeitung steuern**  
Einige IBM Spectrum Protect-Befehle können nacheinander oder gleichzeitig mit anderen Befehlen ausgeführt werden. Sie können auch Befehle von einem Server an andere Server für die Verarbeitung weiterleiten.
- **Tasks gleichzeitig auf mehreren Servern ausführen**  
Mit der Befehlsweiterleitung können Sie Befehle an einen oder an mehrere Server zur Verarbeitung weiterleiten und dann die Ausgabe von diesen Servern sammeln.
- **Berechtigungsklassen für Befehle**  
Die einem Administrator über die Berechtigungsklasse erteilte Berechtigung bestimmt, welche Verwaltungsbefehle der Administrator ausgeben kann.

#### **Zugehörige Konzepte:**

Server-Scripts

#### **Zugehörige Verweise:**

Makros des Verwaltungsklients

## Befehle mit dem Verwaltungsklient ausgeben

---

Der Verwaltungsbefehlszeilenclient ist ein Programm, das auf einem Dateiserver, einer Workstation oder einem Großrechner ausgeführt werden kann.

### Informationen zu diesem Vorgang

---

Stellen Sie sicher, dass Ihr Verwaltungsklient und Ihr Server in kompatiblen Sprachen ausgeführt werden. Weitere Informationen zu Optionen für Sprache und Locale befinden sich in LANGUAGE. Verwenden Ihr Client und Ihr Server unterschiedliche Sprachen, können die von IBM Spectrum Protect generierten Nachrichten unverständlich sein.

Tipp: Textzeichenfolgen, die vom Client an den Server gesendet werden, sind nicht von der Einstellung der Serversprache abhängig. Der Text wird ordnungsgemäß angezeigt, wenn der Verwaltungsklient beim Senden der Zeichenfolge und beim Empfangen der Zeichenfolge in derselben Locale ausgeführt wird.

Beispiel: Angenommen, Sie aktualisieren ein Knotenkontaktfeld mit einem Wert, der nationale Sonderzeichen enthält (`update node myNode contact=NLcontact_info`), und fragen später den Knoten ab (`query node myNode format=detailed`). Wenn der Client bei der Aktualisierung und bei der Abfrage in derselben Locale ausgeführt wird, wird `NLcontact_info` korrekt angezeigt. Wird der Client in einer Locale ausgeführt, wenn Sie das Knotenkontaktfeld aktualisieren, und wird der Client in einer anderen Locale ausgeführt, wenn der Knoten abgefragt wird, wird `NLcontact_info` möglicherweise nicht korrekt angezeigt.

- **Verwaltungsclient starten und stoppen**  
Verwenden Sie den Befehl `DSMADMC`, um eine Verwaltungsclientsitzung zu starten.
- **Serveraktivitäten über den Verwaltungsclient überwachen**  
Um IBM Spectrum Protect-Aktivitäten, wie beispielsweise die Serverumlagerung und Clientanmeldungen, zu überwachen, führen Sie den Verwaltungsclient im Konsolenmodus aus. Im Konsolenmodus können keine Verwaltungsbefehle eingegeben werden.
- **Mounts für austauschbare Datenträger über den Verwaltungsclient überwachen**  
Um die Bereitstellung und das Aufheben der Bereitstellung austauschbarer Datenträger zu überwachen, führen Sie den Verwaltungsclient im Mountmodus aus. Wenn der Client im Mountmodus ausgeführt wird, können keine Verwaltungsbefehle eingegeben werden.
- **Einzelne Befehle mit dem Verwaltungsclient verarbeiten**  
Den Stapelbetrieb verwenden, um einen einzelnen Verwaltungsbefehl einzugeben. Die Verwaltungsclientsitzung wird automatisch beendet, wenn der Befehl verarbeitet wurde.
- **Eine Serie von Befehlen des Verwaltungsclients verarbeiten**  
Sie können den interaktiven Modus verwenden, um eine Serie von Verwaltungsbefehlen zu verarbeiten.
- **Ausgabe von Befehlen formatieren**  
IBM Spectrum Protect formatiert die Befehlsverarbeitungsausgabe entsprechend der Anzeigen- oder Fensterbreite.
- **Befehlsausgabe an einer angegebenen Position sichern**  
Die häufigste Verwendung der Ausgabeumleitung ist das Sichern der Ausgabe von Abfragebefehlen in einer angegebenen Datei oder in einem Programm. Sie können dann den Inhalt der Datei durchsuchen oder in manchen Fällen den Inhalt drucken.
- **Verwaltungsclientoptionen**  
In allen Verwaltungsclientmodi können Sie Optionen verwenden, um die Antworten der Verwaltungsclientsitzungen zu ändern.

## Verwaltungsclient starten und stoppen

---

Verwenden Sie den Befehl `DSMADMC`, um eine Verwaltungsclientsitzung zu starten.

### Informationen zu diesem Vorgang

---

Der IBM Spectrum Protect-Server muss aktiv sein, bevor ein Verwaltungsclient eine Verbindung herstellen kann.

### Vorgehensweise

---

- Um eine Verwaltungsclientsitzung im Befehlszeilenmodus zu starten, geben Sie diesen Befehl an Ihrer Workstation ein:

```
dsmadmc -id=admin -password=admin -dataonly=yes
```

Wenn der Befehl `DSMADMC` mit den Optionen `-ID` und `-PASSWORD` (siehe oben) eingegeben wird, werden Sie nicht zur Eingabe einer Benutzer-ID und eines Kennworts aufgefordert.

- Um eine Verwaltungsclientsitzung im Befehlszeilenmodus zu stoppen, geben Sie den folgenden Befehl ein:

```
quit
```

- Um einen Befehl `DSMADMC` zu unterbrechen, bevor seine Verarbeitung durch den IBM Spectrum Protect-Server beendet wird, verwenden Sie den UNIX-Befehl `kill -9` in einer verfügbaren Befehlszeile. Drücken Sie nicht `Strg+C`, da dies während der Beendigung der Sitzung zu nicht erwarteten Ergebnissen führen kann.

## Serveraktivitäten über den Verwaltungsclient überwachen

---

Um IBM Spectrum Protect-Aktivitäten, wie beispielsweise die Serverumlagerung und Clientanmeldungen, zu überwachen, führen Sie den Verwaltungsclient im Konsolenmodus aus. Im Konsolenmodus können keine Verwaltungsbefehle eingegeben werden.

### Vorgehensweise

---

- Um eine Verwaltungsclientsitzung im Konsolenmodus zu starten, geben Sie den folgenden Befehl ein:

```
dsmadmc -consolemode
```



Wenn die Authentifizierung für den Server aktiviert ist, muss ein Kennwort eingegeben werden. Soll keine Eingabeaufforderung für Benutzer-ID und Kennwort erfolgen, geben Sie den Befehl DSMADMC mit den Optionen -ID und -PASSWORD ein.

- Um eine Verwaltungsclientsitzung im Konsolenmodus zu beenden, verwenden Sie eine Tastaturunterbrechungsfolge.

| Betriebssystem          | Unterbrechungsfolge                  |
|-------------------------|--------------------------------------|
| UNIX- und Linux-Clients | Strg+C                               |
| Windows-Clients         | Strg+C oder Strg+Unterbrechungstaste |

## Mounts für austauschbare Datenträger über den Verwaltungsclient überwachen

Um die Bereitstellung und das Aufheben der Bereitstellung austauschbarer Datenträger zu überwachen, führen Sie den Verwaltungsclient im Mountmodus aus. Wenn der Client im Mountmodus ausgeführt wird, können keine Verwaltungsbefehle eingegeben werden.

### Vorgehensweise

- Um eine Verwaltungsclientsitzung im Mountmodus zu starten, geben Sie den folgenden Befehl ein:

```
dsmadmc -mountmode
```

Wenn die Authentifizierung für den Server aktiviert ist, muss ein Kennwort eingegeben werden. Soll keine Eingabeaufforderung für Benutzer-ID und Kennwort erfolgen, geben Sie den Befehl DSMADMC mit den Optionen -ID und -PASSWORD ein.

- Um eine Verwaltungsclientsitzung im Mountmodus zu beenden, verwenden Sie eine Tastaturunterbrechungsfolge.

| Betriebssystem          | Unterbrechungsfolge                  |
|-------------------------|--------------------------------------|
| UNIX- und Linux-Clients | Strg+C                               |
| Windows-Clients         | Strg+C oder Strg+Unterbrechungstaste |

## Einzelne Befehle mit dem Verwaltungsclient verarbeiten


Den Stapelbetrieb verwenden, um einen einzelnen Verwaltungsbefehl einzugeben. Die Verwaltungsclientsitzung wird automatisch beendet, wenn der Befehl verarbeitet wurde.

### Vorgehensweise

Um eine Verwaltungsclientsitzung im Stapelmodus zu starten, verwenden Sie den folgenden Befehl: `dsmadmc Serverbefehl`

Soll keine Eingabeaufforderung für Benutzer-ID und Kennwort erfolgen, können Sie den Befehl DSMADMC mit den Optionen -ID und -PASSWORD eingeben.

Im Stapelbetrieb muss der vollständige Befehl in einer Zeile eingegeben werden. Passt ein Befehl nicht in eine Zeile, ist er mit Hilfe eines Makros oder einer Prozedur einzugeben. Wird im Stapelbetrieb ein Parameter mit einer Zeichenfolge angegeben, muss die Zeichenfolge in einfache Anführungszeichen ( ' ' ) in dem Makro eingeschlossen werden. Verwenden Sie keine Anführungszeichen für Befehle im Stapelbetrieb, da Ihr Betriebssystem die Anführungszeichen möglicherweise nicht korrekt syntaktisch analysiert.

 Windows-Betriebssysteme Sie können diese Einschränkung bezüglich der Anführungszeichen im Stapelbetrieb für Windows-Clients umgehen, indem Sie das Backslash-(\)-Escapezeichen verwenden. Für den Parameter OBJECTS des Befehls DEFINE CLIENTACTION könnten Sie beispielsweise die Zeichenfolge mit dem Zeichen \ vor den Anführungszeichen in dem Befehl eingeben.

```
dsmadmc -id=admin -password=admin define clientaction test_node domain=test_dom  
action=restore objects='\"C:\program files\test\*\"'
```

## Eine Serie von Befehlen des Verwaltungsclients verarbeiten

Sie können den interaktiven Modus verwenden, um eine Serie von Verwaltungsbefehlen zu verarbeiten.

### Informationen zu diesem Vorgang

Um eine Verwaltungsclientsitzung im interaktiven Modus zu starten, muss eine Serversitzung verfügbar sein. Um die Verfügbarkeit von Serversitzungen für Verwaltungssitzungen und Clientknotensitzungen sicherzustellen, wird der interaktive Modus des Verwaltungsclients

unterbrochen, wenn eine (oder mehrere) der folgenden Bedingungen zutrifft:

- Der Server wurde mit dem Befehl HALT gestoppt.
- Während der mit der Serveroption IDLETIMEOUT angegebenen Zeitspanne wurden keine Befehle von der Verwaltungsclientsitzung ausgegeben.
- Die Verwaltungsclientsitzung wurde mit dem Befehl CANCEL SESSION abgebrochen.

## Vorgehensweise

Um eine Verwaltungssitzung im interaktiven Modus zu starten, verwenden Sie den folgenden Befehl: `dsmadmc`

Bei der Verwendung des interaktiven Modus können Fortsetzungszeichen verwendet werden. Weitere Informationen befinden sich in Fortsetzungszeichen für die Eingabe langer Befehle verwenden.

Die Verwaltungsclientsitzung kann automatisch erneut gestartet werden, indem jedesmal ein anderer Befehl eingegeben wird, wenn die Bedienungsführung `tsm: Servername >` angezeigt wird.

Geben Sie einen Serverbefehl nicht mit dem Befehl DSMADMC ein. Der Verwaltungsclient würde dann im Stapelbetrieb und nicht im interaktiven Modus gestartet. Geben Sie zum Beispiel Folgendes nicht ein:

```
dsmadmc Serverbefehl
```

## Ausgabe von Befehlen formatieren

IBM Spectrum Protect formatiert die Befehlsverarbeitungsausgabe entsprechend der Anzeigen- oder Fensterbreite.

### Vorgehensweise

- Reicht die Anzeigen- oder Fensterbreite für eine horizontale Anzeige der Ausgabe nicht aus, zeigt IBM Spectrum Protect die Informationen vertikal angeordnet an.
- Sie können die Ausgabe von QUERY-Befehlen mit den Verwaltungsoptionen DISPLAYMODE und OUTFILE formatieren.

## Befehlsausgabe an einer angegebenen Position sichern

Die häufigste Verwendung der Ausgabeumleitung ist das Sichern der Ausgabe von Abfragebefehlen in einer angegebenen Datei oder in einem Programm. Sie können dann den Inhalt der Datei durchsuchen oder in manchen Fällen den Inhalt drucken.

### Informationen zu diesem Vorgang

Auf einigen Betriebssystemen können Sie die Ausgabe eines Befehls mithilfe von Sonderzeichen wie z. B. `>`, `>>` und `|` umleiten. Umleitungszeichen leiten die Ausgabe eines Befehls in eine angegebene Datei oder an ein angegebenes Programm und nicht an den Bildschirm. Die Ausgabe eines Befehls kann durch Eingabe von Umleitungszeichen am Ende des Befehls gesichert werden. Um die Ausgabe umzuleiten, lassen Sie ein Leerzeichen zwischen dem Umleitungszeichen und dem Datei- oder Programmnamen. Siehe die nachfolgenden Beispiele.

Bei der Umleitung der Ausgabe sind die Namenskonventionen des Betriebssystems zu beachten, auf dem der Verwaltungsclient ausgeführt wird.

### Vorgehensweise

Die Beispiele in der folgenden Tabelle zeigen, wie die Befehlsausgabe umgeleitet wird.

| Task   | Prozedur  |
|--|---|
| Die Ausgabe eines Befehls QUERY DOMAIN im Stapelbetrieb oder im interaktiven Modus in eine neue Datei umleiten.                  | Verwenden Sie ein einzelnes Größer-als-Zeichen ( <code>&gt;</code> ), um die Ausgabe in eine neue Datei umzuleiten oder eine vorhandene Datei zu überschreiben:<br><pre>dsmadmc -id=xxx -pa=xxx query domain acctg &gt; dominfo.acc</pre> |
| Die Ausgabe eines Befehls QUERY DOMAIN im Stapelbetrieb oder im interaktiven Modus an das Ende einer vorhandenen Datei anhängen. | Verwenden Sie zwei aufeinanderfolgende Größer-als-Zeichen ( <code>&gt;&gt;</code> ), um die Ausgabe an das Ende einer vorhandenen Datei anzuhängen:<br><pre>dsmadmc -id=xxx -pa=xxx query domain acctg &gt;&gt; dominfo.acc</pre>         |

| Task   | Prozedur   |
|--|--|
| Die gesamte Ausgabe von einer Verwaltungsclientsitzung im Konsolenmodus an ein Programm mit dem Namen filter.exe umleiten. | Verwenden Sie den vertikalen Balken ( ), um die gesamte Ausgabe für eine Sitzung an ein Programm umzuleiten:<br><pre>dsmadmc -console -id=admin -password=xxx   filter.exe</pre> Das Programm kann so konfiguriert werden, dass es die Ausgabe auf einzelne Nachrichten überprüft und die entsprechende Aktion ausführt, wie beispielsweise das Senden von Post an einen anderen Benutzer. |
| Die gesamte Ausgabe im Konsolenmodus an eine Datei umleiten  | Geben Sie die Option -OUTFILE mit einem Zieldateinamen an. Mit dem folgenden Befehl wird beispielsweise die gesamte Ausgabe an die Datei save.out umgeleitet:<br><pre>dsmadmc -id=sullivan -password=secret -consolemode -outfile=save.out</pre>   |

## Verwaltungsclientoptionen

In allen Verwaltungsclientmodi können Sie Optionen verwenden, um die Antworten der Verwaltungsclientsitzungen zu ändern.

### Syntax

```

    .----- .
    v       |
>>-DSMADMC-----+-----+-----+-----+-----+-----+-----+-----<
                '-Verwaltungsclientoption-'   '-Serverbefehl-'

```

### Beispiel für die Verwendung von Verwaltungsclientoptionen

Sie können den Befehl DSMADMC mit Ihrer Benutzer-ID und Ihrem Kennwort eingeben, indem Sie die Optionen -ID und -PASSWORD verwenden, sodass Sie nicht zur Eingabe dieser Informationen aufgefordert werden. Soll IBM Spectrum Protect die gesamte Ausgabe in eine Datei umleiten, die Option -OUTFILE mit einem Zieldateinamen angeben. Soll beispielsweise der Befehl QUERY NODE im Stapelbetrieb ausgegeben werden und soll die Ausgabe in die Datei SAVE.OUT umgeleitet werden, Folgendes eingeben:

```
dsmadmc -id=sullivan -password=secret -outfile=save.out query node
```

### Optionen

Verwaltungsclientoptionen können mit dem Befehl DSMADMC angegeben werden und sind nur in einer Verwaltungsclientsitzung gültig. Die Option kann in Großbuchstaben, Kleinbuchstaben oder in einer beliebigen Kombination aus beidem eingegeben werden. Großbuchstaben kennzeichnen die kürzeste zulässige Abkürzung. Steht eine Option nur in Großbuchstaben, kann sie nicht abgekürzt werden.

#### -ALWAYSPrompt

Gibt an, dass eine Eingabeaufforderung angezeigt wird, wenn die Eingabe über die Tastatur erfolgt oder wenn sie umgeleitet wird (zum Beispiel aus einer Datei). Wird diese Option nicht angegeben und wird die Eingabe umgeleitet, wird die Eingabeaufforderung nicht geschrieben.

Wird die Eingabe umgeleitet, wird nur die Befehlsausgabe angezeigt. Wird diese Option angegeben, werden die Eingabeaufforderung und die Befehlsausgabe angezeigt.

#### -CHECKAlias halt

Ermöglicht es dem Verwaltungsclient, einen Aliasnamen für den Befehl HALT zu erkennen, der in der Serveroption ALIASHALT definiert ist. Für ausführliche Informationen siehe ALIASHALT.

#### -COMMA delimited

Gibt an, dass Ausgabe einer Serverabfrage in Tabellenform als Zeichenfolgen formatiert werden soll, die durch Kommas getrennt werden, und nicht im lesbaren Format. Diese Option soll hauptsächlich für die Umleitung der Ausgabe einer SQL-Abfrage (Befehl SELECT) verwendet werden. Das Format mit Kommatrennzeichen ist ein Standarddatenformat, das von vielen produktübergreifenden Programmen verarbeitet werden kann, einschließlich Tabellenkalkulationen, Datenbanken und Berichtsgeneratoren.

#### -CONsole mode

Gibt an, dass IBM Spectrum Protect im Konsolenmodus ausgeführt wird. Der größte Teil der Ausgabe der Serverkonsole wird am Bildschirm angezeigt. Die Ausnahme sind Elemente, wie beispielsweise Antworten auf Abfragebefehle, die an der Konsole ausgegeben werden, Traceausgabe oder alle Systemnachrichten, die an der Konsole angezeigt werden.

#### -DATAONLY=NO oder YES

Gibt an, ob Informationen zur Produktversion und Ausgabespaltenüberschriften mit der Ausgabe angezeigt werden. Der Standardwert ist NO.

NO

Gibt an, dass Informationen zur Produktversion und Ausgabespaltenüberschriften angezeigt werden.

YES

Gibt an, dass Informationen zur Produktversion und Ausgabespaltenüberschriften nicht angezeigt werden.

-DISPLAYmode=LIST oder TABLE

Sie können die QUERY-Ausgabe im Tabellen- oder Listenformat erzwingen, unabhängig von der Spaltenbreite des Befehlszeilenfensters.

Wird die Option -DISPLAYMODE verwendet und soll die Ausgabe in eine Datei gestellt werden, geben Sie nicht die Option -OUTFILE an. Verwenden Sie die Umleitung, um in die Datei zu schreiben.

-ID=Benutzer-ID

Gibt die Benutzer-ID des Administrators an.

-Itemcommit

Gibt an, dass IBM Spectrum Protect Befehle in einer Prozedur oder in einem Makro festschreibt, sobald die einzelnen Befehle verarbeitet werden.

-MOUNTmode

Gibt an, dass IBM Spectrum Protect im Lademodus aktiv ist. Alle Serverladenachrichten für austauschbare Datenträger werden angezeigt.

-NEWLINEAFTERPrompt

Gibt an, dass ein Zeilenvorschubzeichen nach der Eingabeaufforderung geschrieben wird, und Befehle, die über die Tastatur eingegeben werden, unter der Bedienungsführung angezeigt werden. Wird diese Option nicht angegeben, werden die über die Tastatur eingegebenen Befehle rechts neben der Eingabeaufforderung angezeigt.

-NOConfirm

Gibt an, dass IBM Spectrum Protect vor der Verarbeitung von Befehlen, die sich auf die Verfügbarkeit des Servers oder die vom Server verwalteten Daten auswirken, keine Bestätigung anfordern soll.

-OUTfile

Gibt an, dass die Ausgabe von einer Serverabfrage in einer Zeile angezeigt wird. Wenn die Ausgabe in einer Zeile die Spaltenbreite überschreitet, die vom Server definiert ist, wird die Ausgabe in mehreren Zeilen angezeigt. Diese Option ist nur im Stapelbetrieb verfügbar.

-OUTfile=Dateiname

Gibt an, dass die Ausgabe von einer Serverabfrage in eine angegebene Datei umgeleitet wird. Im Stapelbetrieb wird die Ausgabe in eine angegebene Datei umgeleitet und das Format der Ausgabe entspricht dem Format der Ausgabe auf dem Bildschirm.



In Sitzungen, die im interaktiven Modus, Konsolenmodus oder Mountmodus ausgeführt werden, wird die Ausgabe am Bildschirm angezeigt.



-PAssword=Kennwort

Gibt das Kennwort des Administrators an.

-Quiet

Gibt an, dass IBM Spectrum Protect keine Standardausgabenachrichten anzeigt. Bei Verwendung dieser Option werden bestimmte Fehlermeldungen weiterhin angezeigt.

 AIX-Betriebssysteme  Linux-Betriebssysteme-SERVERADDRESS

 AIX-Betriebssysteme  Linux-Betriebssysteme Gibt die Serverzeilengruppe in der Datei dsm.sys an. Der Client verwendet die Serverzeilengruppe, um den Server zu bestimmen, zu dem die Verbindung hergestellt wird. Die Option SERVERADDRESS wird nur von Verwaltungsclients unterstützt, die unter den Betriebssystemen UNIX, Linux und Macintosh ausgeführt werden.

-TABdelimited

Gibt an, dass Ausgabe einer Serverabfrage in Tabellenform als Zeichenfolgen formatiert werden soll, die durch Tabulatoren getrennt werden, und nicht im lesbaren Format. Diese Option soll hauptsächlich für die Umleitung der Ausgabe einer SQL-Abfrage (Befehl SELECT) verwendet werden. Das Format mit Tabulatortrennzeichen ist ein Standarddatenformat, das von vielen produktübergreifenden Programmen verarbeitet werden kann, einschließlich Tabellenkalkulationen, Datenbanken und Berichtsgeneratoren.

-TCPport

Gibt eine TCP/IP-Anschlussadresse für einen IBM Spectrum Protect-Server an. Die Option TCPPORT wird nur von Verwaltungsclients unterstützt, die unter Windows-Betriebssystemen ausgeführt werden, und ist in der Befehlszeile des Windows-Verwaltungsclients gültig.

-TCPserveraddress

Gibt eine TCP/IP-Serveradresse für einen IBM Spectrum Protect-Server an. Die Option TCPSERVERADDRESS wird nur von Verwaltungsclients unterstützt, die unter Windows-Betriebssystemen ausgeführt werden, und ist in der Befehlszeile des Windows-Verwaltungsclients gültig.

Zusätzlich zu den hier aufgeführten Optionen können auch alle Optionen in der Clientoptionsdatei angegeben werden. Jede Option muss mit einem Silbentrennungsstrich beginnen und durch ein Leerzeichen begrenzt werden.


## Befehle im Operations Center ausgeben

---

In der Operations Center-Befehlszeilenschnittstelle können Sie Befehle ausgeben, um IBM Spectrum Protect-Server zu verwalten, die als Hub-Server oder Peripherieserver konfiguriert sind.

### Vorgehensweise

---

Um die Befehlszeilenschnittstelle zu öffnen, bewegen Sie den Mauszeiger über das Globussymbol  in der Operations Center-Menüleiste und klicken Sie auf Command Builder.

## Befehle von der Serverkonsole ausgeben

---

IBM Spectrum Protect stellt eine Benutzer-ID mit dem Namen SERVER\_CONSOLE zur Verfügung, mit der Sie Befehle ausgeben und den Server von der Serverkonsole aus verwalten können, nachdem IBM Spectrum Protect installiert wurde. Bei der Installation wird SERVER\_CONSOLE automatisch als Administrator registriert und erhält die Systemberechtigung.

### Informationen zu diesem Vorgang

---

Wenn Sie über Systemberechtigung verfügen, können Sie neue Berechtigungen für die Benutzer-ID SERVER\_CONSOLE entziehen oder erteilen. Sie können keine der folgenden Aktionen ausführen:

- Benutzer-ID SERVER\_CONSOLE registrieren oder aktualisieren
- Benutzer-ID SERVER\_CONSOLE sperren oder entsperren
- Benutzer-ID SERVER\_CONSOLE umbenennen
- Benutzer-ID SERVER\_CONSOLE löschen
- Befehle von der Benutzer-ID SERVER\_CONSOLE weiterleiten

Nicht alle IBM Spectrum Protect-Befehle werden von der Serverkonsole unterstützt. Sie können den Parameter WAIT nicht von der Serverkonsole aus angeben.

## Verwaltungsbefehle eingeben

---

Befehle bestehen aus Befehlsnamen und normalerweise aus Parametern und Variablen. Syntaxdiagramme zeigen die Regeln, die bei der Eingabe von Befehlen zu befolgen sind.

### Informationen zu diesem Vorgang

---

Um die Hilfe für Befehlszeile für Serverbefehle anzuzeigen, die eindeutige Namen haben, können Sie `help Befehlsname` eingeben, wobei *Befehlsname* der Name des Serverbefehls ist, für den Informationen angezeigt werden sollen. Soll beispielsweise Hilfe für den Befehl REGISTER NODE angezeigt werden, geben Sie `help register node` ein. Die Befehlssyntax und die Parameterbeschreibungen werden in der Ausgabe angezeigt.

Sie können auch `help`, gefolgt von der Nummer des Hilfethemas für den Befehl eingeben. Die Nummern der Hilfethemen sind im Inhaltsverzeichnis für die Befehlszeilenhilfe aufgelistet. Beispiel:

```
3.0 Verwaltungsbefehle
  3.46 REGISTER
    3.46.1 REGISTER ADMIN (Administrator registrieren)
    3.46.2 REGISTER LICENSE (Neue Lizenz registrieren)
    3.46.3 REGISTER NODE (Knoten registrieren)
```

Soll Hilfe für den Befehl REGISTER NODE angezeigt werden, geben Sie Folgendes ein:

```
help 3.46.3
```

Verwenden Sie die Nummern der Hilfethemen, um die Befehlszeilenhilfe für Unterbefehle anzuzeigen. DEFINE DEVCLASS ist ein Beispiel eines Befehls, der Unterbefehle hat. Sie können beispielsweise den Befehl DEFINE DEVCLASS für die Einheitenklasse 3590 und für die Einheitenklasse 3592 angeben:

```
3.0 Verwaltungsbefehle
  ...
  3.13.10 DEFINE DEVCLASS (Einheitenklasse definieren)
    3.13.10.1 DEFINE DEVCLASS (Einheitenklasse 3590 definieren)
```

```
3.13.10.2 DEFINE DEVCLASS (Einheitenklasse 3592 definieren)
...
```

Soll Hilfe für den Befehl DEFINE DEVCLASS für die Einheitenklasse 3590 angezeigt werden, geben Sie Folgendes ein:

```
help 3.13.10.1
```

- **Syntaxdiagramme lesen**  
Zum Lesen eines Syntaxdiagramms für die Eingabe eines Befehls ist dem Pfad der Zeile zu folgen. Gelesen wird von links nach rechts und von oben nach unten.
- **Fortsetzungszeichen für die Eingabe langer Befehle verwenden**  
Fortsetzungszeichen sind nützlich, wenn ein Befehl verarbeitet werden soll, dessen Länge die Anzeigen- oder Fensterbreite überschreitet. Im interaktiven Modus des Verwaltungsclients können Fortsetzungszeichen verwendet werden.
- **IBM Spectrum Protect-Objekte benennen**  
IBM Spectrum Protect schränkt die Anzahl und die Art der Zeichen ein, die zum Benennen von Objekten verwendet werden können.
- **Platzhalterzeichen zur Angabe von Objektname verwenden**  
In einigen Befehlen (z. B. Abfragebefehle) kann mit Hilfe von Platzhalterzeichen eine Suchmusterzeichenfolge erstellt werden, die mehrere Objekte angibt. Platzhalterzeichen erleichtern die Anpassung eines Befehls an individuelle Anforderungen.
- **Beschreibungen in Schlüsselwortparametern angeben**  
Wenn eine Beschreibung (eine Zeichenfolge) eines Parameters mit einem einfachen oder doppelten Anführungszeichen beginnt oder eingebettete Leerzeichen oder Gleichheitszeichen enthält, muss der Wert in einfache (') oder doppelte Anführungszeichen (") eingeschlossen werden.

## Syntaxdiagramme lesen

---

Zum Lesen eines Syntaxdiagramms für die Eingabe eines Befehls ist dem Pfad der Zeile zu folgen. Gelesen wird von links nach rechts und von oben nach unten.

- Das Symbol >>--- kennzeichnet den Anfang eines Syntaxdiagramms.
- Das Symbol ---> am Ende einer Zeile gibt an, dass das Syntaxdiagramm in der nächsten Zeile fortgesetzt wird.
- Das Symbol >--- am Anfang einer Zeile gibt an, dass ein in der vorherigen Zeile begonnenes Syntaxdiagramm fortgesetzt wird.
- Das Symbol ---< kennzeichnet das Ende eines Syntaxdiagramms.

## Befehlsnamen

---

Der Befehlsname kann aus einem einzelnen Aktionswort bestehen, wie beispielsweise HALT, oder aus einem Aktionswort und einem Objekt für die Aktion, wie beispielsweise DEFINE DOMAIN. Sie können den Befehl in eine beliebige Spalte der Eingabezeile eingeben.

Geben Sie den vollständigen Befehlsnamen oder die in dem Syntaxdiagramm des Befehls angegebene Abkürzung ein. Großbuchstaben kennzeichnen die kürzeste zulässige Abkürzung. Steht ein Befehl nur in Großbuchstaben, kann er nicht abgekürzt werden. Der Befehl kann in Großbuchstaben, Kleinbuchstaben oder in einer beliebigen Kombination aus beidem eingegeben werden. In diesem Beispiel kann CMDNA, CMDNAM oder CMDNAME in einer beliebigen Kombination aus Groß- und Kleinbuchstaben eingegeben werden.

```
>>-CMDName-----><
```

Anmerkung: Befehlsnamen im beschreibenden Text werden immer in Großbuchstaben angezeigt.

## Erforderliche Parameter

---

Befindet sich ein Parameter auf derselben Zeile wie der Befehlsname, ist der Parameter erforderlich. Werden zwei oder mehr Parameterwerte als Stapel angezeigt und befindet sich einer davon auf der Zeile, *muss* ein Wert angegeben werden.

In diesem Beispiel müssen Sie PARMNAME=A, PARMNAME=B oder PARMNAME=C eingeben. Direkt vor und hinter dem Gleichheitszeichen (=) dürfen sich keine Leerzeichen befinden.

```
>>-PARMName-----+A-----><
                   +-B-+
                   '-C-'
```

## Optionale Parameter

---

Steht ein Parameter unterhalb der Zeile, ist der Parameter optional. In diesem Beispiel können Sie PARMNAME=A eingeben oder keine Eingabe vornehmen. Direkt vor und hinter dem Gleichheitszeichen (=) dürfen sich keine Leerzeichen befinden.

```
>>+-----><
    '-PARMName-----A-'
```

Werden zwei oder mehr Parameterwerte als Stapel unterhalb der Zeile angezeigt, sind alle Parameterwerte optional. In diesem Beispiel können Sie PARMNAME=A, PARMNAME=B oder PARMNAME=C eingeben oder keine Eingabe vornehmen. Direkt vor und hinter dem Gleichheitszeichen (=) dürfen sich keine Leerzeichen befinden.

```
>>+-----><
    '-PARMName-----+A-+-'
                        +-B-+
                        '-C-'
```

## Standardwerte

Standardwerte werden oberhalb der Zeile angezeigt. Das System verwendet die Standardwerte, sofern sie nicht vom Benutzer überschrieben werden. Der Standardwert kann durch Eingabe einer Option aus dem Stapel unterhalb der Zeile überschrieben werden.

In diesem Beispiel ist PARMNAME=A der Standardwert. Sie können auch PARMNAME=A, PARMNAME=B oder PARMNAME=C eingeben. Direkt vor oder direkt nach dem Gleichheitszeichen (=) dürfen keine Leerzeichen stehen.

```
.-PARMName-----A-----
>>+-----><
    '-PARMName-----+A-+-'
                        +-B-+
                        '-C-'
```

## Variablen

Kursiv hervorgehobene Elemente (wie hier) kennzeichnen Variablen. In diesen Beispielen stellt Variablenname Variablen dar:

```
>>-CMDName--Variablenname-----><

>>+-----><
    '-PARMname-----Variablenname-'
```

## Sonderzeichen

Diese Symbole müssen exakt so eingegeben werden, wie sie im Syntaxdiagramm erscheinen.

- \* Stern
- : Doppelpunkt
- ,
- =' Komma
- = Gleichheitszeichen
- Silbentrennungsstrich
- () Runde Klammer
- .
- Punkt

## Werte wiederholen

Ein nach links zurücklaufender Pfeil bedeutet, daß das Element wiederholt eingegeben werden kann. Ein Zeichen innerhalb des Pfeils gibt an, dass die Elemente, die wiederholt werden, durch dieses Zeichen voneinander getrennt werden müssen.

```
.-,-----.
```

```

      v      |
>>---Dateiname+-----><

```

## Wiederholbare Auswahlangaben

Ein Stapel von Werten gefolgt von einem nach links zurücklaufenden Pfeil bedeutet, dass mehrere Werte ausgewählt werden können oder, wenn zulässig, ein einzelner Wert wiederholt werden kann. In diesem Beispiel kann mehr als ein Wert angegeben werden, wobei die einzelnen Namen durch Komma getrennt werden müssen. Direkt vor oder direkt nach dem Gleichheitszeichen (=) dürfen keine Leerzeichen stehen.

```

      .-,-----
      v      |
>>-PARMName-----+---Wert1---+-----><
                    +-Wert2-+-
                    '-Wert3-'

```

## Fußnoten

Fußnoten sind in runden Klammern eingeschlossen.

```

      .-,-----
      v (1)  |
>>-----Dateiname+-----><

```

Anmerkungen:

1. Sie können bis zu fünf Dateinamen angeben.

## Parameter eingeben

Die Reihenfolge, in der Sie Parameter eingeben, kann wichtig sein. Das folgende Beispiel zeigt einen Teil des Befehls zum Definieren eines Kopierspeicherpools:

```

>>-DEFine STGpool--Poolname--Einheitenklassenname----->
>--POOLtype-----COPY---+----->
                        '-DESCRIPTION-----Beschreibung-'
      .-REclaim-----100-----
>+----->
      '-REclaim-----Prozent-'

```

Die ersten beiden Parameter in diesem Befehl (*Poolname* und *Einheitenklassenname*) sind erforderliche Parameter. *Poolname* und *Einheitenklassenname* sind außerdem positionsgebunden. Das bedeutet, dass sie in der angezeigten Reihenfolge direkt nach dem Befehlsnamen eingegeben werden müssen. Der Parameter *POOLTYPE* ist ein erforderlicher Schlüsselwortparameter. *DESCRIPTION* und *RECLAIM* sind optionale Schlüsselwortparameter. Schlüsselwortparameter werden durch ein Gleichheitszeichen identifiziert, das einen bestimmten Wert oder eine Variable angibt. Schlüsselwortparameter müssen auf positionsgebundene Parameter in einem Befehl folgen.

Die folgenden Befehlseingaben, in denen die Schlüsselwortparameter unterschiedlich angeordnet sind, werden akzeptiert:

```

define stgpool mycopypool mydeviceclass pooltype=copy description=engineering
reclaim=50
define stgpool mycopypool mydeviceclass description=engineering pooltype=copy
reclaim=50

```

Das folgende Beispiel, in dem einer der positionsgebundenen Parameter auf einen Schlüsselwortparameter folgt, wird nicht akzeptiert:

```

define stgpool mycopypool pooltype=copy mydeviceclass description=engineering
reclaim=50

```

## Syntaxfragmente

Einige Diagramme müssen aufgrund ihrer Länge Teile der Syntax mit Fragmenten anzeigen. Der Fragmentname erscheint zwischen vertikalen Balken im Diagramm.



Das erweiterte Fragment erscheint im Diagramm nach allen anderen Parametern oder ganz unten im Diagramm. Das erweiterte Fragment wird durch eine Überschrift mit dem Fragmentnamen gekennzeichnet. Befehle, die direkt auf der Linie stehen, müssen eingegeben werden.

In diesem Beispiel hat das Fragment den Namen "Fragment".

```
>>-| Fragment |-----><
Fragment
  .-A-.
|-----|
  +-B-+
  '-C-'
```

## Fortsetzungszeichen für die Eingabe langer Befehle verwenden

Fortsetzungszeichen sind nützlich, wenn ein Befehl verarbeitet werden soll, dessen Länge die Anzeigen- oder Fensterbreite überschreitet. Im interaktiven Modus des Verwaltungsclients können Fortsetzungszeichen verwendet werden.

### Informationen zu diesem Vorgang

Ohne Fortsetzungszeichen können maximal 256 Zeichen eingegeben werden. Mit Fortsetzungszeichen können maximal 1500 Zeichen eingegeben werden.

Anmerkung: Im Befehl MACRO gelten die Höchstwerte nach dem Anwenden von Substitutionsvariablen. Mit Fortsetzungszeichen kann folgendes ausgeführt werden:

- Einen Bindestrich am Ende der fortzusetzenden Zeile eingeben.  
Beispiel:

```
register admin pease mypasswd -
contact="david, ext1234"
```

- Eine Werteliste wird fortgesetzt, indem ein Bindestrich oder ein umgekehrter Schrägstrich ohne vorangehende Leerstellen hinter dem letzten Komma der in der ersten Zeile eingegebenen Liste eingegeben wird. Dann werden die übrigen Elemente der Liste auf der nächsten Zeile ohne vorangehende Leerstellen eingegeben. Beispiel:

```
stgpools=stg1, stg2, stg3, -
stg4, stg5, stg6
```

- Um eine in Anführungszeichen eingeschlossene Wertefolge fortzusetzen, muss der erste Abschnitt der Folge zwischen Anführungszeichen eingegeben und mit einem Bindestrich oder einem umgekehrten Schrägstrich am Zeilenende abgeschlossen werden. Dann wird der Rest der Wertefolge zwischen derselben Art von Anführungszeichen auf der nächsten Zeile eingegeben.  
Beispiel:

```
contact="david pease, bldg. 100, room 2b, san jose, "-
"ext. 1234, alternate contact-norm pass, ext 2345"
```

IBM Spectrum Protect verknüpft die beiden Zeichenfolgen ohne dazwischenliegende Leerzeichen. Es darf nur diese Methode zur Fortsetzung einer Zeichenfolge in Anführungszeichen über mehrere Zeilen verwendet werden.

## IBM Spectrum Protect-Objekte benennen

IBM Spectrum Protect schränkt die Anzahl und die Art der Zeichen ein, die zum Benennen von Objekten verwendet werden können.

### Informationen zu diesem Vorgang

Folgende Zeichen können für die Definition von Objektnamen verwendet werden.

| Zeichen | Beschreibung                |
|---------|-----------------------------|
| A-Z     | Alle Buchstaben von A bis Z |
| 0-9     | Alle Zahlen von 0 bis 9     |
| _       | Unterstreichung             |
| .       | Punkt                       |

| Zeichen | Beschreibung          |
|---------|-----------------------|
| -       | Silbentrennungsstrich |
| +       | Plus                  |
| &       | Et-Zeichen            |

Die folgende Tabelle zeigt die maximal zulässige Länge von Zeichen für die Benennung von Objekten.

| Art des Namens   | Maximale Länge |
|--|----------------|
| Administratoren, Clientoptionsgruppen, Clientknoten, Kennwörter, Servergruppen, Server, Namen, Namen virtueller Dateibereiche                      | 64             |
| IDs wiederanlauffähiger Exporte  | 64             |
| TCP/IP-Adressen (IPv4 oder IPv6) der höheren und unteren Ebene   | 64             |
| Einheitenklassen, Laufwerke, Kassettenarchive, Verwaltungsklassen, Maßnahmendomänen, Profile, Zeitpläne, Scripts, Sicherungsgruppen, Speicherpools | 30             |

Folgende Zeichen können für die Definition von Kennwörtern verwendet werden:

```

a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~

```

Kennwörter, die als "LOCAL" betrachtet werden, sind die Kennwörter, die mit dem IBM Spectrum Protect-Server authentifiziert werden. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden. Sobald ein Knoten oder Administrator für die Verwendung des Parameters SESSIONSECURITY=STRICT aktualisiert wird, muss beim Kennwort die Groß-/Kleinschreibung beachtet werden, wenn das Kennwort das nächste Mal geändert wird. Kennwörter, die als "LDAP" betrachtet werden, sind die Kennwörter, die mit einem LDAP-Verzeichnisserver authentifiziert werden. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung beachtet werden.

Wenn Sie Befehle DEFINE verwenden, um Datenbank-, Wiederherstellungsprotokoll- und Speicherpooldatenträger zu definieren, ist die Namenskonvention für den Datenträgernamen abhängig vom verwendeten Typ des Datenträgers mit sequenziellem Zugriff oder mit wahlfreiem Zugriff. Ausführliche Informationen befinden sich unter dem jeweiligen VOLUME-Befehl.

## Platzhalterzeichen zur Angabe von Objektamen verwenden

In einigen Befehlen (z. B. Abfragebefehle) kann mit Hilfe von Platzhalterzeichen eine Suchmusterzeichenfolge erstellt werden, die mehrere Objekte angibt. Platzhalterzeichen erleichtern die Anpassung eines Befehls an individuelle Anforderungen.

### Informationen zu diesem Vorgang

Welche Platzhalterzeichen verwendet werden, ist abhängig von dem Betriebssystem, über das die Befehle ausgegeben werden. Mögliche Platzhalterzeichen sind beispielsweise ein Stern (\*), der beliebigen (0 oder mehr) Zeichen entspricht, und ein Fragezeichen (?) oder ein Prozentzeichen (%), die exakt einem Zeichen entsprechen.

Tabelle 1 enthält Referenzen für Platzhalterzeichen einiger Betriebssysteme. Die für das verwendete System geeigneten Platzhalterzeichen sind zu verwenden.

Tabelle 1. Platzhalterzeichen nach Betriebssystem

| Betriebssystem      | Beliebige Entsprechung | Exakte Entsprechung |
|---------------------|------------------------|---------------------|
| AIX, Linux, Windows | *                      | ?                   |
| TSO                 | *                      | %                   |

Sollen beispielsweise alle Verwaltungsklassen, deren Namen mit DEV beginnen, in allen Maßnahmengruppen in DOMAIN1 abgefragt werden und verwendet das System einen Stern als Zeichen für eine *beliebige Entsprechung*, kann folgendes eingegeben werden:

```
query mgmtclass domain1 * dev*
```

Verwendet das System ein Fragezeichen als Zeichen für eine *exakte Entsprechung* und sollen die Verwaltungsklassen in POLICYSET1 in DOMAIN1 abgefragt werden, kann Folgendes eingegeben werden:

```
query mgmtclass domain1 policyset1 mc?
```

IBM Spectrum Protect zeigt Informationen über Verwaltungsklassen mit den Namen MC an.

Tabelle 2 zeigt weitere Beispiele der Verwendung von Platzhalterzeichen für beliebige Entsprechungen.

Tabelle 2. Zeichen für beliebige Entsprechung

| Muster   | Entspricht          | Entspricht nicht  |
|----------|---------------------|-------------------|
| ab*      | ab, abb, abxxx      | a, b, aa, bb      |
| ab*rs    | abrs, abtrs, abrrrs | ars, aabrs, abrrs |
| ab*ef*rs | abefrs, abefghrs    | abefr, abers      |

Tabelle 3 zeigt weitere Beispiele der Verwendung von Platzhalterzeichen für exakte Entsprechungen. Das Fragezeichen (?) kann durch ein Prozentzeichen (%) ersetzt werden, wenn die Plattform dieses Zeichen anstelle von ? verwendet.

Tabelle 3. Exakte Entsprechung

| Muster   | Entspricht        | Entspricht nicht         |
|----------|-------------------|--------------------------|
| ab?      | abc               | ab, abab, abzzzz         |
| ab?rs    | abfrs             | abrs, abllrs             |
| ab?ef?rs | abdefjrs          | abefrs, abdefrs, abefjrs |
| ab??rs   | abcdrs,<br>abzzrs | abrs, abjrs, abkkrs      |

## Beschreibungen in Schlüsselwortparametern angeben

Wenn eine Beschreibung (eine Zeichenfolge) eines Parameters mit einem einfachen oder doppelten Anführungszeichen beginnt oder eingebettete Leerzeichen oder Gleichheitszeichen enthält, muss der Wert in einfache (') oder doppelte Anführungszeichen (") eingeschlossen werden.

### Informationen zu diesem Vorgang

Das Anfangsanführungszeichen und das abschließende Anführungszeichen müssen von derselben Art sein. Wenn das Anfangsanführungszeichen ein einfaches Anführungszeichen ist, muß das abschließende Anführungszeichen auch ein einfaches Anführungszeichen sein.

Soll beispielsweise der neue Client-Knoten Louie mit dem Kennwort secret und seinem Titel als Kontaktinformationen registriert werden, folgendes eingeben:

```
register node louie secret contact="manager of dept. 61f"
```

Die folgende Tabelle zeigt die Eingabemöglichkeiten für eine Beschreibung für den Parameter CONTACT. Der Wert darf Anführungszeichen, eingebettete Leerzeichen und Gleichheitszeichen enthalten.

| Für diese Beschreibung       | Folgendes eingeben   |
|------------------------------|--|
| manager                      | contact=manager  |
| manager's                    | contact="manager's" oder contact='manager's'                                       |
| "manager"                    | contact=""manager"" oder contact=""manager""                                       |
| manager's report             | contact="manager's report" oder contact='manager's report'                         |
| manager's "report"           | contact='manager's "report"'   |
| manager=dept. 61f            | contact='manager=dept. 61f'  |
| manager reports to dept. 61f | contact='manager reports to dept. 61f' oder contact="manager reports to dept. 61f" |

## Befehlsverarbeitung steuern

Einige IBM Spectrum Protect-Befehle können nacheinander oder gleichzeitig mit anderen Befehlen ausgeführt werden. Sie können auch Befehle von einem Server an andere Server für die Verarbeitung weiterleiten.

### Informationen zu diesem Vorgang

- Serverbefehlsverarbeitung  
IBM Spectrum Protect verarbeitet Verwaltungsbefehle im Vordergrund oder im Hintergrund. Im Vordergrund verarbeitete Befehle

müssen beendet sein, bevor Sie einen weiteren Befehl ausgeben können. Werden Befehle im Hintergrund verarbeitet, können Sie jederzeit zusätzliche Befehle ausgeben.

- Hintergrundprozesse stoppen  
Mit dem Befehl CANCEL PROCESS können Befehle abgebrochen werden, die Hintergrundprozesse generieren.

## Serverbefehlsverarbeitung

---

IBM Spectrum Protect verarbeitet Verwaltungsbefehle im Vordergrund oder im Hintergrund. Im Vordergrund verarbeitete Befehle müssen beendet sein, bevor Sie einen weiteren Befehl ausgeben können. Werden Befehle im Hintergrund verarbeitet, können Sie jederzeit zusätzliche Befehle ausgeben.

Die meisten IBM Spectrum Protect-Befehle werden im Vordergrund verarbeitet. Bei einigen Befehlen, die normalerweise im Hintergrund verarbeitet werden (z. B. BACKUP DB), können Sie den Parameter WAIT (WAIT=YES) mit dem Befehl angeben, so dass der Befehl im Vordergrund verarbeitet wird. Möglicherweise soll aus einem der folgenden Gründe ein Befehl im Vordergrund und nicht im Hintergrund verarbeitet werden:

- Um schnell zu bestimmen, ob ein Befehl erfolgreich ausgeführt wurde. Wenn Sie einen Befehl eingeben, der im Vordergrund verarbeitet wird, sendet IBM Spectrum Protect eine Bestätigungsnachricht, die die erfolgreiche Ausführung des Befehls anzeigt. Wird der Befehl im Hintergrund verarbeitet, müssen Sie das Feature 'Berichte zum Betrieb' (Operational Reporting) öffnen oder das Aktivitätenprotokoll abfragen, um zu bestimmen, ob der Befehl erfolgreich ausgeführt wurde.
- Zur Überwachung von Serveraktivitäten (z. B. Nachrichten) auf dem Verwaltungsclient während der Verarbeitung eines Befehls. Das ist unter Umständen dem Durchsuchen eines langen Aktivitätenprotokolls nach Beendigung des Befehls vorzuziehen.
- Damit ein anderer Prozess unmittelbar nach Beendigung des Befehls gestartet werden kann. Sie können beispielsweise WAIT=YES für einen Befehl angeben, dessen Verarbeitung nur kurze Zeit dauert, so dass Sie nach Beendigung der Verarbeitung sofort die Verarbeitung eines anderen Befehls starten können.
- Zum Serialisieren von Befehlen in einem Verwaltungsscript, wenn es darauf ankommt, dass ein Befehl beendet wird, bevor ein anderer beginnt.

Überprüfen Sie die jeweilige Befehlsbeschreibung, um zu bestimmen, ob ein Befehl über einen Parameter WAIT verfügt.

Sie können im Vordergrund verarbeitete Befehle über die Serverkonsole oder eine andere Verwaltungsclientsitzung abbrechen.

Jedem Hintergrundprozess wird eine Prozessnummer zugeordnet. Mit dem Befehl QUERY PROCESS können der Status und die Prozessnummer eines Hintergrundprozesses abgefragt werden.

Anmerkung:

- Wenn Sie einen Zeitplan mit einem Befehl definieren, in dem WAIT=NO (Standardwert) angegeben ist, und Sie QUERY EVENT ausgeben, um den Status Ihrer geplanten Operation festzustellen, haben fehlgeschlagene Operationen den Ereignisstatus COMPLETED mit dem Rückgabewert OK. Damit in der Ausgabe von QUERY EVENT der Fehlerstatus angezeigt wird, muss für den Parameter WAIT der Wert YES angegeben werden. Dadurch wird die geplante Operation im Vordergrund ausgeführt, und Sie werden nach ihrer Beendigung über den Status informiert.
- Von der Serverkonsole aus können Sie keine Befehle im Vordergrund verarbeiten.

## Hintergrundprozesse stoppen

---

Mit dem Befehl CANCEL PROCESS können Befehle abgebrochen werden, die Hintergrundprozesse generieren.

### Informationen zu diesem Vorgang

---

Mit dem Befehl QUERY PROCESS können der Status und die Prozessnummer eines Hintergrundprozesses abgefragt werden. Ist ein Hintergrundprozess bei seinem Abbruch aktiv, stoppt der Server den Prozess. Nicht festgeschriebene Änderungen werden rückgängig gemacht. Festgeschriebene Änderungen werden jedoch nicht rückgängig gemacht.

Wenn ein QUERY-Befehl über den Verwaltungsclient ausgegeben wird, können mehrere Ausgabeanzeigen generiert werden. In diesem Fall kann die Anzeige der Ausgabe an der Client-Workstation abgebrochen werden, wenn keine zusätzliche Ausgabe benötigt wird. Die Verarbeitung des Befehls wird dabei nicht beendet.

## Tasks gleichzeitig auf mehreren Servern ausführen

---

Mit der Befehlsweiterleitung können Sie Befehle an einen oder an mehrere Server zur Verarbeitung weiterleiten und dann die Ausgabe von diesen Servern sammeln.

### Informationen zu diesem Vorgang

---

Um Befehle an andere Server weiterzuleiten, müssen Sie auf jedem Server, an den der Befehl weitergeleitet wird, dieselbe Administrator-ID und dasselbe Kennwort sowie die erforderliche Administratorberechtigung haben. Sie können von der Serverkonsole aus keine Befehle an andere Server weiterleiten.

Nachdem die Verarbeitung des Befehls auf allen Servern beendet wurde, wird die vollständige Ausgabe für jeden Server angezeigt. Beispielsweise wird die Ausgabe von SERVER\_A vollständig angezeigt, dann die Ausgabe von SERVER\_B. Die Ausgabe beinhaltet Übersichtsnachrichten für jeden einzelnen Server und zeigt an, welcher Server die Ausgabe verarbeitet hat. Rückkehrcodes zeigen an, ob die Befehle erfolgreich auf den Servern verarbeitet wurden. Diese Rückkehrcodes zeigen drei Bewertungen an: 0, ERROR oder WARNING.

Jeder Server, der als Ziel eines weitergeleiteten Befehls angegeben wird, muss zuerst mit dem Befehl DEFINE SERVER definiert werden. Der Befehl wird automatisch an alle Server weitergeleitet, die als Teil einer Servergruppe angegeben sind, oder an einzelne Server, die mit dem Befehl angegeben werden.

Die folgenden Beispiele beschreiben das Weiterleiten des Befehls QUERY STGPOOL an einen Server, an mehrere Server, an eine Servergruppe, an mehrere Servergruppen oder an eine Kombination von Servern und Servergruppen. Die einzelnen Server oder Servergruppen in einer Liste müssen ohne Leerzeichen durch ein Komma voneinander getrennt werden.

## Befehle an einen einzelnen Server weiterleiten

---

### Vorgehensweise

Soll der Befehl QUERY STGPOOL an den Server ASTRO weitergeleitet werden, Folgendes eingeben:

```
astro: query stgpool
```

Der Doppelpunkt hinter dem Server-Namen zeigt das Ende der Leitweginformationen an. Dies wird auch als *Serverpräfix* bezeichnet. Eine andere Möglichkeit, das Ende der Leitweginformationen anzugeben, ist die Verwendung von runden Klammern, die den Server-Namen einschließen, zum Beispiel:

```
(astro) query stgpool
```

## Befehle an mehrere Server weiterleiten

---

### Informationen zu diesem Vorgang

#### Vorgehensweise

Soll der Befehl QUERY STGPOOL an die Server HD\_QTR, MIDAS, SATURN weitergeleitet werden, Folgendes eingeben:

```
hd_qtr,midas,saturn: query stgpool
```

Wenn der erste Server nicht für IBM Spectrum Protect definiert wurde, wird der Befehl an den nächsten definierten Server in der Server-Liste weitergeleitet.

Sie können den Befehl auch wie folgt eingeben:

```
(hd_qtr,midas,saturn) query stgpool
```

## Befehle an eine Servergruppe weiterleiten

---

### Informationen zu diesem Vorgang

In diesem Beispiel sind in der Servergruppe ADMIN die Server SECURITY, PAYROLL, PERSONNEL als Gruppenteile definiert. Der Befehl wird an jeden dieser Server weitergeleitet.

#### Vorgehensweise

Soll der Befehl QUERY STGPOOL an die Servergruppe ADMIN weitergeleitet werden, Folgendes eingeben:

```
admin: query stgpool
```

Sie können den Befehl auch wie folgt eingeben:

```
(admin) query stgpool
```

## Befehle an Servergruppen weiterleiten

---

## Informationen zu diesem Vorgang

In diesem Beispiel sind in der Servergruppe ADMIN2 die Server SERVER\_A, SERVER\_B und SERVER\_C und in der Servergruppe ADMIN3 die Server ASTRO, GUMBY und CRUSTY als Gruppenteile definiert. Der Befehl wird an die Server SERVER\_A, SERVER\_B, SERVER\_C, ASTRO, GUMBY und CRUSTY weitergeleitet.

### Vorgehensweise

Soll der Befehl QUERY STGPOOL an die beiden Servergruppen ADMIN2 und ADMIN3 weitergeleitet werden, Folgendes eingeben:

```
admin2,admin3: query stgpool
```

Sie können den Befehl auch wie folgt eingeben:

```
(admin2,admin3) query stgpool
```

## Befehle an zwei Server und eine Servergruppe weiterleiten

---

### Informationen zu diesem Vorgang

In diesem Beispiel sind in der Servergruppe DEV\_GROUP die Server SALES, MARKETING und STAFF als Gruppenteile definiert. Der Befehl wird an die Server SALES, MARKETING, STAFF, MERCURY und JUPITER weitergeleitet.

### Vorgehensweise

Soll der Befehl QUERY STGPOOL an die Servergruppe DEV\_GROUP und an die Server MERCURY und JUPITER weitergeleitet werden, Folgendes eingeben:

```
dev_group,mercury,jupiter: query stgpool
```

Sie können den Befehl auch wie folgt eingeben:

```
(dev_group,mercury,jupiter) query stgpool
```

## Befehle innerhalb von Prozeduren weiterleiten

---

### Informationen zu diesem Vorgang

Werden Befehle innerhalb von Prozeduren weitergeleitet, muß der Server oder die Server-Gruppe in runde Klammern eingeschlossen und der Doppelpunkt übergangen werden. Andernfalls wird der Befehl bei Ausgabe des Befehls RUN nicht weitergeleitet und nur auf dem Server ausgeführt, auf dem der Befehl RUN ausgegeben wird.

Soll beispielsweise der Befehl QUERY STGPOOL innerhalb einer Prozedur weitergeleitet werden, wie folgt vorgehen:

### Vorgehensweise

1. Die Prozedur QU\_STG definieren, um sie an die Servergruppe DEV\_GROUP weiterzuleiten.

```
define script qu_stg "(dev_group) query stgpool"
```

2. Die Prozedur QU\_STG ausführen:

```
run qu_stg
```

### Ergebnisse

In diesem Beispiel sind in der Servergruppe DEV\_GROUP die Server SALES, MARKETING und STAFF als Gruppenteile definiert. Der Befehl QUERY STGPOOL wird an diese Server weitergeleitet.

## Berechtigungsklassen für Befehle

---

Die einem Administrator über die Berechtigungsklasse erteilte Berechtigung bestimmt, welche Verwaltungsbefehle der Administrator ausgeben kann.

Es gibt vier Administratorberechtigungsklassen in IBM Spectrum Protect:

- Systemberechtigung
- Maßnahmenberechtigung

- Speicherberechtigung
- Bedienerberechtigung

Wenn ein Administrator mit Hilfe des Befehls REGISTER ADMIN registriert wurde, kann er eine beschränkte Befehlsgruppe, einschließlich aller Abfragebefehle, ausgeben. Wenn Sie IBM Spectrum Protect installieren, wird die Serverkonsole als Systemadministrator mit dem Namen SERVER\_CONSOLE definiert und erhält die Systemberechtigung.

- Befehle, die die Systemberechtigung erfordern  
Ein Administrator mit Systemberechtigung verfügt über die höchste Berechtigungsstufe für den Server. Mit Systemberechtigung kann ein Administrator alle Verwaltungsbefehle ausgeben und hat die Berechtigung, alle Maßnahmendomänen und alle Speicherpools zu verwalten.
- Befehle, die die Maßnahmenberechtigung erfordern  
Ein Administrator mit Maßnahmenberechtigung kann Befehle für Maßnahmenverwaltungsobjekte ausgeben, wie z. B. Maßnahmendomänen, Maßnahmengruppen, Verwaltungsklassen, Kopiengruppen und Zeitpläne. Die Maßnahmenberechtigung kann uneingeschränkt sein oder kann auf bestimmte Maßnahmendomänen beschränkt werden.
- Befehle, die die Speicherberechtigung erfordern  
Ein Administrator mit Speicherberechtigung kann Befehle ausgeben, die Speicherressourcen für den Server zuordnen und steuern. Die Speicherberechtigung kann uneingeschränkt sein oder kann auf bestimmte Speicherpools beschränkt werden.
- Befehle, die die Bedienerberechtigung erfordern  
Ein Administrator mit Bedienerberechtigung kann Befehle ausgeben, die den direkten Betrieb des Servers und die Verfügbarkeit von Speicherdatenträgern steuern.
- Befehle, die jeder Administrator ausgeben kann  
Eine begrenzte Anzahl von Befehlen kann von jedem Administrator verwendet werden, auch wenn er über keine speziellen Administratorberechtigungen verfügt.

## Befehle, die die Systemberechtigung erfordern

Ein Administrator mit Systemberechtigung verfügt über die höchste Berechtigungsstufe für den Server. Mit Systemberechtigung kann ein Administrator alle Verwaltungsbefehle ausgeben und hat die Berechtigung, alle Maßnahmendomänen und alle Speicherpools zu verwalten.

Tabelle 1 enthält die Befehle, die Administratoren mit Systemberechtigung ausgeben können. In einigen Fällen können Administratoren mit niedrigeren Berechtigungsstufen, beispielsweise mit uneingeschränkter Speicherberechtigung ebenfalls diese Befehle ausgeben. Außerdem kann mit der Serveroption REQSYSAUTHOUTFILE angegeben werden, dass bestimmte Befehle die Systemberechtigung erfordern, wenn sie bewirken, dass der Server in eine externe Datei schreibt. Weitere Informationen zu dieser Serveroption finden Sie in REQSYSAUTHOUTFILE.

Tabelle 1. Systemberechtigungsbeefehle

| Befehlsname | Befehlsname |
|-------------|-------------|
|-------------|-------------|

| Befehlsname   | Befehlsname  |
|---|--|
| <ul style="list-style-type: none"> <li>• AUDIT LDAPDIRECTORY</li> <li>• AUDIT LICENSES</li> <li>• ACCEPT DATE</li> <li>• BEGIN EVENTLOGGING</li> <li>• CANCEL EXPIRATION</li> <li>• CANCEL PROCESS</li> <li>• CANCEL REPLICATION</li> <li>• CANCEL REQUEST</li> <li>• CANCEL RESTORE</li> <li>• CLEAN DRIVE</li> <li>• COPY ACTIVATEDATA</li> <li>• COPY DOMAIN</li> <li>• COPY POLICYSET</li> <li>• COPY PROFILE</li> <li>• COPY SCHEDULE (Siehe Anmerkung.)</li> <li>• COPY SCRIPT</li> <li>• COPY SERVERGROUP</li> <li>• DEFINE BACKUPSET</li> <li>• DEFINE CLIENTACTION</li> <li>• DEFINE CLIENTOPT</li> <li>• DEFINE CLOPTSET</li> <li>• DEFINE COLLOGGROUP</li> <li>• DEFINE COLLOCMEMBER</li> <li>• DEFINE DEVCLASS</li> <li>• DEFINE DOMAIN</li> <li>• DEFINE DRIVE</li> <li>• DEFINE EVENTSERVER</li> <li>• DEFINE GRPMEMBER</li> <li>• DEFINE LIBRARY</li> <li>• DEFINE MACHINE</li> <li>• DEFINE MACHNODEASSOCIATION</li> <li>• DEFINE NODEGROUP</li> <li>• DEFINE NODEGROUPMEMBER</li> <li>• DEFINE PATH</li> <li>• DEFINE PROFASSOCIATION</li> <li>• DEFINE PROFILE</li> <li>• DEFINE RECMEDMACHASSOCIATION</li> <li>• DEFINE RECOVERYMEDIA</li> <li>• DEFINE SCHEDULE (Siehe Anmerkung.)</li> <li>• DEFINE SCRIPT</li> <li>• DEFINE SERVER</li> <li>• DEFINE SERVERGROUP</li> </ul> | <ul style="list-style-type: none"> <li>• DEFINE SPACETRIGGER</li> <li>• DEFINE STGPOOL</li> <li>• DEFINE SUBSCRIPTION</li> <li>• DEFINE VIRTUALFSMAPPING</li> <li>• DEFINE VOLUME</li> <li>• DELETE BACKUPSET</li> <li>• DELETE CLIENTOPT</li> <li>• DELETE CLOPTSET</li> <li>• DEFINE COLLOGGROUP</li> <li>• DEFINE COLLOCMEMBER</li> <li>• DELETE DOMAIN</li> <li>• DELETE DRIVE</li> <li>• DELETE EVENTSERVER</li> <li>• DELETE GRPMEMBER</li> <li>• DELETE LIBRARY</li> <li>• DELETE MACHINE</li> <li>• DELETE MACHNODEASSOCIATION</li> <li>• DELETE NODEGROUP</li> <li>• DELETE NODEGROUPMEMBER</li> <li>• DELETE PROFASSOCIATION</li> <li>• DELETE PROFILE</li> <li>• DELETE RECMEDMACHASSOCIATION</li> <li>• DELETE RECOVERYMEDIA</li> <li>• DELETE SCHEDULE (Siehe Anmerkung.)</li> <li>• DELETE SCRIPT</li> <li>• DELETE SERVER</li> <li>• DELETE SERVERGROUP</li> <li>• DELETE SPACETRIGGER</li> <li>• DELETE STGPOOL</li> <li>• DELETE SUBSCRIBER</li> <li>• DELETE SUBSCRIPTION</li> <li>• DELETE VIRTUALFSMAPPING</li> <li>• DISABLE EVENTS</li> <li>• ENABLE EVENTS</li> <li>• END EVENTLOGGING</li> <li>• EXPIRE INVENTORY</li> <li>• EXPORT ADMIN</li> <li>• EXPORT NODE</li> <li>• EXPORT POLICY</li> <li>• EXPORT SERVER</li> <li>• GENERATE BACKUPSET</li> <li>• GRANT AUTHORITY</li> </ul> |



| Befehlsname   | Befehlsname  |
|---|--|
| <ul style="list-style-type: none"> <li>• GRANT PROXYNODE</li> <li>• IDENTIFY DUPLICATES</li> <li>• IMPORT NODE</li> <li>• IMPORT POLICY</li> <li>• IMPORT SERVER</li> <li>• INSERT MACHINE</li> <li>• LABEL LIBVOLUME</li> <li>• LOCK ADMIN</li> <li>• LOCK PROFILE</li> <li>• MIGRATE STGPOOL</li> <li>• MOVE DRMEDIA</li> <li>• MOVE MEDIA</li> <li>• MOVE GRPMEMBER</li> <li>• NOTIFY SUBSCRIBERS</li> <li>• PERFORM LIBACTION</li> <li>• PING SERVER</li> <li>• PREPARE</li> <li>• QUERY BACKUPSETCONTENTS</li> <li>• QUERY MEDIA</li> <li>• QUERY RPFCONTENT</li> <li>• QUERY TOC</li> <li>• RECLAIM STGPOOL</li> <li>• RECONCILE VOLUMES</li> <li>• REGISTER ADMIN</li> <li>• REGISTER LICENSE</li> <li>• REMOVE ADMIN</li> <li>• REMOVE REPLNODE</li> <li>• RENAME ADMIN</li> <li>• RENAME SCRIPT</li> <li>• RENAME SERVERGROUP</li> <li>• RENAME STGPOOL</li> <li>• REPLICATE NODE</li> <li>• RESET PASSEXP</li> <li>• RESTORE NODE</li> <li>• REVOKE AUTHORITY</li> <li>• REVOKE PROXYNODE</li> <li>• RUN</li> <li>• SET ACCOUNTING</li> <li>• SET ACTLOGRETENTION</li> <li>• SET ARCHIVERETENTIONPROTECTION</li> <li>• SET ARREPLRULEDEFAULT</li> <li>• SET BKREPLRULEDEFAULT</li> <li>• SET CLIENTACTDURATION</li> </ul> | <ul style="list-style-type: none"> <li>• SET CONFIGMANAGER</li> <li>• SET CONFIGREFRESH</li> <li>• SET CONTEXTMESSAGING</li> <li>• SET CROSSDEFINE</li> <li>• SET DBRECOVERY</li> <li>• SET DEFAULTAUTHENTICATION</li> <li>• SET DRMACTIVEDATASTGPOOL</li> <li>• SET DRMCHECKLABEL</li> <li>• SET DRMCMDFILENAME</li> <li>• SET DRMCOPYCONTAINERSTGPOOL</li> <li>• SET DRMCOPYSTGPOOL</li> <li>• SET DRMCOURIERNAME</li> <li>• SET DRMDBBACKUPEXPIREDAYS</li> <li>• SET DRMFILEPROCESS</li> <li>• SET DRMINSTRPREFIX</li> <li>• SET DRMNOTMOUNTABLENAME</li> <li>• SET DRMPPLANPREFIX</li> <li>• SET DRMPPLANVPOSTFIX</li> <li>• SET DRMPRIMSTGPOOL</li> <li>• SET DRMRPFEXPIREDAYS</li> <li>• SET DRMVaultNAME</li> <li>• SET EVENTRETENTION</li> <li>• SET INVALIDPWLIMIT</li> <li>• SET LDAPPASSWORD</li> <li>• SET LDAPUSER</li> <li>• SET LICENSEAUDITPERIOD</li> <li>• SET MAXCMDRETRIES</li> <li>• SET MAXSCHEDSESSIONS</li> <li>• SET MINPWLENGTH</li> <li>• SET PASSEXP</li> <li>• SET QUERYSCHEDPERIOD</li> <li>• SET RANDOMIZE</li> <li>• SET REPLRETENTION</li> <li>• SET REPLSERVER</li> <li>• SET RETRYPERIOD</li> <li>• SET SCHEDMODES</li> <li>• SET SERVERHLADDRESS</li> <li>• SET SERVERLLADDRESS</li> <li>• SET SERVERNAME</li> <li>• SET SERVERPASSWORD</li> <li>• SET SPREPLRULEDEFAULT</li> <li>• SET SUBFILE</li> <li>• SET TOCLOADRETENTION</li> </ul> |
| <ul style="list-style-type: none"> <li>• SETOPT</li> <li>• UNLOCK ADMIN</li> <li>• UNLOCK PROFILE</li> <li>• UPDATE ADMIN</li> <li>• UPDATE BACKUPSET</li> <li>• UPDATE CLIENTOPT</li> <li>• UPDATE CLOPTSET</li> <li>• UPDATE COLLOGGROUP</li> <li>• UPDATE DEVCLASS</li> <li>• UPDATE DRIVE</li> <li>• UPDATE LIBRARY</li> <li>• UPDATE LIBVOLUME</li> <li>• UPDATE MACHINE</li> </ul>  | <ul style="list-style-type: none"> <li>• UPDATE NODEGROUP</li> <li>• UPDATE PATH</li> <li>• UPDATE PROFILE</li> <li>• UPDATE RECOVERYMEDIA</li> <li>• UPDATE REPLRULE</li> <li>• UPDATE SCHEDULE (Siehe Anmerkung.)</li> <li>• UPDATE SCRIPT</li> <li>• UPDATE SERVER</li> <li>• UPDATE SERVERGROUP</li> <li>• UPDATE SPACETRIGGER</li> <li>• UPDATE VIRTUALFSMAPPING</li> <li>• UPDATE VOLHISTORY</li> <li>• VALIDATE LANFREE</li> <li>• VALIDATE REPLICATION</li> </ul>  |
| <p>Anmerkung: Dieser Befehl ist durch die Berechtigung eingeschränkt, die einem Administrator erteilt wird. Die Systemberechtigung ist nur für Verwaltungsbefehlszeitpläne erforderlich. Die System- oder Maßnahmenberechtigung ist für Clientoperationszeitpläne erforderlich.</p>   |  |

## Befehle, die die Maßnahmenberechtigung erfordern

Ein Administrator mit Maßnahmenberechtigung kann Befehle für Maßnahmenverwaltungsobjekte ausgeben, wie z. B. Maßnahmendomänen, Maßnahmengruppen, Verwaltungsklassen, Kopiengruppen und Zeitpläne. Die Maßnahmenberechtigung kann uneingeschränkt sein oder kann auf bestimmte Maßnahmendomänen beschränkt werden.

Mit der uneingeschränkten Maßnahmenberechtigung können Sie alle Administratorbefehle ausgeben, für die die Maßnahmenberechtigung erforderlich ist. Es können Befehle ausgegeben werden, die alle vorhandenen Maßnahmendomänen sowie alle Maßnahmendomänen betreffen, die in Zukunft definiert werden. Ein Administrator mit uneingeschränkter Maßnahmenberechtigung kann keine Maßnahmendomänen definieren, löschen oder kopieren.

Mit der eingeschränkten Maßnahmenberechtigung können Sie Administratorbefehle ausgeben, die eine oder mehrere Maßnahmendomänen betreffen, für die die Berechtigung erteilt wird. Für den Befehl DELETE MGMTCLASS ist beispielsweise die Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Verwaltungsklasse gehört.

Tabelle 1 enthält die Befehle, die ein Administrator mit Maßnahmenberechtigung ausgeben kann.

Tabelle 1. Maßnahmenberechtigungsbefehle

| Befehlsname  | Befehlsname  |
|--|--|
| <ul style="list-style-type: none"> <li>• ACTIVATE POLICYSET</li> <li>• ASSIGN DEFMGMTCLASS</li> <li>• CLEAN DRIVE</li> <li>• BACKUP NODE</li> <li>• COPY MGMTCLASS</li> <li>• COPY POLICYSET</li> <li>• COPY SCHEDULE (Siehe Anmerkung 2.)</li> <li>• DEFINE ASSOCIATION</li> <li>• DEFINE BACKUPSET</li> <li>• DEFINE COPYGROUP</li> <li>• DEFINE CLIENTACTION</li> <li>• DEFINE CLIENTOPT</li> <li>• DEFINE MGMTCLASS</li> <li>• DEFINE NODEGROUP</li> <li>• DEFINE NODEGROUPMEMBER</li> <li>• DEFINE POLICYSET</li> <li>• DEFINE SCHEDULE</li> <li>• DELETE ASSOCIATION</li> <li>• DELETE BACKUPSET</li> <li>• DELETE COPYGROUP</li> <li>• DELETE EVENT (Siehe Anmerkung 1.)</li> <li>• DELETE FILESPACE</li> <li>• DELETE MGMTCLASS</li> <li>• DELETE NODEGROUP</li> <li>• DELETE NODEGROUPMEMBER</li> </ul> | <ul style="list-style-type: none"> <li>• DELETE POLICYSET</li> <li>• DELETE PATH</li> <li>• DELETE SCHEDULE (Siehe Anmerkung 2.)</li> <li>• GENERATE BACKUPSET</li> <li>• LOCK NODE</li> <li>• QUERY BACKUPSETCONTENTS</li> <li>• REGISTER NODE</li> <li>• REMOVE NODE</li> <li>• RENAME FILESPACE</li> <li>• RENAME NODE</li> <li>• SET SUMMARYRETENTION</li> <li>• RESTORE NODE</li> <li>• QUERY TOC</li> <li>• UNLOCK NODE</li> <li>• UPDATE BACKUPSET</li> <li>• UPDATE COPYGROUP</li> <li>• UPDATE DOMAIN</li> <li>• UPDATE MGMTCLASS</li> <li>• UPDATE NODE</li> <li>• UPDATE NODEGROUP</li> <li>• UPDATE POLICYSET</li> <li>• UPDATE SCHEDULE (Siehe Anmerkung 2.)</li> <li>• VALIDATE POLICYSET</li> </ul> |
| <p>Anmerkungen:</p> <ol style="list-style-type: none"> <li>1. Dieser Befehl kann durch die Maßnahmendomäne eingeschränkt werden. Ein Administrator mit uneingeschränkter Maßnahmenberechtigung oder eingeschränkter Maßnahmenberechtigung für eine angegebene Maßnahmendomäne kann diesen Befehl ausgeben.</li> <li>2. Dieser Befehl ist durch die Berechtigung eingeschränkt, die einem Administrator erteilt wird. Die Systemberechtigung ist nur für Verwaltungsbefehlszeitpläne erforderlich. Die System- oder Maßnahmenberechtigung ist für Clientoperationszeitpläne erforderlich.</li> </ol>  |  |

## Befehle, die die Speicherberechtigung erfordern

Ein Administrator mit Speicherberechtigung kann Befehle ausgeben, die Speicherressourcen für den Server zuordnen und steuern. Die Speicherberechtigung kann uneingeschränkt sein oder kann auf bestimmte Speicherpools beschränkt werden.

Mit der uneingeschränkten Speicherberechtigung können alle Administratorbefehle ausgegeben werden, für die Speicherberechtigung erforderlich ist. Es können Befehle ausgegeben werden, die alle vorhandenen Speicherpools sowie alle Speicherpools betreffen, die in Zukunft definiert werden. Außerdem können Befehle ausgegeben werden, die die Datenbank und das Wiederherstellungsprotokoll betreffen. Ein Administrator mit uneingeschränkter Speicherberechtigung kann Speicherpools nicht definieren oder löschen.

Mit der eingeschränkten Speicherberechtigung können Administratorbefehle ausgegeben werden, die nur einen Speicherpool betreffen, für den eine Berechtigung erteilt wurde. Der Befehl DELETE VOLUME betrifft beispielsweise nur einen Datenträger aus dem Speicherpool, der für einen bestimmten Speicherpool definiert ist.

Tabelle 1 enthält die Befehle, die ein Administrator mit Speicherberechtigung ausgeben kann.

Tabelle 1. Speicherberechtigungsbefehle

| Befehlsname   | Befehlsname  |
|---|--|
| <ul style="list-style-type: none"> <li>• AUDIT LIBRARY</li> <li>• AUDIT VOLUME (Siehe Anmerkung.)</li> <li>• BACKUP DB</li> <li>• BACKUP DEVCONFIG</li> <li>• BACKUP STGPOOL</li> <li>• BACKUP VOLHISTORY</li> <li>• CHECKIN LIBVOLUME</li> <li>• CHECKOUT LIBVOLUME</li> <li>• COPY ACTIVATEDATA (Siehe Anmerkung.)</li> <li>• DEFINE COLLOGROUP</li> <li>• DEFINE COLLOCMEMBER</li> <li>• DEFINE DATAMOVER</li> <li>• DEFINE DEVCLASS</li> <li>• DEFINE DRIVE</li> <li>• DEFINE LIBRARY</li> <li>• DEFINE PATH</li> <li>• DEFINE VIRTUALFSMAPPING</li> <li>• DEFINE VOLUME (Siehe Anmerkung.)</li> <li>• DEFINE SPACETRIGGER</li> <li>• DELETE COLLOGROUP</li> <li>• DELETE COLLOCMEMBER</li> <li>• DELETE DATAMOVER</li> <li>• DELETE DEVCLASS</li> <li>• DELETE DRIVE</li> <li>• DELETE LIBRARY</li> <li>• DELETE PATH</li> </ul> | <ul style="list-style-type: none"> <li>• DELETE SPACETRIGGER</li> <li>• DELETE VIRTUALFSMAPPING</li> <li>• DELETE VOLHISTORY</li> <li>• DELETE VOLUME (Siehe Anmerkung.)</li> <li>• GRANT PROXYNODE</li> <li>• LABEL LIBVOLUME</li> <li>• MIGRATE STGPOOL</li> <li>• MOVE DATA (Siehe Anmerkung.)</li> <li>• MOVE MEDIA</li> <li>• QUERY TAPEALERTMSG</li> <li>• RECLAIM STGPOOL</li> <li>• RESTORE STGPOOL</li> <li>• RESTORE VOLUME</li> <li>• REVOKE PROXYNODE</li> <li>• SET TAPEALERTMSG</li> <li>• UPDATE COLLOGROUP</li> <li>• UPDATE DATAMOVER</li> <li>• UPDATE DEVCLASS</li> <li>• UPDATE DRIVE</li> <li>• UPDATE LIBRARY</li> <li>• UPDATE PATH</li> <li>• UPDATE SPACETRIGGER</li> <li>• UPDATE STGPOOL (Siehe Anmerkung.)</li> <li>• UPDATE VIRTUALFSMAPPING</li> </ul> |
| <p>Anmerkung: Dieser Befehl kann durch den Speicherpool eingeschränkt werden. Ein Administrator mit uneingeschränkter Speicherberechtigung oder eingeschränkter Speicherberechtigung für einen angegebenen Speicherpool kann diesen Befehl ausgeben.</p>  |  |

## Befehle, die die Bedienerberechtigung erfordern

Ein Administrator mit Bedienerberechtigung kann Befehle ausgeben, die den direkten Betrieb des Servers und die Verfügbarkeit von Speicherdatenträgern steuern.

Tabelle 1 enthält die Befehle, die ein Administrator mit Bedienerberechtigung ausgeben kann.

Tabelle 1. Bedienerberechtigungsbefehle

| Befehlsname  | Befehlsname   |
|--|---|
| <ul style="list-style-type: none"> <li>• CANCEL SESSION</li> <li>• DISABLE SESSIONS</li> <li>• DISMOUNT VOLUME</li> <li>• ENABLE SESSIONS</li> <li>• HALT</li> </ul> | <ul style="list-style-type: none"> <li>• MOVE DRMEDIA</li> <li>• MOVE MEDIA</li> <li>• QUERY MEDIA</li> <li>• REPLY</li> <li>• UPDATE VOLUME</li> <li>• VARY</li> </ul> |

## Befehle, die jeder Administrator ausgeben kann

Eine begrenzte Anzahl von Befehlen kann von jedem Administrator verwendet werden, auch wenn er über keine speziellen Administratorberechtigungen verfügt.

Tabelle 1 enthält die Befehle, die jeder registrierte Administrator ausgeben kann.

Tabelle 1. Befehle, die von allen Administratoren ausgegeben werden

| Befehlsname  | Befehlsname   |
|--|---|
| <ul style="list-style-type: none"> <li>• COMMIT</li> <li>• HELP</li> <li>• ISSUE MESSAGE</li> <li>• MACRO</li> <li>• PARALLEL</li> <li>• QUERY ACTLOG</li> <li>• QUERY ADMIN</li> <li>• QUERY ASSOCIATION</li> <li>• QUERY AUDITOCUPANCY</li> <li>• QUERY BACKUPSET</li> <li>• QUERY CLOPTSET</li> <li>• QUERY COLLOCGROUP</li> <li>• QUERY CONTENT</li> <li>• QUERY COPYGROUP</li> <li>• QUERY DATAMOVER</li> <li>• QUERY DB</li> <li>• QUERY DBSPACE</li> <li>• QUERY DEVCLASS</li> <li>• QUERY DIRSPACE</li> <li>• QUERY DOMAIN</li> <li>• QUERY DRIVE</li> <li>• QUERY DRMEDIA</li> <li>• QUERY DRMSTATUS</li> <li>• QUERY ENABLED</li> <li>• QUERY EVENT</li> <li>• QUERY EVENTRULES</li> <li>• QUERY EVENTSERVER</li> <li>• QUERY FILESPACE</li> <li>• QUERY LIBRARY</li> <li>• QUERY LIBVOLUME</li> <li>• QUERY LICENSE</li> <li>• QUERY LOG</li> <li>• QUERY MACHINE</li> <li>• QUERY MGMTCLASS</li> <li>• QUERY MOUNT</li> <li>• QUERY NASBACKUP</li> </ul> | <ul style="list-style-type: none"> <li>• QUERY NODE</li> <li>• QUERY NODEDATA</li> <li>• QUERY NODEGROUP</li> <li>• QUERY OCCUPANCY</li> <li>• QUERY OPTION</li> <li>• QUERY PATH</li> <li>• QUERY POLICYSET</li> <li>• QUERY PROCESS</li> <li>• QUERY PROFILE</li> <li>• QUERY PROXYNODE</li> <li>• QUERY RECOVERYMEDIA</li> <li>• QUERY REPLICATION</li> <li>• QUERY REPLNODE</li> <li>• QUERY REPLRULE</li> <li>• QUERY REQUEST</li> <li>• QUERY RESTORE</li> <li>• QUERY RPFIL</li> <li>• QUERY SCHEDULE</li> <li>• QUERY SCRIPT</li> <li>• QUERY SERVER</li> <li>• QUERY SERVERGROUP</li> <li>• QUERY SESSION</li> <li>• QUERY SPACETRIGGER</li> <li>• QUERY STATUS</li> <li>• QUERY STGPOOL</li> <li>• QUERY SUBSCRIBER</li> <li>• QUERY SUBSCRIPTION</li> <li>• QUERY SYSTEM</li> <li>• QUERY</li> <li>• VIRTUALFSMAPPING</li> <li>• QUERY VOLHISTORY</li> <li>• QUERY VOLUME</li> <li>• QUIT</li> <li>• ROLLBACK</li> <li>• SELECT</li> <li>• SERIAL</li> </ul> |

## Verwaltungsbefehle

Verwaltungsbefehle sind zum Verwalten und Konfigurieren des Servers verfügbar.

Die Informationen zu jedem Befehl beinhalten

- eine Beschreibung der Tasks, die ein Befehl ausführt.
  - die für den Befehl erforderliche Administrator-Berechtigungsklasse.
  - ein Syntaxdiagramm, das die erforderlichen und wahlfreien Parameter für den Befehl kennzeichnet.
  - Beschreibungen jedes Befehlsparameters.
  - Beispiele für die Verwendung eines Befehls.
  - eine Liste der zugehörigen Befehle.
- ACCEPT DATE (Aktuelles Systemdatum akzeptieren)  
Mit diesem Befehl können Sie den Server mit der normalen Verarbeitung beginnen lassen, wenn der Server aufgrund einer Abweichung zwischen dem Serverdatum und dem aktuellen Systemdatum die normale Verarbeitung nicht startet.
  - ACTIVATE POLICYSET (Neue Maßnahmengruppe aktivieren)  
Mit diesem Befehl kann der Inhalt einer Maßnahmengruppe in die AKTIVE Maßnahmengruppe für die Domäne kopiert werden. Der Server verwendet die Regeln in der AKTIVEN Maßnahmengruppe, um Clientoperationen in der Domäne zu verwalten. Für eine Maßnahmendomäne können mehrere Maßnahmengruppen definiert werden, aber es kann nur eine Maßnahmengruppe aktiv sein. Die aktuelle AKTIVE Maßnahmengruppe wird durch die Maßnahmengruppe ersetzt, die bei Ausgabe dieses Befehls angegeben wird. Die AKTIVE Maßnahmengruppe kann nur geändert werden, indem eine andere Maßnahmengruppe aktiviert wird.

- **ASSIGN DEFMGMTCLASS** (Standardverwaltungsklasse zuordnen)  
Mit diesem Befehl kann eine Verwaltungsklasse als Standardverwaltungsklasse für eine Maßnahmengruppe angegeben werden. Es muß eine Standardverwaltungsklasse für eine Maßnahmengruppe zugeordnet werden, damit diese Maßnahmengruppe aktiviert werden kann.
- **AUDIT-Befehle**  
Mit den AUDIT-Befehlen kann die Qualität der Datenbankinformationen und der Speicherpoolatenträger überprüft oder untersucht werden. Mit dem Befehl AUDIT LDAPDIRECTORY werden Knoten oder Administrator-IDs auf einem LDAP-Verzeichnisserver gelöscht, die ihre Kennwörter nicht mit dem LDAP-Verzeichnisserver authentifizieren.
- **BACKUP-Befehle**  
Mit den BACKUP-Befehlen können Sicherungskopien der IBM Spectrum Protect-Informationen oder -Objekte erstellt werden.
- **BEGIN EVENTLOGGING** (Ereignisprotokollierung beginnen)  
Mit diesem Befehl kann das Protokollieren von Ereignissen für einen oder mehrere Empfänger begonnen werden. Ein Empfänger, für den die Ereignisprotokollierung begonnen hat, ist ein *aktiver Empfänger*.
- **CANCEL-Befehle**  
Mit den CANCEL-Befehlen kann eine Task oder ein Prozess vor der Beendigung abgebrochen werden.
- **CHECKIN LIBVOLUME** (Speicherdatenträger in ein Speicherarchiv zurückstellen)  
Mit diesem Befehl kann ein Speicherdatenträger mit sequenziellem Zugriff oder ein Reinigungsband dem Serverdatenträgerbestand für ein automatisiertes Speicherarchiv hinzugefügt werden. Der Server kann einen Datenträger, der sich physisch in einem automatisierten Speicherarchiv befindet, erst verwenden, wenn dieser Datenträger zurückgestellt wurde.
- **CHECKOUT LIBVOLUME** (Speicherdatenträger aus Kassettenarchiv entnehmen)  
Mit diesem Befehl kann ein Speicherdatenträger mit sequenziellem Zugriff aus dem Serverdatenträgerbestand für ein automatisiertes Kassettenarchiv entfernt werden. Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.
- **CLEAN DRIVE** (Laufwerk reinigen)  
Verwenden Sie diesen Befehl, wenn IBM Spectrum Protect unabhängig von der Reinigungshäufigkeit sofort eine Reinigungskassette in ein Laufwerk laden soll.
- **COMMIT** (Festschreiben von Befehlen in einem Makro steuern)  
Mit diesem Befehl kann das Festschreiben eines Befehls in einem Makro gesteuert und die Datenbank nach der Verarbeitung von Befehlen aktualisiert werden. Wird dieser Befehl im Konsolenmodus des Verwaltungsclients ausgegeben, wird keine Nachricht generiert.
- **CONVERT STGPOOL** (Speicherpool in einen Containerspeicherpool konvertieren)  
Mit diesem Befehl können Sie einen primären Speicherpool, der eine Einheitenklasse FILE, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet, in einen Verzeichniscontainerspeicherpool oder einen Cloud-Containerspeicherpool konvertieren. Sie können Containerspeicherpools sowohl für die Inline-Datendeduplizierung als auch für die clientseitige Datendeduplizierung verwenden.
- **COPY-Befehle**  
Mit den COPY-Befehlen kann eine Kopie von IBM Spectrum Protect-Objekten oder -Daten erstellt werden.
- **DEACTIVATE DATA** (Daten für einen Clientknoten inaktivieren)  
Mit diesem Befehl können Sie angeben, dass aktive Daten, die für einen Anwendungsclientknoten vor einem angegebenen Datum gesichert wurden, nicht mehr benötigt werden. Der Befehl markiert die Daten als inaktiv, sodass sie gemäß Ihren Datenaufbewahrungsmaßnahmen gelöscht werden können.
- **DECOMMISSION-Befehle**  
Verwenden Sie die DECOMMISSION-Befehle, um Clientknoten aus der Produktionsumgebung zu entfernen. Clientknoten umfassen Anwendungen, Systeme und virtuelle Maschinen.
- **DEFINE-Befehle**  
Mit den DEFINE-Befehlen können IBM Spectrum Protect-Objekte erstellt werden.
- **DELETE-Befehle**  
Mit den DELETE-Befehlen kann ein IBM Spectrum Protect-Objekt gelöscht oder entfernt werden.
- **DISABLE-Befehle**  
Mit den DISABLE-Befehlen können Sie einige durch den Server ausgeführte Operationstypen verhindern.
- **DISMOUNT-Befehl**  
Mit dem Befehl DISMOUNT kann ein Datenträger nach der Adresse der realen Einheit oder nach dem Datenträgernamen entladen werden.
- **DISPLAY OBJNAME** (Vollständigen Objektnamen anzeigen)  
Mit diesem Befehl kann IBM Spectrum Protect einen vollständigen Objektnamen anzeigen, wenn der in einer Nachricht oder in einer Abfrageausgabe angezeigte Name aufgrund der Länge abgekürzt wurde. Objektnamen, die sehr lang sind, sind über normale Betriebssystemfunktionen schwer anzuzeigen und zu verwenden. Der IBM Spectrum Protect-Server kürzt lange Namen ab und ordnet ihnen eine Token-ID zu, die verwendet werden kann, wenn der Objektname 1024 Byte überschreitet. Die Token-ID wird in einer Zeichenfolge angezeigt, die IDs für den Knoten, den Dateibereich und den Objektnamen einschließt. Das Format ist: [TSMOBJ:nID.fsID.objID]. Bei Angabe mit dem Befehl DISPLAY OBJNAME kann die Token-ID verwendet werden, um den vollständigen Objektnamen anzuzeigen.
- **ENABLE-Befehle**  
Mit den ENABLE-Befehlen können Sie einige durch den Server ausgeführte Operationstypen zulassen.

- ENCRYPT STGPOOL (Daten in einem Speicherpool verschlüsseln)  
Mit diesem Befehl können Daten in einem Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool verschlüsselt werden.
- END EVENTLOGGING (Ereignisprotokollierung stoppen)  
Mit diesem Befehl kann das Protokollieren von Ereignissen für einen aktiven Empfänger gestoppt werden.
- EXPIRE INVENTORY (Datenträgerbestandsverfall manuell starten)  
Mit diesem Befehl kann die Verarbeitung des Datenträgerbestandsverfalls manuell gestartet werden. Beim Bestandsverfallsprozess werden Kopien von Clientsicherungs- und Archivierungsdateien aus dem Serverspeicher entfernt. Das Entfernen basiert auf Maßnahmenspezifikationen in den Sicherungs- und Archivierungskopiengruppen der Verwaltungsklassen, an die die Dateien gebunden sind.
- EXPORT-Befehle  
Mit den EXPORT-Befehlen können Informationen von einem IBM Spectrum Protect-Server auf sequenzielle austauschbare Datenträger kopiert werden.
- EXTEND DBSPACE (Speicherbereich für die Datenbank erhöhen)  
Verwenden Sie diesen Befehl, um den Speicherbereich für die Datenbank zu vergrößern, indem Verzeichnisse für die Datenbank hinzugefügt werden.
- GENERATE-Befehle  
Verwenden Sie die GENERATE-Befehle für Sicherungsgruppen für einen ausgewählten Dateibereich oder Clientknoten.
- GRANT-Befehle  
Verwenden Sie den Befehl GRANT, um entsprechende Berechtigungen oder entsprechenden Zugriff zu erteilen.
- HALT (Server abschalten)  
Mit diesem Befehl kann der Server abgeschaltet werden. Der Befehl HALT erzwingt ein sofortiges Abschalten, wobei alle Verwaltungs- und Clientknotensitzungen abgebrochen werden, auch wenn sie noch nicht beendet sind.
- HELP (Hilfe für Befehle und Fehlernachrichten anfordern)  
Mit diesem Befehl können Verwaltungsbefehle und Fehlernachrichten angezeigt werden. Der Befehl kann von einem Verwaltungsbefehlszeilenclient ausgegeben werden.
- IDENTIFY DUPLICATES (Doppelte Daten in einem Speicherpool identifizieren)  
Verwenden Sie diesen Befehl, um Prozesse zu starten oder zu stoppen, die doppelte Daten in einem Speicherpool identifizieren. Sie können die Anzahl der Prozesse zum Identifizieren doppelter Daten und ihre Dauer angeben.
- Befehle IMPORT  
Mit den IMPORT-Befehlen können Informationen von Exportdatenträgern auf einen IBM Spectrum Protect-Server importiert werden.
- INSERT MACHINE (Maschinenkenndaten oder Wiederh.-Anweisungen einfügen)  
Mit diesem Befehl können vorhandenen Maschineninformationen in der Datenbank Client-Maschinenkenndaten oder Wiederherstellungsanweisungen hinzugefügt werden.
- ISSUE MESSAGE (Nachricht aus einem Server-Script ausgeben)  
Diesen Befehl mit Rückkehrcodeverarbeitung in einem Script verwenden, um eine Nachricht aus einem Server-Script auszugeben, mit der die Fehlerquelle bei einem Befehl in dem Script bestimmt wird.
- LABEL LIBVOLUME (Datenträger im Kassettenarchiv Kennsatz zuordnen)  
Mit diesem Befehl kann Banddatenträgern ein Kennsatz zugeordnet werden; in einem automatisierten Kassettenarchiv wird den Datenträgern automatisch beim Zurückstellen ein Kennsatz zugeordnet. Mit diesem Befehl verwendet der Server den Kennsatz mit vollständiger Länge, mit dem die Datenträger häufig vorgekennzeichnet sind.
- LOAD DEFALERTTRIGGERS (Standardgruppe von Alertauslösern laden)  
Verwenden Sie diesen Befehl, um die Standardgruppe von Alertauslösern auf den IBM Spectrum Protect-Server zu laden.
- LOCK-Befehle  
Mit den LOCK-Befehlen kann der Benutzerzugriff auf den Server verhindert werden.
- MACRO (Makro aufrufen)  
Mit diesem Befehl kann eine Datei über die Verwaltungsbefehlszeile aufgerufen werden, die auszuführende IBM Spectrum Protect-Verwaltungsbefehle enthält.
- MIGRATE STGPOOL (Speicherpool in nächsten Speicherpool umlagern)  
Mit diesem Befehl können Dateien aus einem Speicherpool in den nächsten Speicherpool in der Speicherhierarchie umgelagert werden.
- MOVE-Befehle  
Mit den MOVE-Befehlen können Sicherungs- oder Archivierungsdaten zwischen Speicherpools oder Datenträger zur Wiederherstellung nach einem Katastrophenfall vor Ort und an einen ausgelagerten Standort versetzt werden.
- NOTIFY SUBSCRIBERS (Verwaltete Server auf Profilaktualisierung hinweisen)  
Mit diesem Befehl können auf einem Konfigurationsmanager ein oder mehrere verwaltete Server benachrichtigt werden, dass ihre Konfigurationsdaten sofort aktualisiert werden müssen.
- PERFORM LIBACTION (Alle Laufwerke und Pfade für ein Kassettenarchiv definieren oder löschen)  
Verwenden Sie diesen Befehl, um alle Laufwerke und ihre Pfade für ein einzelnes Kassettenarchiv in einem Schritt zu definieren oder zu löschen.
- PING SERVER (Verbindung zwischen Servern testen)  
Mit diesem Befehl kann die Verbindung zwischen dem lokalen Server und einem fernen Server getestet werden.
- PREPARE (Wiederherstellungsplandatei erstellen)  
Mit diesem Befehl kann eine Wiederherstellungsplandatei erstellt werden, die die für die Wiederherstellung eines IBM Spectrum

- Protect-Servers erforderlichen Daten enthält. Eine Wiederherstellungsplandatei kann in einem Dateisystem gespeichert werden, auf das vom Quellenserver oder einem Zielservers zugriffen werden kann.
- PROTECT STGPOOL (Daten schützen, die zu einem Speicherpool gehören)  
Verwenden Sie diesen Befehl, um Daten in einem Verzeichniscontainerspeicherpool zu schützen, indem eine Kopie der Daten in einem anderen Speicherpool auf einem Zielreplikationsserver oder auf demselben Server gespeichert wird und die Daten auf Band geschützt werden. Wenn Sie den Verzeichniscontainerspeicherpool schützen, können Sie später mithilfe des Befehls REPAIR STGPOOL versuchen, beschädigte Daten in dem Speicherpool zu reparieren.
  - QUERY-Befehle  
Mit den QUERY-Befehlen können Informationen zu IBM Spectrum Protect-Objekten angefordert oder angezeigt werden.
  - QUIT (Interaktiven Modus des Verwaltungsclient verlassen)  
Mit diesem Befehl kann eine Verwaltungs-Client-Sitzung im interaktiven Modus beendet werden.
  - RECLAIM STGPOOL (Datenträger im Speicherpool mit sequenziellem Zugriff wiederherstellen)  
Verwenden Sie diesen Befehl, um Datenträger in einem Speicherpool mit sequenziellem Zugriff wiederherzustellen. Bei der Wiederherstellung werden keine inaktiven Versionen von Sicherungsdaten von Datenträgern in Pools für aktive Daten versetzt.
  - RECONCILE VOLUMES (Unterschiede abstimmen)  
Diesen Befehl vom Quellen-Server ausgeben, um Unterschiede zwischen den Definitionen der virtuellen Datenträger auf dem Quellen-Server und den Archivierungsdateien auf dem Ziel-Server abzustimmen. IBM Spectrum Protect sucht alle Datenträger mit der angegebenen Einheitenklasse auf dem Quellen-Server und alle entsprechenden Archivierungsdateien auf dem Ziel-Server. Der Datenträgerbestand auf dem Ziel-Server wird auch mit der lokalen Definition für virtuelle Datenträger verglichen, um festzustellen, ob Inkonsistenzen vorhanden sind.
  - REGISTER-Befehle  
Mit den REGISTER-Befehlen können Objekte in IBM Spectrum Protect definiert oder hinzugefügt werden.
  - REMOVE-Befehle  
Mit den REMOVE-Befehlen kann ein Objekt aus IBM Spectrum Protect entfernt werden.
  - RENAME-Befehle  
Mit den RENAME-Befehlen kann der Name eines vorhandenen Objekts geändert werden.
  - REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)  
Mit diesem Befehl können deduplizierte Speicherbereiche in einem Verzeichniscontainerspeicherpool repariert werden. Beschädigte deduplizierte Speicherbereiche werden mit Bereichen repariert, die auf dem Zielreplikationsserver oder in Containerkopierspeicherpools auf demselben Server gesichert werden.
  - REPLICATE NODE (Daten in Dateibereichen replizieren, die zu einem Clientknoten gehören)  
Verwenden Sie diesen Befehl, um Daten in Dateibereichen zu replizieren, die zu einem oder mehreren Clientknoten oder zu definierten Gruppen von Clientknoten gehören.
  - REPLY (Verarbeitung einer Anforderung fortsetzen)  
Mit Hilfe dieses Befehls und einer Identifikationsnummer kann der Server darüber informiert werden, dass eine angeforderte Operation beendet wurde. Nicht alle Serveranforderungen erfordern eine Antwort. Dieser Befehl ist nur erforderlich, wenn die Anforderungsnachricht ausdrücklich angibt, dass eine Antwort benötigt wird.
  - RESET PASSEXP (Kennwortablaufdauer zurücksetzen)  
Verwenden Sie den Befehl RESET PASSEXP, um die Kennwortablaufdauer für Kennwörter von Administratoren und Clientknoten auf die allgemeine Kennwortablaufdauer zurückzusetzen. Der Befehl RESET PASSEXP gilt nicht für Kennwörter, die auf einem LDAP-Verzeichnisserver gespeichert werden.
  - RESTART EXPORT (Ausgesetzte Exportoperation erneut starten)  
Mit diesem Befehl kann eine ausgesetzte Exportoperation erneut gestartet werden.
  - RESTORE-Befehle  
Mit den RESTORE-Befehlen können IBM Spectrum Protect-Speicherpools oder -Datenträger zurückgeschrieben werden.
  - REVOKE-Befehle  
Mit den REVOKE-Befehlen können Sie Berechtigungen oder den Zugriff widerrufen.
  - ROLLBACK (Nicht festgeschriebene Änderungen in einem Makro rückgängig machen)  
Mit diesem Befehl können innerhalb eines Makros Änderungen rückgängig gemacht werden, die von Befehlen, die vom Server ausgeführt wurden, vorgenommen, jedoch noch nicht in der Datenbank festgeschrieben wurden. Eine festgeschriebene Änderung ist permanent und kann nicht rückgängig gemacht werden. Der Befehl ROLLBACK ist für das Testen von Makros nützlich.
  - RUN (IBM Spectrum Protect-Prozedur ausführen)  
Mit diesem Befehl kann eine IBM Spectrum Protect-Prozedur ausgeführt werden. Soll dieser Befehl auf einem anderen Server ausgegeben werden, muß die Prozedur, die ausgeführt wird, auf diesem Server definiert sein.
  - SELECT (SQL-Abfrage für die IBM Spectrum Protect-Datenbank ausführen)  
Verwenden Sie den Befehl SELECT, um eine angepasste Abfrage der IBM Spectrum Protect-Datenbank zu erstellen und zu formatieren.
  - SET-Befehle  
Mit den SET-Befehlen können Sie Werte angeben, die viele verschiedene IBM Spectrum Protect-Operationen betreffen.
  - SETOPT (Serveroption für dynamisches Aktualisieren definieren)  
Mit dem Befehl SETOPT können Sie die meisten Serveroptionen dynamisch aktualisieren, ohne den Server zu stoppen und erneut zu starten. Für die Option DBDIAGLOGSIZE müssen Sie den Server stoppen und erneut starten. Ein Befehl SETOPT, der in einem Makro oder in einer Prozedur enthalten ist, kann nicht rückgängig gemacht werden.
  - SHRED DATA (Daten schreddern)  
Verwenden Sie diesen Befehl, um den Prozess zum Schreddern gelöschter sensibler Daten manuell zu starten. Das manuelle

- Schreddern ist nur möglich, wenn das automatische Schreddern inaktiviert ist.
- SUSPEND EXPORT** (Momentan aktive Exportoperation aussetzen)  
Mit diesem Befehl können Sie eine momentan aktive Exportoperation zwischen Servern aussetzen, die einen anderen FILEDATA-Wert als NONE hat. Die Exportoperation, die ausgesetzt werden soll, muss nach der Initialisierungsphase liegen, um für die Aussetzung ausgewählt werden zu können. Der Status der Exportoperation wird gespeichert. Die Operation kann mit dem Befehl RESTART EXPORT erneut gestartet werden.
- UNLOCK-Befehle**  
Verwenden Sie die UNLOCK-Befehle, um den Zugriff erneut einzurichten, nachdem ein Objekt gesperrt wurde.
- UPDATE-Befehle**  
Mit den UPDATE-Befehlen können ein oder mehrere Attribute eines vorhandenen IBM Spectrum Protect-Objekts geändert werden.
- VALIDATE-Befehle**  
Mit dem Befehl VALIDATE kann überprüft werden, ob ein Objekt für IBM Spectrum Protect vollständig oder gültig ist.
- VARY** (Datenträger mit wahlfreiem Zugriff an-/abhängen)  
Mit diesem Befehl kann ein Speicherpooldatenträger mit wahlfreiem Zugriff für den Server angehängt oder abgehängt werden.

## ACCEPT DATE (Aktuelles Systemdatum akzeptieren)

Mit diesem Befehl können Sie den Server mit der normalen Verarbeitung beginnen lassen, wenn der Server aufgrund einer Abweichung zwischen dem Serverdatum und dem aktuellen Systemdatum die normale Verarbeitung nicht startet.

Wenn der Server aufgrund einer Abweichung zwischen dem Serverdatum und dem aktuellen Datum die normale Verarbeitung nicht startet, wird mit diesem Befehl der Server gezwungen, das aktuelle Datum und die aktuelle Uhrzeit als gültig zu akzeptieren. Ist die Systemzeit gültig und wurde der Server längere Zeit nicht ausgeführt, sollte dieser Befehl ausgeführt werden, um es dem Server zu ermöglichen, mit der normalen Verarbeitung zu beginnen.

Achtung: Ist das Systemdatum ungültig oder wurde der Server zuvor mit einem ungültigen Systemdatum erstellt oder ausgeführt und wird dieser Befehl ausgegeben, kann jede Serververarbeitung oder jeder Befehl, die bzw. der Datumsangaben verwendet, zu unerwarteten Ergebnissen führen. Beispielsweise kann die Dateiverfallsverarbeitung betroffen sein. Wird der Server mit dem korrekten Datum gestartet, werden Dateien, die mit zukünftigen Datumsangaben gesichert wurden, erst dann für die Verfallsverarbeitung berücksichtigt, wenn dieses zukünftige Datum erreicht wird. Dateien, die mit zurückliegenden Datumsangaben gesichert wurden, verfallen schneller. Wenn die Serververarbeitung ein zukünftiges Datum erkennt, wird eine Fehlernachricht ausgegeben.

Wenn der Server ein ungültiges Datum oder eine ungültige Uhrzeit erkennt, werden Serversitzungen inaktiviert (wie bei der Ausgabe des Befehls DISABLE SESSIONS). Die Verarbeitung von Verfalls-, Umlagerungs- und Wiederherstellungsoperationen sowie von Operationen zum Löschen der Datenträgerhistory kann nicht fortgesetzt werden.

Verwenden Sie den Befehl ENABLE SESSIONS ALL nach der Ausgabe des Befehls ACCEPT DATE, um Sitzungen für den Start erneut zu aktivieren.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-ACcEpt Date-----<<
```

### Parameter

Keine.

### Beispiel: Das aktuelle Systemdatum akzeptieren

Dem Server das Akzeptieren des aktuellen Datums als gültiges Datum erlauben.

```
accept date
```

### Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für ACCEPT DATE

| Befehl | Beschreibung |
|--------|--------------|
|--------|--------------|



| Befehl          | Beschreibung   |
|-----------------|--|
| ENABLE SESSIONS | Nimmt die Serveraktivität nach einem Befehl DISABLE oder ACCEPT DATE wieder auf. |

## ACTIVATE POLICYSET (Neue Maßnahmengruppe aktivieren)

Mit diesem Befehl kann der Inhalt einer Maßnahmengruppe in die AKTIVE Maßnahmengruppe für die Domäne kopiert werden. Der Server verwendet die Regeln in der AKTIVEN Maßnahmengruppe, um Clientoperationen in der Domäne zu verwalten. Für eine Maßnahmendomäne können mehrere Maßnahmengruppen definiert werden, aber es kann nur eine Maßnahmengruppe aktiv sein. Die aktuelle AKTIVE Maßnahmengruppe wird durch die Maßnahmengruppe ersetzt, die bei Ausgabe dieses Befehls angegeben wird. Die AKTIVE Maßnahmengruppe kann nur geändert werden, indem eine andere Maßnahmengruppe aktiviert wird.

Bevor eine Maßnahmengruppe aktiviert wird, muss mit dem Befehl VALIDATE POLICYSET geprüft werden, ob die Maßnahmengruppe vollständig und gültig ist.

Der Befehl ACTIVATE POLICYSET schlägt fehl, wenn eine der folgenden Bedingungen vorhanden ist:

- Eine Kopiengruppe gibt einen Kopierspeicherpool als Zielort an.
- Eine Verwaltungsklasse gibt einen Kopierspeicherpool als Zielort für Dateien an, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.
- Die Maßnahmengruppe hat keine Standardverwaltungsklasse.
- Ein Parameter TOCDESTINATION ist angegeben, und der Speicherpool ist entweder ein Kopienpool oder der Speicherpool hat ein anderes Format als NATIVE oder NONBLOCK.

Die AKTIVE Maßnahmengruppe und die letzte aktivierte Maßnahmengruppe müssen nicht notwendigerweise identisch sein. Die ursprüngliche Maßnahmengruppe, die aktiviert wurde, kann ohne Auswirkungen auf die AKTIVE Maßnahmengruppe geändert werden.

Ist für den Server der Aufbewahrungsschutz für Daten aktiviert, müssen die folgenden Bedingungen zutreffen:

- Alle Verwaltungsklassen in der Maßnahmengruppe, die aktiviert werden soll, müssen eine Archivierungskopiengruppe enthalten.
- Ist eine Verwaltungsklasse in der aktiven Maßnahmengruppe vorhanden, muss eine Verwaltungsklasse mit demselben Namen in der Maßnahmengruppe vorhanden sein, die aktiviert werden soll.
- Ist eine Archivierungskopiengruppe in der aktiven Maßnahmengruppe vorhanden, muss die entsprechende Kopiengruppe in der zu aktivierenden Maßnahmengruppe über einen Wert für RETVER verfügen, der mindestens so groß wie die entsprechenden Werte in der aktiven Kopiengruppe ist.

Achtung: Der Aufbewahrungsschutz gilt nur für Archivierungsobjekte.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Maßnahmengruppe gehört.

### Syntax

```
>>-ACTivate Policyset--Domänenname--Name_der_Maßnahmengruppe---<<
```

### Parameter

Domänenname (Erforderlich)

Gibt die Maßnahmendomäne an, für die eine Maßnahmengruppe aktiviert werden soll.

Name\_der\_Maßnahmengruppe (Erforderlich)

Gibt die Maßnahmengruppe an, die aktiviert werden soll.

### Beispiel: Eine Maßnahmengruppe für eine bestimmte Maßnahmendomäne aktivieren

Die Maßnahmengruppe VACATION in der Maßnahmendomäne EMPLOYEE\_RECORDS aktivieren.

```
activate policyset employee_records vacation
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für ACTIVATE POLICYSET

| Befehl             | Beschreibung  |
|--------------------|---|
| COPY POLICYSET     | Erstellt eine Kopie einer Maßnahmengruppe.  |
| DEFINE POLICYSET   | Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.   |
| DELETE POLICYSET   | Löscht eine Maßnahmengruppe einschließlich ihrer Verwaltungsklassen und Kopiengruppen aus einer Maßnahmendomäne.        |
| QUERY DOMAIN       | Zeigt Informationen über Maßnahmendomänen an.   |
| QUERY POLICYSET    | Zeigt Informationen über Maßnahmengruppen an.   |
| UPDATE POLICYSET   | Ändert die Beschreibung einer Maßnahmengruppe.  |
| VALIDATE POLICYSET | Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert. |

## ASSIGN DEFMGMTCLASS (Standardverwaltungsklasse zuordnen)

Mit diesem Befehl kann eine Verwaltungsklasse als Standardverwaltungsklasse für eine Maßnahmengruppe angegeben werden. Es muß eine Standardverwaltungsklasse für eine Maßnahmengruppe zugeordnet werden, damit diese Maßnahmengruppe aktiviert werden kann.

Um sicherzustellen, dass Clients immer Dateien sichern und archivieren können, wählen Sie eine Standardverwaltungsklasse aus, die sowohl eine Archivierungskopiengruppe als auch eine Sicherungskopiengruppe enthält.

Der Server verwendet die Standardverwaltungsklasse, um Clientdateien zu verwalten, wenn keine Verwaltungsklasse zugeordnet oder geeignet ist. Beispielsweise verwendet der Server die Standardverwaltungsklasse, wenn ein Benutzer keine Verwaltungsklasse in der Einschluss-/Ausschlussliste angibt.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Maßnahmengruppe gehört.

### Syntax

```
>>-ASsign DEFMGmtclass--Domänenname--Name_der_Maßnahmengruppe--Klassenname-><
```

### Parameter

Domänenname (Erforderlich)

Gibt die Maßnahmendomäne an, zu der die Verwaltungsklasse gehört.

Name\_der\_Maßnahmengruppe (Erforderlich)

Gibt die Maßnahmengruppe an, für die die Standardverwaltungsklasse zugeordnet werden soll. Für die aktive Maßnahmengruppe (ACTIVE) kann keine Standardverwaltungsklasse zugeordnet werden.

Klassenname (Erforderlich)

Gibt die Verwaltungsklasse an, die als Standardverwaltungsklasse für die Maßnahmengruppe verwendet werden soll.

### Beispiel: Eine Standardverwaltungsklasse zuordnen

DEFAULT1 als Standardverwaltungsklasse für Maßnahmengruppe SUMMER in der Maßnahmendomäne PROG1 zuordnen.

```
assign defmgmtclass prog1 summer default1
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für ASSIGN DEFMGMTCLASS

| Befehl             | Beschreibung                                       |
|--------------------|--|
| ACTIVATE POLICYSET | Wertet eine Maßnahmengruppe aus und aktiviert sie. |

| Befehl             | Beschreibung  |
|--------------------|---|
| DEFINE COPYGROUP   | Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse. |
| DEFINE MGMTCLASS   | Definiert eine Verwaltungsklasse.   |
| DEFINE POLICYSET   | Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.   |
| DELETE MGMTCLASS   | Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe.                     |
| QUERY COPYGROUP    | Zeigt die Attribute einer Kopiengruppe an.  |
| QUERY MGMTCLASS    | Zeigt Informationen zu Verwaltungsklassen an.   |
| QUERY POLICYSET    | Zeigt Informationen über Maßnahmengruppen an.   |
| UPDATE COPYGROUP   | Ändert ein oder mehrere Attribute einer Kopiengruppe.   |
| UPDATE MGMTCLASS   | Ändert die Attribute einer Verwaltungsklasse.   |
| VALIDATE POLICYSET | Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert.       |

## AUDIT-Befehle

Mit den AUDIT-Befehlen kann die Qualität der Datenbankinformationen und der Speicherpooldatenträger überprüft oder untersucht werden. Mit dem Befehl AUDIT LDAPDIRECTORY werden Knoten oder Administrator-IDs auf einem LDAP-Verzeichnisserver gelöscht, die ihre Kennwörter nicht mit dem LDAP-Verzeichnisserver authentifizieren.

- AUDIT CONTAINER
  - AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Cloud-Container prüfen)
  - AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)
- AUDIT LDAPDIRECTORY (LDAP-Verzeichnisserver prüfen)
- AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Kassettenarchiv prüfen)
- AUDIT LIBVOLUME (Datenbankinformationen für einen Banddatenträger prüfen)
- AUDIT LICENSES (Serverspeicherbelegung prüfen)
- AUDIT VOLUME (Datenbankinformationen für Speicherpooldatenträger prüfen)

## AUDIT CONTAINER-Befehle

Mit dem Befehl AUDIT CONTAINER können Sie nach Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Cloud- oder Verzeichnisspeicherpool suchen.

- AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Cloud-Container prüfen)  
Mit diesem Befehl können Sie nach Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Cloud-Containerspeicherpool suchen. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.
- AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)  
Mit diesem Befehl können Sie nach Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Verzeichniscontainerspeicherpool suchen.

## AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Cloud-Container prüfen)

Mit diesem Befehl können Sie nach Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Cloud-Containerspeicherpool suchen. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.

Mit diesem Befehl können Sie die folgenden Aktionen für einen Container in einem Cloud-Containerspeicherpool ausführen:

- Den Inhalt eines Containers durchsuchen, um die Integrität der Datenbereiche zu überprüfen
- Daten aus einem Container entfernen, der als *beschädigt* markiert ist, wenn beispielsweise eine Datei Verweise in der Serverdatenbank hat, aber fehlende oder beschädigte Daten in der Cloud hat

- Einen vollständigen Container als beschädigt markieren
- Daten entfernen, die als *verwaist* markiert sind, wenn beispielsweise ein in der Cloud gespeichertes Objekt keinen Verweis in der Serverdatenbank hat

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-AUDit Container--+-Containername-----+-->
                    +-STGpool---+Poolname-----+
                    '-STGpool---+Poolname--STGPOOLDIRectory---+Verzeichnisname-'

.-Action----SCANAll-----.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-Action----+SCANAll-----+'
                    +-REMOVEDamaged-+
                    +-MARKDamaged---+
                    '-SCANDamaged---'

.-FORCEOrphandbdel-----No-----.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-FORCEOrphandbdel---+-No---+'
                         '-Yes-'

.-MAXProcess---4-----.-Wait---No-----.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-MAXProcess---Anzahl-' '-Wait---+No---+'
                                 '-Yes-'

.-BEGINDate---+vor der ersten Prüfung-.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-BEGINDate---+Anfangsdatum-----'

.-BEGINTime---00:00:00----.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-BEGINTime---+Anfangszeit-'

.-ENDDate---+nach der letzten Prüfung-.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-ENDDate---+Enddatum-----'

.-ENDTime---23:59:59-.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-ENDTime---+Endzeit--'
```

## Parameter

### Containername

Gibt den Namen des Containers an, der geprüft werden soll. Wird dieser Parameter nicht angegeben, müssen Sie einen Cloud-Containerspeicherpool angeben.

### STGpool

Gibt den Namen des Cloud-Containerspeicherpools an, der geprüft werden soll. Dieser Parameter ist wahlfrei. Wird nur dieser Parameter angegeben, werden alle Container geprüft, die für den Speicherpool definiert sind. Wird dieser Parameter nicht angegeben, müssen Sie einen Container angeben.

### STGPOOLDIRectory

Gibt den Namen des Cloud-Containerspeicherpoolverzeichnisses an, das geprüft werden soll. Dieser Parameter ist wahlfrei. Einschränkung: Sie müssen einen Speicherpool angeben, der lokalen Speicher verwendet.

### Aktion

Gibt an, welche Aktion der Server ausführt, wenn ein Container in einem Cloud-Containerspeicherpool geprüft wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

#### SCANAll

Gibt an, dass der Server Datenbanksätze identifiziert, die sich auf Datenbereiche mit Inkonsistenzen beziehen. Es erfolgt eine Überprüfung auf Daten im Cloud-Containerspeicherpool, die nicht mit den Daten in der Serverdatenbank übereinstimmen. Dieser Wert ist der Standardwert. Der Server markiert den Datenbereich in der Datenbank als beschädigt. Tipp: Wenn Sie den Parameter ACTION=SCANALL für einen IBM® Cloud Object Storage-Speicherpool angeben, der eine Vault mit inaktiverter Namensindexierung verwendet, wird bei der Prüfoperation die gesamte Vault durchsucht, um

verwaiste Bereiche in jedem Container zu identifizieren. Geben Sie in dieser Situation WAIT=YES an, wenn die Prüfoperation auf die Beendigung der Suche nach verwaisten Bereichen warten soll, bevor die Prüfung als abgeschlossen zurückgemeldet wird. Diese Suche nach verwaisten Bereichen erfolgt nur, wenn Sie keinen Containernamen angeben. Wenn Sie einen Container angeben, der sich in einer Vault mit inaktiver Namensindexierung befindet, sucht die Prüfoperation nicht nach verwaisten Bereichen.

**REMOVEDamaged**

Gibt an, dass der Server alle Referenzen auf beschädigte Bereiche aus der Serverdatenbank entfernt. Falls gefunden, werden die beschädigten Bereiche auch aus dem Cloud-Containerspeicherpool entfernt. Der Server entfernt auch alle verwaisten Bereiche aus dem Cloud-Containerspeicherpool und entfernt die Referenzen auf diese verwaisten Bereiche aus der Datenbank, wie mit dem Parameter FORCEORPHANDBDEL angegeben ist.

**MARKDaged**

Gibt an, dass der Server explizit alle Datenbereiche in dem Container als beschädigt markiert.

**SCANDamaged**

Gibt an, dass der Server nur die vorhandenen beschädigten Bereiche in dem Container überprüft.

Wichtig: Wenn keine Verbindung zur Cloud vorhanden ist, werden die Parameter ACTION=SCANALL und ACTION=SCANDAMAGED nicht ausgeführt. Der Parameter ACTION=MARKDAMAGED wird jedoch ohne eine Cloudverbindung wie erwartet ausgeführt, und der Parameter ACTION=REMOVEDAMAGED markiert alle beschädigten Daten als verwaist. Sobald die Verbindung zur Cloud wieder hergestellt wurde, löscht der Server die verwaisten Bereiche.

Statusrücksetzbedingung: Wenn bei der Prüfung kein Fehler bei einem Datenbereich erkannt wird, der als beschädigt markiert ist, wird der Status des Datenbereichs zurückgesetzt. Der Datenbereich kann dann verwendet werden. Diese Bedingung bietet eine Möglichkeit, den Status von beschädigten Datenbereichen zurückzusetzen, wenn Fehler durch ein korrigierbares Problem verursacht werden. Die Optionen SCANALL und SCANDAMAGED sind die einzigen Optionen, die einen beschädigten Bereich zurücksetzen, wenn festgestellt wird, dass der Bereich nicht beschädigt ist.

**FORCEOrphandbdel**

Gibt an, dass der Server das Löschen von verwaisten Bereichen aus der Serverdatenbank erzwingt, auch wenn sie nicht aus dem Cloud-Containerspeicherpool gelöscht werden. Dieser Parameter ist wahlfrei. Wenn Sie diesen Parameter angeben, müssen Sie auch den Parameter ACTION=REMOVEDAMAGED angeben. Folgende Optionen sind verfügbar:

**Yes**

Gibt an, dass der Server alle verwaisten Bereiche aus der Serverdatenbank löscht, auch wenn sie nicht aus dem Cloud-Containerspeicherpool gelöscht werden.

**No**

Gibt an, dass der Server die verwaisten Bereiche in der Serverdatenbank behält, wenn sie nicht aus dem Cloud-Containerspeicherpool gelöscht werden können. Dieser Wert ist der Standardwert.

**MAXProcess**

Gibt die maximale Anzahl paralleler Prozesse für die Überprüfung eines Containers in einem Cloud-Containerspeicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert im Bereich von 1 bis 99 ein. Der Standardwert ist 4.

Einschränkung: Der Server ignoriert diesen Parameter, wenn Sie MAXPROCESS mit dem Parameter ACTION=REMOVEDAMAGED verwenden.

**Wait**

Gibt an, ob die Prüfoperation im Vordergrund oder im Hintergrund ausgeführt wird. Dieser Parameter ist wahlfrei. Folgende Optionen sind verfügbar:

**No**

Gibt an, dass die Operation im Hintergrund ausgeführt wird. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden. Dieser Wert ist der Standardwert.

**Yes**

Gibt an, dass die Operation im Vordergrund ausgeführt wird. Die Ausführung der Operation nimmt unter Umständen viel Zeit in Anspruch. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.

Einschränkung: Sie können den Parameter WAIT=YES nicht an der Serverkonsole angeben.

**BEGINDate**

Gibt den Datumsbereichswert an, bei dem die Prüfung gestartet werden soll. Container, die zuletzt innerhalb des angegebenen Datumsbereichs geprüft wurden, werden geprüft. Wenn Sie eine Uhrzeit, aber kein Anfangsdatum angeben, wird das aktuelle Datum verwendet. Wenn Sie kein Anfangs- und Enddatum angeben, werden alle Container geprüft. Der Standardwert ist das Datum vor der Ausführung der ersten Prüfung für den Container. Dieser Parameter ist wahlfrei.

Sie können die Uhrzeit, zu der die Prüfung beginnen soll, wie folgt angeben:

| Wert       | Beschreibung          | Beispiel   |
|------------|-----------------------|------------|
| MM/TT/JJJJ | Ein bestimmtes Datum. | 09/15/2016 |

| Wert                           | Beschreibung   | Beispiel  |
|--------------------------------|--|---|
| TODAY                          | Das aktuelle Datum.  | TODAY   |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY-7 <i>oder</i> -7.<br>Um alle Container zu prüfen, die in der letzten Woche geprüft wurden, geben Sie BEGINDATE=TODAY-7 oder BEGINDATE= -7 an. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM  |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br>Um Container einzuschließen, die am Tag vor dem letzten Tag des Vormonats geprüft wurden.   |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM  |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br>Um Container einzuschließen, die am zehnten Tag des aktuellen Monats geprüft wurden.  |

#### BEGINTime

Gibt den Zeitbereichswert an, bei dem die Prüfung gestartet werden soll. Container, die zuletzt innerhalb des angegebenen Zeitbereichs geprüft wurden, werden geprüft. Wenn Sie keine Anfangs- und Endzeit angeben, wird der Zeitbereich auf 00:00:00 bis 23:59:59 gesetzt. Der Standardwert ist 00:00:00. Wenn Sie keinen Datumsbereich angegeben haben, ist der Standardwert das heutige Datum. Dieser Parameter ist wahlfrei.

Sie können die Uhrzeit, zu der die Prüfung beginnen soll, wie folgt angeben:

| Wert                         | Beschreibung   | Beispiel   |
|------------------------------|--|--|
| HH:MM:SS                     | Eine bestimmte Uhrzeit am angegebenen Anfangsdatum.                                    | 10:30:08   |
| NOW                          | Die aktuelle Uhrzeit am angegebenen Anfangsdatum.                                      | NOW  |
| NOW+HH:MM <i>oder</i> +HH:MM | Die aktuelle Uhrzeit plus der Anzahl Stunden und Minuten am angegebenen Anfangsdatum.  | NOW+03:00 <i>oder</i> +03:00.<br>Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTIME=NOW+3 oder BEGINTIME=+3 ausgegeben, werden Container mit der Uhrzeit der letzten Prüfung 12:00 Uhr oder später am Anfangsdatum geprüft.                   |
| NOW-HH:MM <i>oder</i> -HH:MM | Die aktuelle Uhrzeit minus der Anzahl Stunden und Minuten am angegebenen Anfangsdatum. | NOW-04:00 <i>oder</i> -04:00.<br>Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTime=NOW-3:30 oder BEGINTime= -3:30 ausgegeben, prüft IBM Spectrum Protect Container mit der Uhrzeit der letzten Prüfung 5:30 Uhr oder später am Anfangsdatum. |

#### ENDDate

Gibt den Datumsbereichswert an, bei dem die Prüfung gestoppt werden soll. Container, die zuletzt innerhalb des angegebenen Datumsbereichs geprüft wurden, werden geprüft. Wenn Sie eine Uhrzeit, aber keinen Datumswert angeben, wird das aktuelle Datum verwendet. Wenn Sie kein Anfangs- und Enddatum angeben, werden alle Container geprüft. Der Standardwert ist das Datum nach der Ausführung der letzten Prüfung für den Container. Dieser Parameter ist wahlfrei.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                         | Beschreibung   | Beispiel   |
|------------------------------|--|--|
| MM/TT/JJJJ                   | Ein bestimmtes Datum.  | 09/15/2016   |
| TODAY                        | Das aktuelle Datum.  | TODAY  |
| TODAY-Tage <b>oder</b> -Tage | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY-1 <i>oder</i> -1.<br>Um Container einzuschließen, die bis gestern geprüft wurden, können Sie ENDDATE=TODAY-1 oder ENDDATE= -1 angeben. |

| Wert                           | Beschreibung   | Beispiel  |
|--------------------------------|--|---|
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.                            | EOLM  |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.      | EOLM-1<br>Um Container einzuschließen, die am Tag vor dem letzten Tag des Vormonats geprüft wurden. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.                      | BOTM  |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage. | BOTM+9<br>Um Container einzuschließen, die am zehnten Tag des aktuellen Monats geprüft wurden.      |

#### ENDTime

Gibt den Zeitbereichswert an, bei dem die Prüfung gestoppt werden soll. Container, die zuletzt innerhalb des angegebenen Zeitbereichs geprüft wurden, werden geprüft. Wenn Sie keine Anfangs- und Endzeit angeben, wird der Zeitbereich auf 00:00:00 bis 23:59:59 gesetzt. Der Standardwert ist 23:59:59. Dieser Parameter ist wahlfrei.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert                         | Beschreibung   | Beispiel  |
|------------------------------|--|---|
| HH:MM:SS                     | Eine bestimmte Uhrzeit am angegebenen Enddatum.                                    | 10:30:08  |
| NOW                          | Die aktuelle Uhrzeit am angegebenen Enddatum.                                      | NOW   |
| NOW+HH:MM <i>oder</i> +HH:MM | Die aktuelle Uhrzeit plus der Anzahl Stunden und Minuten am angegebenen Enddatum.  | NOW+03:00 <i>oder</i> +03:00.<br>Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW+3:00 oder ENDTIME= +3:00 ausgegeben, werden Container mit der Uhrzeit der letzten Prüfung 12:00 Uhr oder früher am angegebenen Enddatum geprüft. |
| NOW-HH:MM <i>oder</i> -HH:MM | Die aktuelle Uhrzeit minus der Anzahl Stunden und Minuten am angegebenen Enddatum. | NOW-03:30 <i>oder</i> -03:30.<br>Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW-3:30 oder ENDTIME= -3:30 ausgegeben, werden Container mit der Uhrzeit der letzten Prüfung 5:30 Uhr oder früher am angegebenen Enddatum geprüft.  |

### Beispiel: Einen bestimmten Container in einem Cloud-Containerspeicherpool prüfen

Den Container 42-00000my000example000container000 in einem Cloud-Containerspeicherpool prüfen.

```
audit container 42-00000my000example000container000 action=scanall
```




### Beispiel: Einen Cloud-Containerspeicherpool innerhalb eines bestimmten Zeitrahmens prüfen

Einen Cloud-Containerspeicherpool mit dem Namen POOL3 prüfen und nur Container einschließen, die gestern zwischen 9:30 und 12:30 Uhr geprüft wurden.

```
audit container stgpool=pool3 begindate=today-1  
begintime=09:30:00 endtime=12:30:00
```

Tabelle 1. Zugehörige Befehle für AUDIT CONTAINER

| Befehl          | Beschreibung                                    |
|-----------------|---|
| CANCEL PROCESS  | Bricht einen Serverhintergrundprozess ab.       |
| QUERY CONTAINER | Zeigt Informationen zu einem Container an.      |
| QUERY DAMAGED   | Zeigt Informationen zu beschädigten Dateien an. |

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

# AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)

---

Mit diesem Befehl können Sie nach Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Verzeichniscontainerspeicherpool suchen.

Mit diesem Befehl können Sie die folgenden Aktionen für einen Container in einem Verzeichniscontainerspeicherpool ausführen:

- Den Inhalt eines Containers durchsuchen, um die Integrität der Datenbereiche zu überprüfen
- Beschädigte Daten aus einem Container entfernen
- Einen vollständigen Container als beschädigt markieren

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
>>-AUDit CONTainer--+-Containername-----+-->
      +-STGpool----Poolname-----+
      '-STGpool----Poolname--STGPOOLDirectory----Verzeichnisname-'

  .-Action----SCANAll-----
>+-----+-----+-----+----->
  '-Action----+SCANAll-----+'
      +-REMOVEDamaged-+
      +-MARKDamaged--+
      '-SCANDamaged--+'

  .-MAXProcess----4-----  .-Wait----No-----
>+-----+-----+-----+----->
  '-MAXProcess----Anzahl-'   '-Wait----+No--+'
                        '-Yes-'

  .-BEGINdate----vor der ersten Prüfung-.
>+-----+-----+-----+----->
  '-BEGINdate----Anfangsdatum-----'

  .-BEGINTime----00:00:00----
>+-----+-----+-----+----->
  '-BEGINTime----Anfangszeit-'

  .-ENDDate----nach der letzten Prüfung-.
>+-----+-----+-----+----->
  '-ENDDate----Enddatum-----'

  .-ENDTime----23:59:59-.
>+-----+-----+-----+-----><
  '-ENDTime----Endzeit--'
```

## Parameter

---

### Containername

Gibt den Namen des Containers an, der geprüft werden soll. Wird dieser Parameter nicht angegeben, müssen Sie einen Verzeichniscontainerspeicherpool angeben.

### STGpool

Gibt den Namen des Verzeichniscontainerspeicherpools an, der geprüft werden soll. Dieser Parameter ist wahlfrei. Wird nur dieser Parameter angegeben, werden alle Container geprüft, die für den Speicherpool definiert sind. Wird dieser Parameter nicht angegeben, müssen Sie einen Container angeben.

### STGPOOLDirectory

Gibt den Namen des Containerspeicherpoolverzeichnis an, das geprüft werden soll. Dieser Parameter ist wahlfrei. Wird dieser Parameter angegeben, werden alle Container geprüft, die für das Containerspeicherpoolverzeichnis definiert sind. Um diesen Parameter anzugeben, müssen Sie auch einen Speicherpool angeben.

### Aktion

Gibt an, welche Aktion der Server ausführt, wenn ein Container in einem Verzeichniscontainerspeicherpool geprüft wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:



## SCANALL

Gibt an, dass der Server Datenbanksätze identifiziert, die sich auf Datenbereiche mit Inkonsistenzen beziehen. Dieser Wert ist der Standardwert. Der Server markiert den Datenbereich in der Datenbank als beschädigt.

Tipp: Wenn Sie den Befehl PROTECT STGPOOL für einen Verzeichniscontainerspeicherpool auf dem Zielsystem verwendet haben, können Sie den beschädigten Datenbereich mithilfe des Befehls REPAIR STGPOOL reparieren.

## REMOVEDamaged

Gibt an, dass der Server alle Dateien aus der Datenbank entfernt, die den beschädigten Datenbereich referenzieren.

## MARKDamaged

Gibt an, dass der Server explizit alle Datenbereiche in dem Container als beschädigt markiert.

## SCANDamaged

Gibt an, dass der Server nur die vorhandenen beschädigten Bereiche in dem Container überprüft.

Statusrücksetzbedingung: Wenn bei der Prüfung kein Fehler bei einem Datenbereich erkannt wird, der als beschädigt markiert ist, wird der Status des Datenbereichs zurückgesetzt. Der Datenbereich kann dann verwendet werden. Diese Bedingung bietet eine Möglichkeit, den Status von beschädigten Datenbereichen zurückzusetzen, wenn Fehler durch ein korrigierbares Problem verursacht werden. Die Optionen SCANALL und SCANDAMAGED sind die einzigen Optionen, die einen beschädigten Bereich zurücksetzen, wenn festgestellt wird, dass der Bereich nicht beschädigt ist.

## MAXProcess

Gibt die maximale Anzahl paralleler Prozesse für die Überprüfung eines Containers in einem Verzeichniscontainerspeicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert im Bereich von 1 bis 99 ein. Der Standardwert ist 4.

## Wait

Gibt an, ob die Prüfoperation im Vordergrund oder im Hintergrund ausgeführt wird. Dieser Parameter ist wahlfrei. Folgende Optionen sind verfügbar:

### No

Gibt an, dass die Operation im Hintergrund ausgeführt wird. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden. Dies ist der Standardwert.

### Yes

Gibt an, dass die Operation im Vordergrund ausgeführt wird. Die Ausführung der Operation nimmt unter Umständen viel Zeit in Anspruch. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.

Einschränkung: Sie können den Parameter WAIT=YES nicht an der Serverkonsole angeben.

## BEGINDate

Gibt den Datumsbereichswert an, bei dem die Prüfung gestartet werden soll. Container, die zuletzt innerhalb des angegebenen Datumsbereichs geprüft wurden, werden geprüft. Wenn Sie eine Uhrzeit, aber kein Anfangsdatum angeben, wird das aktuelle Datum verwendet. Wenn Sie kein Anfangs- und Enddatum angeben, werden alle Container geprüft. Der Standardwert ist das Datum vor der Ausführung der ersten Prüfung für den Container. Dieser Parameter ist wahlfrei.

Sie können die Uhrzeit, zu der die Prüfung beginnen soll, wie folgt angeben:

| Wert                           | Beschreibung   | Beispiel  |
|--------------------------------|--|---|
| MM/TT/JJJJ                     | Ein bestimmtes Datum.  | 09/15/2016  |
| TODAY                          | Das aktuelle Datum.  | TODAY   |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY-7 <i>oder</i> -7.<br><br>Um alle Container zu prüfen, die in der letzten Woche geprüft wurden, geben Sie BEGINDATE=TODAY-7 oder BEGINDATE= -7 an. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM  |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br><br>Um Container einzuschließen, die am Tag vor dem letzten Tag des Vormonats geprüft wurden.   |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM  |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br><br>Um Container einzuschließen, die am zehnten Tag des aktuellen Monats geprüft wurden.  |

## BEGINTime

Gibt den Zeitbereichswert an, bei dem die Prüfung gestartet werden soll. Container, die zuletzt innerhalb des angegebenen Zeitbereichs geprüft wurden, werden geprüft. Wenn Sie keine Anfangs- und Endzeit angeben, wird der Zeitbereich auf 00:00:00 bis 23:59:59 gesetzt. Der Standardwert ist 00:00:00. Wenn Sie keinen Datumsbereich angegeben haben, ist der Standardwert das heutige Datum. Dieser Parameter ist wahlfrei.

Sie können die Uhrzeit, zu der die Prüfung beginnen soll, wie folgt angeben:

| Wert                  | Beschreibung   | Beispiel   |
|-----------------------|--|--|
| HH:MM:SS              | Eine bestimmte Uhrzeit am angegebenen Anfangsdatum.                                    | 10:30:08   |
| NOW                   | Die aktuelle Uhrzeit am angegebenen Anfangsdatum.                                      | NOW  |
| NOW+HH:MM oder +HH:MM | Die aktuelle Uhrzeit plus der Anzahl Stunden und Minuten am angegebenen Anfangsdatum.  | NOW+03:00 oder +03:00.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTIME=NOW+3 oder BEGINTIME=+3 ausgegeben, werden Container mit der Uhrzeit der letzten Prüfung 12:00 Uhr oder später am Anfangsdatum geprüft.                  |
| NOW-HH:MM oder -HH:MM | Die aktuelle Uhrzeit minus der Anzahl Stunden und Minuten am angegebenen Anfangsdatum. | NOW-04:00 oder -04:00.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTIME=NOW-3:30 oder BEGINTIME=-3:30 ausgegeben, prüft IBM Spectrum Protect Container mit der Uhrzeit der letzten Prüfung 5:30 Uhr oder später am Anfangsdatum. |

#### ENDDate

Gibt den Datumsbereichswert an, bei dem die Prüfung gestoppt werden soll. Container, die zuletzt innerhalb des angegebenen Datumsbereichs geprüft wurden, werden geprüft. Wenn Sie eine Uhrzeit, aber keinen Datumswert angeben, wird das aktuelle Datum verwendet. Wenn Sie kein Anfangs- und Enddatum angeben, werden alle Container geprüft. Der Standardwert ist das Datum nach der Ausführung der letzten Prüfung für den Container. Dieser Parameter ist wahlfrei.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum.  | 09/15/2016   |
| TODAY                          | Das aktuelle Datum.  | TODAY  |
| TODAY-Tage oder -Tage          | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY-1 oder -1.<br><br>Um Container einzuschließen, die bis gestern geprüft wurden, können Sie ENDDATE=TODAY-1 oder ENDDATE=-1 angeben. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br><br>Um Container einzuschließen, die am Tag vor dem letzten Tag des Vormonats geprüft wurden.                                  |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br><br>Um Container einzuschließen, die am zehnten Tag des aktuellen Monats geprüft wurden.                                       |

#### ENDTime

Gibt den Zeitbereichswert an, bei dem die Prüfung gestoppt werden soll. Container, die zuletzt innerhalb des angegebenen Zeitbereichs geprüft wurden, werden geprüft. Wenn Sie keine Anfangs- und Endzeit angeben, wird der Zeitbereich auf 00:00:00 bis 23:59:59 gesetzt. Der Standardwert ist 23:59:59. Dieser Parameter ist wahlfrei.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert     | Beschreibung                                    | Beispiel |
|----------|---|----------|
| HH:MM:SS | Eine bestimmte Uhrzeit am angegebenen Enddatum. | 10:30:08 |

| Wert                  | Beschreibung   | Beispiel   |
|-----------------------|--|--|
| NOW                   | Die aktuelle Uhrzeit am angegebenen Enddatum.                                      | NOW  |
| NOW+HH:MM oder +HH:MM | Die aktuelle Uhrzeit plus der Anzahl Stunden und Minuten am angegebenen Enddatum.  | NOW+03:00 oder +03:00.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW+3:00 oder ENDTIME= +3:00 ausgegeben, werden Container mit der Uhrzeit der letzten Prüfung 12:00 Uhr oder früher am angegebenen Enddatum geprüft. |
| NOW-HH:MM oder -HH:MM | Die aktuelle Uhrzeit minus der Anzahl Stunden und Minuten am angegebenen Enddatum. | NOW-03:30 oder -03:30.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW-3:30 oder ENDTIME= -3:30 ausgegeben, werden Container mit der Uhrzeit der letzten Prüfung 5:30 Uhr oder früher am angegebenen Enddatum geprüft.  |

### Beispiel: Einen bestimmten Speicherpoolcontainer prüfen

Den Speicherpoolcontainer 0000000000000721.dcf prüfen.

```
audit container n:\ddcont2\07\0000000000000721.dcf action=scanall
```

### Beispiel: Beschädigte Daten aus einem Verzeichniscontainerspeicherpool entfernen

Einen Verzeichniscontainerspeicherpool mit dem Namen NEWDEDUP prüfen und beschädigte Dateien entfernen.

```
audit container stgpool=newdedup action=removedamaged
```

### Beispiel: Alle Daten in einem Verzeichniscontainerspeicherpool als beschädigt markieren

Einen Verzeichniscontainerspeicherpool mit dem Namen NEWDEDUP prüfen und alle Dateien als beschädigt markieren.

```
audit container stgpool=newdedup maxprocess=2 action=markdamaged
```

### Beispiel: Einen Verzeichniscontainerspeicherpool innerhalb eines bestimmten Zeitrahmens prüfen

Einen Verzeichniscontainerspeicherpool mit dem Namen POOL2 prüfen und nur Container einschließen, die gestern zwischen 9:30 und 12:30 Uhr geprüft wurden.

```
audit container stgpool=pool2 begindate=today-1  
begintime=09:30:00 endtime=12:30:00
```

Tabelle 1. Zugehörige Befehle für AUDIT CONTAINER

| Befehl         | Beschreibung   |
|----------------|--|
| CANCEL PROCESS | Bricht einen Serverhintergrundprozess ab.                                    |
| MOVE CONTAINER | Versetzt den Inhalt eines Speicherpoolcontainers in einen anderen Container. |
| QUERY DAMAGED  | Zeigt Informationen zu beschädigten Dateien an.                              |

## AUDIT LDAPDIRECTORY (LDAP-Verzeichnissever prüfen)

Verwenden Sie diesen Befehl, um einen durch IBM Spectrum Protect gesteuerten Namensbereich auf einem Lightweight Directory Access Protocol-Server (LDAP-Server) zu prüfen. Der LDAP-Server und der Namensbereich werden mithilfe einer oder mehrerer Optionen LDAPURL angegeben.

Einschränkung: Verwenden Sie diesen Befehl nur, wenn Sie die Kennwortauthentifizierung wie in Benutzer mithilfe eines LDAP-Servers authentifizieren beschrieben konfiguriert haben. Die zum Befehl AUDIT LDAPDIRECTORY bereitgestellten Informationen gelten nur für Umgebungen, in denen die Kennwortauthentifizierung wie in Benutzer mithilfe eines LDAP-Servers authentifizieren beschrieben konfiguriert ist.

Knoten und Administrator-IDs, die ihre Kennwörter nicht mit dem LDAP-Verzeichnisserver authentifizieren, werden mit dem Befehl `AUDIT LDAPDIRECTORY FIX=YES` gelöscht. Knoten oder Administrator-IDs, die in der IBM Spectrum Protect-Datenbank nicht mehr vorhanden sind, werden ebenfalls gelöscht.

Stellen Sie vor der Ausgabe dieses Befehls sicher, dass die Option `LDAPURL` in der Datei `dsmserv.opt` angegeben ist. Weitere Informationen befinden sich unter Option `LDAPURL`. Wenn Sie mehrere Optionen `LDAPURL` in der Datei `dsmserv.opt` angegeben haben, werden die Optionen in der Reihenfolge ihrer Anordnung geprüft. Wird die Option `LDAPURL` nicht angegeben, schlägt der Befehl fehl.

## Berechtigungsklasse

---

Für diesen Befehl sind Systemberechtigungen erforderlich.

## Syntax

---

```
                .-Fix-----No-----.  
>>-AUDIT LDAPdirectory-+-----+----->  
                '-Fix-----+No---+'  
                    '-Yes-'  
  
                .-Wait-----No-----.  
>-+-----+-----<  
                '-Wait-----+No---+'  
                    '-Yes-'
```

## Parameter

---

### Fix

Dieser optionale Parameter gibt an, wie der IBM Spectrum Protect-Server Inkonsistenzen zwischen der Datenbank und dem externen Verzeichnis beseitigt. Der Standardwert ist `NO`. Sie können die folgenden Werte angeben:

#### No

Der Server meldet alle Inkonsistenzen zurück, aber ändert nicht das externe Verzeichnis.

#### Yes

Der Server beseitigt alle Inkonsistenzen, die er beseitigen kann, und schlägt bei Bedarf weitere Aktionen vor.

Wichtig: Sind LDAP-Einträge vorhanden, die mit anderen IBM Spectrum Protect-Servern gemeinsam genutzt werden, kann die Auswahl von `YES` zur Folge haben, dass diese Server nicht mehr synchron sind.

### Wait

Dieser optionale Parameter gibt an, ob darauf gewartet werden soll, dass der IBM Spectrum Protect-Server die Verarbeitung dieses Befehls im Vordergrund beendet. Der Standardwert ist `NO`. Sie können die folgenden Werte angeben:

#### No

Der Server verarbeitet diesen Befehl im Hintergrund und Sie können mit anderen Tasks fortfahren, während der Befehl verarbeitet wird. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden entweder in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, je nachdem, wo die Nachrichten protokolliert werden.

#### Yes

Der Server verarbeitet diesen Befehl im Vordergrund. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.

Einschränkung: Von der Serverkonsole aus kann `WAIT=YES` nicht angegeben werden.

## Beispiel: Ein LDAP-Verzeichnis prüfen und Inkonsistenzen beseitigen

---

Das LDAP-Verzeichnis prüfen, das in der Option `LDAPURL` angegeben wurde. Der IBM Spectrum Protect-Server beseitigt einige Inkonsistenzen.

```
audit ldapdirectory fix=yes
```

```
ANR2749W Administrator ADMIN1 wurde auf dem LDAP-Verzeichnisserver, aber nicht in der Datenbank lokalisiert.
```

```
ANR2749W Administrator ADMIN2 wurde auf dem LDAP-Verzeichnisserver, aber nicht in der Datenbank lokalisiert.
```

```
ANR2749W Administrator NODE1 wurde auf dem LDAP-Verzeichnisserver, aber nicht in der Datenbank lokalisiert.
```

```
ANR2749W Administrator NODE2 wurde auf dem LDAP-Verzeichnisserver, aber nicht in der Datenbank lokalisiert.
```

```
ANR2748W Knoten NODE1 wurde auf dem LDAP-Verzeichnisserver, aber nicht in der Datenbank lokalisiert.
```

ANR2748W Knoten NODE2 wurde auf dem LDAP-Verzeichnisserver, aber nicht in der Datenbank lokalisiert. ANR2745I Befehl AUDIT LDAPDIRECTORY wurde beendet: 4 Administratoreinträge sind nur auf dem LDAP-Verzeichnisserver (nicht auf dem IBM Spectrum Protect-Server), 0 Administratoreinträge sind nur auf dem IBM Spectrum Protect-Server (nicht auf dem LDAP-Verzeichnisserver), 2 Knoteneinträge sind nur auf dem LDAP-Verzeichnisserver (nicht auf dem IBM Spectrum Protect-Server), 0 Knoteneinträge sind nur auf dem IBM Spectrum Protect-Server (nicht auf dem LDAP-Verzeichnisserver), 6 Einträge wurden insgesamt auf dem LDAP-Server gelöscht.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für AUDIT LDAPDIRECTORY

| Befehl                    | Beschreibung  |
|---------------------------|---|
| SET DEFAULTAUTHENTICATION | Gibt die Standardkennwortauthentifizierungsmethode für alle Befehle REGISTER NODE oder REGISTER ADMIN an. |
| SET LDAPPASSWORD          | Legt das Kennwort für den LDAPUSER fest.  |
| SET LDAPUSER              | Definiert den Benutzer, der die Kennwörter und Administratoren auf dem LDAP-Verzeichnisserver überwacht.  |

## AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Kassettenarchiv prüfen)

Mit diesem Befehl können Sie Datenträgerbestände in einem automatisierten Kassettenarchiv prüfen und synchronisieren.

Wird der Befehl AUDIT LIBRARY auf einem Kassettenarchivclient ausgegeben, synchronisiert der Client seinen Bestand mit dem Bestand auf dem Kassettenarchivmanager. Stellt der Kassettenarchivclient Inkonsistenzen fest, korrigiert er die Inkonsistenzen, indem er das Eigentumsrecht für den Datenträger auf dem Kassettenarchivmanager ändert.

Wird der Befehl AUDIT LIBRARY auf einem Server ausgegeben, auf dem das Kassettenarchiv ein SCSI-, 349X- oder ACSLS-Kassettenarchiv ist (LIBTYPE=SCSI, LIBTYPE=349X oder LIBTYPE=ACSL), synchronisiert der Server seinen Bestand mit dem Bestand der Kassettenarchiveinheit. Stellt der Server Inkonsistenzen fest, löscht er fehlende Datenträger aus seinem Bestand.

- In SCSI-Kassettenarchiven aktualisiert der Server auch die Positionen der Datenträger in seinem Bestand, die seit der letzten Prüfung versetzt wurden.
- In 349X-Kassettenarchiven stellt der Server auch sicher, dass sich Arbeitsdatenträger in der Arbeitsdatenträgerkategorie und private Datenträger in der privaten Kategorie befinden.

Wird der Befehl AUDIT LIBRARY auf einem Server ausgegeben, der ein Kassettenarchivmanager für das Kassettenarchiv ist (SHARED=YES), aktualisiert der Server das Eigentumsrecht seiner Datenträger, wenn Inkonsistenzen festgestellt werden.

Unabhängig vom Servertyp oder Kassettenarchivtyp werden durch die Ausgabe des Befehls AUDIT LIBRARY nicht automatisch neue Datenträger zu einem Kassettenarchiv hinzugefügt. Um neue Datenträger hinzuzufügen, müssen Sie den Befehl CHECKIN LIBVOLUME verwenden.

Achtung: Die folgenden Vorsichtsmaßnahmen gelten nur für SCSI-, 349X- und ACSLS-Kassettenarchive (LIBTYPE=SCSI, LIBTYPE=349X und LIBTYPE=ACSL):

- Die Ausführung des Befehls AUDIT LIBRARY verhindert jede andere Kassettenarchivaktivität, bis die Prüfung abgeschlossen ist. Der Server verarbeitet beispielsweise keine Zurückschreibungs- oder Abrufanforderungen, die das Kassettenarchiv betreffen, wenn der Befehl AUDIT LIBRARY ausgeführt wird.
- Finden andere Aktivitäten in dem Kassettenarchiv statt, geben Sie den Befehl AUDIT LIBRARY nicht aus. Wird der Befehl AUDIT LIBRARY ausgegeben, wenn ein Kassettenarchiv aktiv ist, können unvorhersehbare Ergebnisse auftreten (beispielsweise eine Blockierung), wenn ein Prozess, der gegenwärtig auf das Kassettenarchiv zugreift, das Laden eines neuen Bands anfordert.

Dieser Befehl erstellt einen Hintergrundprozess, den Sie mit dem Befehl CANCEL PROCESS abbrechen können. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-AUDIT LIBRARY--Kassettenarchivname----->
```



# AUDIT LIBVOLUME (Datenbankinformationen für einen Banddatenträger prüfen)

Verwenden Sie diesen Befehl, um zu bestimmen, ob ein Banddatenträger unbeschädigt ist, und um Daten auf einem Banddatenträger zu prüfen.

Sie können den Befehl AUDIT LIBVOLUME für jeden Banddatenträger ausgeben, der in ein Speicherarchiv zurückgestellt wurde. Der Befehl wird standardmäßig im Hintergrund ausgeführt. Sie können den Befehl für die folgenden Speicherarchivtypen ausgeben, die über ein Bandlaufwerk IBM® TS1140, IBM LTO 5 oder ein Bandlaufwerk einer späteren Generation verfügen:

- SCSI-Bandarchiv
- Virtuelles Bandarchiv (VTL = Virtual Tape Library)

Die folgende Tabelle enthält die Bandlaufwerke, die Banddatenträger mit den Datenträgertypen für IBM TS1140- und IBM LTO 5-Bandlaufwerke und LTO-Bandlaufwerke einer höheren Generation prüfen können:

Tabelle 1. Bandlaufwerke und Datenträgertypen

| Laufwerk  | Datenträgertyp                        |
|-----------|---------------------------------------|
| TS1140    | JB, JX, JA, JW, JJ, JR, JC, JY und JK |
| IBM LTO 5 | LTO 3, LTO 4 und LTO 5                |
| IBM LTO 6 | LTO 4, LTO 5 und LTO 6                |
| IBM LTO 7 | LTO 5, LTO 6 und LTO 7                |

Die folgende Tabelle zeigt die Mindestversion des Einheitentreibers, die für die Ausführung des Befehls erforderlich ist:

Tabelle 2. Mindestversion des IBM Einheitentreibers

| Treibername                   | Einheitentreiberversion |
|-------------------------------|-------------------------|
| Atape-Treiber unter AIX       | 12.3.5.00               |
| lin_tape-Treiber unter Linux  | 1.6.7.00                |
| IBM Bandtreiber unter Windows | 6.2.2.00                |

Einschränkung: Sie können den Befehl CANCEL PROCESS nicht ausgeben, während der Befehl AUDIT LIBVOLUME ausgeführt wird.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung oder die uneingeschränkte Speicherberechtigung für das Speicherarchiv erforderlich, für das der Banddatenträger definiert ist.

## Syntax

```
>>-AUDit LIBVolume--Speicherarchivname--Datenträgername----->
    .-Wait----No-----
>----->
    '-Wait-----No----'
        '-Yes-'
```

## Parameter

Speicherarchivname (Erforderlich)

Gibt den Namen des Speicherarchivs an, in dem sich der Banddatenträger befindet, der geprüft werden soll.

Datenträgername (Erforderlich)

Gibt den Namen des physischen Banddatenträgers an, der geprüft werden soll.

Wait (Optional)

Gibt an, ob die Prüfoperation im Vordergrund oder im Hintergrund ausgeführt wird. Dieser Parameter ist wahlfrei. Folgende Optionen sind verfügbar:

No

Gibt an, dass die Operation im Hintergrund ausgeführt wird. Der Wert NO ist der Standardwert.

Yes

Gibt an, dass die Operation im Vordergrund ausgeführt wird. Die Ausführung der Operation nimmt unter Umständen viel Zeit in Anspruch.

## Beispiel: Einen Banddatenträger prüfen

Das Speicherarchiv EZLIFE prüfen, das einen Banddatenträger mit dem Namen KM0347L5 enthält.

```
audit libvolume ezlife KM0347L5
```

## AUDIT LICENSES (Serverspeicherbelegung prüfen)

Mit diesem Befehl können der Serverspeicher, der von den Clientknoten verwendet wird, und die Serverlizenzen geprüft werden. Der Prüfvorgang bestimmt, ob die aktuelle Konfiguration die Lizenzbedingungen erfüllt.

Ein Prüfvorgang erstellt einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wird der Server angehalten und erneut gestartet, wird ein Prüfvorgang automatisch wie durch den Befehl SET LICENSEAUDITPERIOD angegeben ausgeführt. Zum Anzeigen der Prüfergebnisse den Befehl QUERY LICENSE verwenden.

Achtung: Die Prüfung des Server-Speichers kann viel CPU-Zeit in Anspruch nehmen. Mit der Server-Option AUDITSTORAGE kann angegeben werden, daß der Speicher nicht geprüft werden soll.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-AUDit LICenses-----><
```

## Parameter

Keine.

## Beispiel: Serverlizenzen prüfen

Den Befehl AUDIT LICENSES ausgeben.

```
audit licenses
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für AUDIT LICENSES

| Befehl                 | Beschreibung   |
|------------------------|--|
| CANCEL PROCESS         | Bricht einen Serverhintergrundprozess ab.  |
| QUERY AUDITOCUPANCY    | Zeigt die Serverspeicherauslastung für einen Clientknoten an.  |
| QUERY LICENSE          | Zeigt Informationen über Lizenzen und Prüfvorgänge an.   |
| QUERY PROCESS          | Zeigt Informationen über Hintergrundprozesse an.   |
| QUERY STATUS           | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| REGISTER LICENSE       | Registriert eine Lizenz für den IBM Spectrum Protect-Server.   |
| SET LICENSEAUDITPERIOD | Gibt die Anzahl Tage zwischen den automatischen Lizenzprüfungen an.  |

## AUDIT VOLUME (Datenbankinformationen für Speicherpooldatenträger prüfen)



Mit diesem Befehl können Inkonsistenzen zwischen Datenbankinformationen und einem Datenträger aus dem Speicherpool festgestellt werden. Verarbeitungsinformationen, die während einer Prüfung generiert werden, werden an das Aktivitätenprotokoll und die Serverkonsole gesendet.

Einschränkung: Sie können diesen Befehl nicht für Datenträger verwenden, die Containerkopierspeicherpools zugeordnet sind. Sie können nur Datenträger prüfen, die zu Speicherpools mit DATAFORMAT=NATIVE und DATAFORMAT=NONBLOCK gehören.

Ein Datenträger kann nicht geprüft werden, wenn er gerade aus einem primären Pool oder einem Kopierspeicherpool gelöscht wird.

Wenn eine Prüfverarbeitung aktiv ist, können Clients keine Daten von dem angegebenen Datenträger zurückschreiben oder neue Daten auf dem Datenträger speichern.

Wird von dem Server eine Datei mit Fehlern erkannt, hängt die Bearbeitung der Datei von dem Typ des Speicherpools ab, zu dem der Datenträger gehört, ob die Option FIX in diesem Befehl angegeben wurde und ob die Datei auch auf einem Datenträger gespeichert ist, der anderen Pools zugeordnet ist.

Wenn IBM Spectrum Protect keine Fehler für eine Datei feststellt, die als beschädigt markiert war, wird der Status der Datei zurückgesetzt, so dass die Datei verwendet werden kann.

Der Server löscht keine Archivierungsdateien, für die das Löschen unzulässig ist. Ist der Aufbewahrungsschutz für Archivierung aktiviert, löscht der Server keine Archivierungsdateien, deren Aufbewahrungszeitraum nicht abgelaufen ist.

Um Informationen über den Inhalt eines Datenträgers aus dem Speicherpool anzuzeigen, den Befehl QUERY CONTENT verwenden.

Sollen mehrere Datenträger geprüft werden, können Sie die Parameter FROMDATE und TODATE verwenden. Sollen alle Datenträger in einem Speicherpool geprüft werden, verwenden Sie den Parameter STGPOOL. Wenn Sie die Parameter FROMDATE und/oder TODATE verwenden, beschränkt der Server die Prüfung auf die Datenträger mit sequenziellem Zugriff, die die Datumskriterien erfüllen, und schließt automatisch alle angehängten Plattendatenträger im Speicher ein. Um die Anzahl der Datenträger, die Plattendatenträger einschließen können, zu begrenzen, verwenden Sie die Parameter FROMDATE, TODATE und STGPOOL.

Wird ein Server mit aktiviertem Aufbewahrungsschutz für Archivierung ausgeführt und sind Daten in Speicherpools gespeichert, die mit dem Parameter RECLAMATIONTYPE=SNAPLOCK definiert sind, sollte das Datum des letzten Zugriffs auf dem NetApp SnapLock-Dateiserver für einen Datenträger mit dem Enddatum der Wiederherstellungsperiode übereinstimmen, das angezeigt wird, wenn Sie einen Befehl QUERY VOLUME F=D für diesen Datenträger ausgeben. Bei der AUDIT VOLUME-Verarbeitung werden diese Daten verglichen. Stimmen sie nicht überein und wird der Befehl AUDIT VOLUME mit dem Parameter FIX=NO ausgeführt, wird eine Nachricht ausgegeben, in der angegeben ist, dass der Befehl mit dem Parameter FIX=YES ausgeführt werden muss, um die Inkonsistenz zu beseitigen. Stimmen die Daten nicht überein und wird der Befehl AUDIT VOLUME mit dem Parameter FIX=YES ausgeführt, werden die Inkonsistenzen beseitigt.

Achtung: Verwenden Sie den Parameter FIX=Yes nur, wenn die Infrastruktur für Ihr Bandlaufwerk und Speicherbereichsnetz (SAN) stabil ist. Stellen Sie sicher, dass die Bandköpfe sauber sind und die Bandeinheitentreiber stabil und zuverlässig sind. Andernfalls besteht die Möglichkeit, dass fehlerfreie Daten gelöscht werden, wenn dieser Parameter verwendet wird. Der Server kann nicht feststellen, ob ein Band physisch beschädigt oder eine Bandspeicherinfrastruktur instabil ist.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool erforderlich, in dem der Datenträger definiert ist.

## Syntax

```
                                .-Fix---No-----.
>>-AUDit Volume--+Datenträgername+----->
                '-| A |-----' '-Fix---No---+'
                                '-Yes-'
```

```
.-SKIPPartial-----No-----.  .-Quiet---No-----.
>+-----+----->
'-SKIPPartial-----+No---+' '-Quiet-----+No---+'
                '-Yes-'                '-Yes-'
```

A (mindestens einer dieser Parameter muss angegeben werden)

```
|-----+----->
| (1) |
|-----STGPool-----Poolname-
```

```

      (1)                                (1)
      .-----FROMDate-----TODAY-.   .-TODate-----TODay-----
>--+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
      '-FROMDate-----Datum-----'   '-TODate-----Datum-----'

```

Anmerkungen:

1. Sie können keinen Datenträgernamen angeben, wenn Sie einen Speicherpoolnamen, FROMDATE oder TODATE angeben.

## Parameter

### Datenträgername

Gibt den Namen des Datenträgers aus dem Speicherpool an, der geprüft werden soll. Dieser Parameter ist erforderlich, wenn Sie keinen Speicherpool angeben. Sie können einen Datenträgernamen nicht zusammen mit den Parametern FROMDATE und TODATE angeben.

### Fix

Gibt an, wie der Server Inkonsistenzen zwischen dem Datenträgerbestand und dem angegebenen Datenträger aus dem Speicherpool beseitigt. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

Die Aktionen, die der Server ausführt, sind davon abhängig, ob der Datenträger einem primären Pool oder einem Kopienspeicherpool zugeordnet ist.

#### Primärer Speicherpool:

Anmerkung: Wenn der Befehl AUDIT VOLUME keinen Fehler in einer Datei feststellt, die zuvor als beschädigt markiert war, setzt IBM Spectrum Protect den Status der Datei zurück, so dass sie verwendet werden kann. Auf diese Weise kann der Status beschädigter Dateien zurückgesetzt werden, wenn festgestellt wird, dass die Fehler durch einen korrigierbaren Hardwarefehler, wie z. B. einen verschmutzten Bandkopf, verursacht wurden.

#### Fix=No

IBM Spectrum Protect listet Datenbanksätze auf, die sich auf Dateien mit Inkonsistenzen beziehen; die Sätze werden jedoch nicht gelöscht.

- IBM Spectrum Protect markiert die Datei in der Datenbank als beschädigt. Wenn eine Sicherungskopie in einem Kopienspeicherpool gespeichert ist, kann die Datei mit dem Befehl RESTORE VOLUME oder RESTORE STGPOOL zurückgeschrieben werden.
- Handelt es sich bei der Datei um eine Cache-Kopie, müssen Verweise auf die Datei auf diesem Datenträger mit Hilfe des Befehls AUDIT VOLUME und durch die Angabe von FIX=YES gelöscht werden. Wenn die physische Datei keine Cachekopie ist und eine Kopie in einem Kopienspeicherpool gespeichert ist, kann die Datei mit dem Befehl RESTORE VOLUME oder RESTORE STGPOOL zurückgeschrieben werden.

#### Fix=Yes

Der Server beseitigt alle festgestellten Inkonsistenzen:

- Wenn die physische Datei eine Cache-Kopie ist, löscht der Server die Datenbanksätze, die auf die Cache-Datei verweisen. Die Primärdatei wird auf einem anderen Datenträger gespeichert.
- Wenn die physische Datei keine Cache-Kopie ist und die Datei außerdem in mindestens einem Kopienspeicherpool gespeichert ist, wird der Fehler gemeldet und die physische Datei in der Datenbank als beschädigt markiert. Die physische Datei kann mit dem Befehl RESTORE VOLUME oder RESTORE STGPOOL zurückgeschrieben werden.
- Wenn die physische Datei keine Cache-Kopie und nicht in einem Kopienspeicherpool gespeichert ist, werden alle logischen Dateien, bei denen Inkonsistenzen festgestellt werden, aus der Datenbank gelöscht.
- Wird der Aufbewahrungsschutz für Archivierung mit dem Befehl SET ARCHIVERETENTIONPROTECTION aktiviert, kann bei Bedarf eine zwischengespeicherte Kopie von Daten gelöscht werden. Daten in primären Speicherpools und Kopienspeicherpools können nur als beschädigt gekennzeichnet und nie gelöscht werden.

Der Befehl AUDIT VOLUME darf nicht mit FIX=YES verwendet werden, wenn ein Zurückschreibungsprozess (RESTORE STGPOOL oder RESTORE VOLUME) aktiv ist. Durch den Befehl AUDIT VOLUME könnte die Zurückschreibung unvollständig sein.

#### Kopienspeicherpool:

##### Fix=No

Der Server meldet den Fehler und markiert die Kopie der physischen Datei in der Datenbank als beschädigt.

##### Fix=Yes

Der Server löscht alle Verweise auf die physische Datei und alle Datenbanksätze, die auf eine nicht vorhandene physische Datei zeigen.

## SKIPPartial

Gibt an, ob IBM Spectrum Protect partielle Dateien ignoriert; hierbei handelt es sich um Dateien, die sich über mehrere Speicherpooldatenträger erstrecken. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Bei der Ausführung einer Prüfoperation für einen Datenträger mit sequenziellem Zugriff verhindert dieser Parameter zusätzliche Ladevorgänge für Datenträger mit sequenziellem Zugriff, die für die Prüfung partieller Dateien eventuell erforderlich sind. Gültige Werte:

### No

IBM Spectrum Protect prüft Dateien, die sich über mehrere Datenträger erstrecken.

Wenn Sie nicht SKIPPARTIAL=YES angeben, versucht IBM Spectrum Protect, alle auf dem Datenträger gespeicherten Dateien, einschließlich der Dateien, die sich über andere Datenträger erstrecken, zu verarbeiten. Um Dateien zu prüfen, die sich über mehrere Datenträger erstrecken, müssen die folgenden Bedingungen erfüllt sein:

- Bei Datenträgern mit sequenziellem Zugriff müssen die zusätzlichen Datenträger mit sequenziellem Zugriff über den Zugriffsmodus Lesen/Schreiben oder Lesezugriff verfügen.
- Bei Datenträgern mit wahlfreiem Zugriff müssen die zusätzlichen Datenträger online sein.

### Yes

IBM Spectrum Protect prüft nur Dateien, die auf dem Datenträger gespeichert sind, der geprüft werden soll. Der Status aller partiellen Dateien ist unbekannt.

## Quiet

Gibt an, ob IBM Spectrum Protect detaillierte Informationsnachrichten für nicht abrufbare Dateien auf dem Datenträger an das Aktivitätenprotokoll und die Server-Konsole sendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

### No

Gibt an, daß IBM Spectrum Protect detaillierte Informationsnachrichten und einen Ergebnisbericht sendet. Jede Nachricht enthält den Knotennamen, den Dateibereichsnamen und den Client-Namen für die Datei.

### Yes

Gibt an, daß IBM Spectrum Protect nur einen Ergebnisbericht sendet.

## FROMDate

Gibt das Anfangsdatum des Bereichs an, für den Datenträger geprüft werden sollen. Standardwert ist das aktuelle Datum. Alle Datenträger mit sequenziellem Zugriff, die die Zeitbereichskriterien erfüllen und nach diesem Datum beschrieben wurden, werden geprüft. Der Server schließt alle angehängten Plattendatenträger im Speicher ein. Der Server startet einen Prüfprozess für jeden Datenträger und führt die Prozesse fortlaufend aus. Sie können diesen Parameter nicht verwenden, wenn Sie einen Datenträger angegeben haben. Dieser Parameter ist wahlfrei. Um die Anzahl der Datenträger, die Plattendatenträger einschließen können, zu begrenzen, verwenden Sie die Parameter FROMDATE, TODATE und STGPOOL.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                           | Beschreibung   | Beispiel  |
|--------------------------------|--|---|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 10/15/2001<br><br>Wird ein Datum eingegeben, werden alle in Frage kommenden Datenträger, die an diesem Tag beschrieben wurden (ab 00:00:01), ausgewertet.   |
| TODAY                          | Das aktuelle Datum   | TODAY   |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY-7 <b>oder</b> -7.<br><br>Sollen Informationen beginnend mit den Datenträgern angezeigt werden, die vor einer Woche beschrieben wurden, können Sie FROMDATE=TODAY-7 oder FROMDATE= -7 angeben. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM  |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.  |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM  |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.   |

## TODate

Gibt das Enddatum des Bereichs an, für den Datenträger geprüft werden sollen. Alle Datenträger mit sequenziellem Zugriff, die die Zeitbereichskriterien erfüllen und vor diesem Datum beschrieben wurden, werden geprüft. Der Server schließt alle angehängten Plattendatenträger im Speicher ein. Wird kein Wert angegeben, verwendet der Server standardmäßig das aktuelle Datum. Sie können diesen Parameter nicht verwenden, wenn Sie einen Datenträger angegeben haben. Dieser Parameter ist wahlfrei. Um die Anzahl der Datenträger, die Plattendatenträger einschließen können, zu begrenzen, verwenden Sie die Parameter FROMDATE, TODATE und STGPOOL.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                           | Beschreibung   | Beispiel  |
|--------------------------------|--|---|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 10/15/2001<br><br>Wird ein Datum eingegeben, werden alle in Frage kommenden Datenträger, die an diesem Tag beschrieben wurden (bis 23:59:59), ausgewertet.        |
| TODAY                          | Das aktuelle Datum   | TODAY   |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY-1 <b>oder</b> -1.<br><br>Sollen Informationen angezeigt werden, die bis gestern erstellt wurden, können Sie TODATE=TODAY-1 oder einfach TODATE= -1 angeben. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM  |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.  |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM  |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.   |

## STGPool

Dieser Parameter gibt an, dass der Server nur die Datenträger aus dem angegebenen Speicherpool prüft. Dieser Parameter ist wahlfrei. Sie können diesen Parameter nicht verwenden, wenn Sie einen Datenträger angegeben haben.

### Beispiel: Datenbankinformationen für einen bestimmten Speicherpooldatenträger prüfen

Überprüfen, ob die Datenbankinformationen für den Datenträger aus dem Speicherpool PROG2 konsistent mit den auf dem Datenträger gespeicherten Daten sind. IBM Spectrum Protect berichtigt alle Inkonsistenzen.

```
audit volume prog2 fix=yes
```

### Beispiel: Datenbankinformationen für alle Datenträger prüfen, die während eines bestimmten Datumsbereichs beschrieben wurden

Überprüfen, ob die Datenbankinformationen für alle auswählbaren Datenträger, die vom 3/20/2002 bis zum 3/22/2002 beschrieben wurden, mit den auf dem Datenträger gespeicherten Daten konsistent sind.

```
audit volume fromdate=03/20/2002 todate=03/22/2002
```

### Beispiel: Datenbankinformationen für alle Datenträger in einem bestimmten Speicherpool prüfen

Überprüfen, ob die Datenbankinformationen für alle Datenträger in Speicherpool STPOOL3 mit den auf dem Datenträger gespeicherten Daten für den aktuellen Tag konsistent sind.

```
audit volume stgpool=STPOOL3
```

### Beispiel: Datenbankinformationen für alle Datenträger in einem bestimmten Speicherpool prüfen, die in den letzten beiden Tagen beschrieben wurden

Überprüfen, ob die Datenbankinformationen für alle Datenträger in Speicherpool STPOOL3 mit den auf dem Datenträger gespeicherten Daten für die letzten beiden Tage konsistent sind.

```
audit volume stgpool=STPOOL3 fromdate=-1
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für AUDIT VOLUME

| Befehl                         | Beschreibung  |
|--------------------------------|---|
| CANCEL PROCESS                 | Bricht einen Serverhintergrundprozess ab.                             |
| QUERY CONTENT                  | Zeigt Informationen über Dateien in einem Speicherpooldatenträger an. |
| QUERY PROCESS                  | Zeigt Informationen über Hintergrundprozesse an.                      |
| QUERY VOLUME                   | Zeigt Informationen über Speicherpooldatenträger an.                  |
| SET ARCHIVERETENTIONPROTECTION | Gibt an, ob der Aufbewahrungsschutz für Daten aktiviert ist.          |

## BACKUP-Befehle

Mit den BACKUP-Befehlen können Sicherungskopien der IBM Spectrum Protect-Informationen oder -Objekte erstellt werden.

- BACKUP DB (Datenbank sichern)
- BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)
- BACKUP NODE (NAS-Knoten sichern)
- BACKUP STGPOOL (Daten eines primären Speicherpools in einem Kopierspeicherpool sichern)
- BACKUP VOLHISTORY (Protokolldaten sequenzieller Datenträger speichern)

## BACKUP DB (Datenbank sichern)

Mit diesem Befehl kann eine IBM Spectrum Protect-Datenbank auf Datenträgern mit sequenziellem Zugriff gesichert werden.

Achtung: Um eine Datenbank zurückzuschreiben, muss der Server Informationen aus der Datenträgerhistorydatei und der Einheitenkonfigurationsdatei verwenden. Sie müssen Kopien der Datenträgerhistorydatei und der Einheitenkonfigurationsdatei erstellen und speichern. Diese Dateien können nicht erneut erstellt werden.

Um zu bestimmen, wieviel zusätzlichen Speicherbereich eine Sicherung erfordert, geben Sie den Befehl QUERY DB aus.

Einschränkungen: Sie können eine Serverdatenbank nicht zurückschreiben, wenn der Release-Level der Serverdatenbanksicherung von dem Release-Level des Servers abweicht, der zurückgeschrieben wird. Beispielsweise tritt ein Fehler auf, wenn Sie eine Datenbank der Version 6.3 zurückschreiben und Sie einen Server der Version 7.1 verwenden.

Nach der Beendigung der Datenbanksicherung sichert der IBM Spectrum Protect-Server Informationen auf der Basis der Optionen, die in der Serveroptionsdatei angegeben sind. Die folgenden Informationen werden gesichert:

- Protokolldaten sequenzieller Datenträger für alle Dateien, die mit der Option VOLUMEHISTORY angegeben sind
- Informationen zur Einheitenkonfiguration für alle Dateien, die mit der Option DEVCONFIG angegeben sind
- Masterverschlüsselungsschlüssel des Servers

Wenn auf dem Datenträger oder in dem Dateibereich mit dem definierten Verzeichnis für aktive Protokolldateien nicht genügend Speicherbereich verfügbar ist, können Sie die DB2-Option *overflowlogpath* definieren, um ein Verzeichnis mit dem erforderlichen verfügbaren Speicherbereich zu verwenden. Geben Sie beispielsweise den folgenden Befehl aus, um das Verzeichnis `/home/tsminst2/overflow_dir` zu verwenden:

```
db2 update db cfg for TSMDB1 using overflowlogpath /home/tsminst2/overflow_dir
```

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-BACKup DB--DEVclass----Einheitenklassenname----->  
.-Type----Full-----.
```



## VOLUMenames

Gibt die Datenträger an, die zur Sicherung der Datenbank verwendet werden. Dieser Parameter ist wahlfrei. Wird jedoch SCRATCH=NO angegeben, muß eine Datenträgerliste angegeben werden.

### Datenträgername

Gibt die Datenträger an, die zur Sicherung der Datenbank verwendet werden. Mehrere Datenträger angeben, indem die Namen durch Kommas und ohne Leerzeichen voneinander getrennt werden.

### FILE:Dateiname

Gibt den Namen einer Datei an, die eine Liste der Datenträger enthält, die zur Sicherung der Datenbank verwendet werden. Jeder Datenträgername muss sich auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

Um beispielsweise die Datenträger DB0001, DB0002 und DB0003 zu verwenden, erstellen Sie eine Datei, die diese Zeilen enthält:

```
DB0001
DB0002
DB0003
```

Geben Sie der Datei den entsprechenden Namen. Beispiel:

- Linux-BetriebssystemeTAPEVOL
- Windows-BetriebssystemeTAPEVOL.DATA

Dann können die Datenträger für den Befehl wie folgt angegeben werden:

Linux-Betriebssysteme

```
VOLUMENAMES=FILE:TAPEVOL
```

Windows-Betriebssysteme

```
VOLUMENAMES=FILE:TAPEVOL.DATA
```

## NUMStreams

Gibt die Anzahl der parallelen Datenversetzungsdatenströme an, die beim Sichern der Datenbank verwendet werden sollen. Der Mindestwert ist 1 und der Maximalwert ist 32. Die Erhöhung des Werts hat eine entsprechende Erhöhung der Anzahl der zu verwendenden Datenbanksicherungssitzungen und der Anzahl von Laufwerken zur Folge, die für die Einheitenklasse verwendet werden müssen. Wird ein Wert für NUMSTREAMS im Befehl BACKUP DB angegeben, überschreibt er den Wert, der in dem Befehl SET DBRECOVERY definiert ist. Andernfalls wird der im Befehl SET DBRECOVERY definierte Wert verwendet. Der Wert für NUMSTREAMS wird für alle Typen der Datenbanksicherung verwendet.

Wird ein Wert angegeben, der größer als die Anzahl der für die Einheitenklasse verfügbaren Laufwerke ist, wird nur die Anzahl der verfügbaren Laufwerke verwendet. Die verfügbaren Laufwerke sind die Laufwerke, die für die Einheitenklasse durch den Parameter MOUNTLIMIT oder durch die Anzahl der Onlinelaufwerke für die angegebene Einheitenklasse definiert sind. Die Sitzung wird in der Ausgabe von QUERY SESSION angezeigt.

Wenn Sie die Anzahl der Datenströme erhöhen, werden mehr Datenträger aus der entsprechenden Einheitenklasse für diese Operation verwendet. Mit einer größeren Anzahl von Datenträgern kann die Geschwindigkeit von Datenbanksicherungen erhöht werden, jedoch auf Kosten einer größeren Anzahl von Datenträgern, die nicht vollständig belegt sind.

## Scratch

Gibt an, ob Arbeitsdatenträger für die Sicherung verwendet werden können. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Die folgenden Werte sind gültig:

### Yes

Gibt an, dass Arbeitsdatenträger verwendet werden können.

Werden SCRATCH=YES und der Parameter VOLUMENAMES angegeben, werden Arbeitsdatenträger von IBM Spectrum Protect nur verwendet, wenn auf den angegebenen Datenträgern kein Speicherbereich verfügbar ist.

Wird keine Datenträgerliste durch Verwendung des Parameters VOLUMENAMES angegeben, muss entweder SCRATCH=YES angegeben oder der Standardwert verwendet werden.

### No

Gibt an, dass Arbeitsdatenträger nicht verwendet werden können.

Werden Datenträger durch Verwendung des Parameters VOLUMENAMES und SCRATCH=NO angegeben, schlägt die Sicherung fehl, wenn für die Speicherung der Sicherungsdaten auf den angegebenen Datenträgern nicht genügend Speicherbereich zur Verfügung steht.

## Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Der Standardwert ist NO. Die folgenden Werte sind gültig:

No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

Nachrichten, die von dem Hintergrundprozess erstellt werden, werden entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wenn ein BACKUP DB-Hintergrundprozess abgebrochen wird, wurde ein Teil der Datenbank vor dem Abbruch eventuell bereits gesichert.

Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Erst nachdem der Befehl vollständig ausgeführt wurde, kann mit anderen Aufgaben fortgefahren werden. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist.

Einschränkung: Sie können nicht WAIT=YES an der Serverkonsole angeben.

#### DEDUPDevice

Gibt an, dass eine Zielspeichereinheit die Datendeduplizierung unterstützt. Bei Angabe von YES wird das Format von Sicherungsbildern für Datendeduplizierungseinheiten optimiert. Dadurch werden Sicherungsoperationen effizienter ausgeführt. Die folgenden Werte sind gültig:

No

Gibt an, dass eine Zielspeichereinheit die Datendeduplizierung nicht unterstützt. NO ist der Standardwert. Stellen Sie sicher, dass dieser Parameter für die folgenden Einheiten auf NO gesetzt wird:

- SCSI-Kassettenarchive
- Alle Einheiten, die mit der Einheitenklasse FILE definiert werden
- Virtuelle Bandarchive (VTL, Virtual Tape Library), die die Funktion der Datendeduplizierung nicht unterstützen

Yes

Gibt an, dass eine Zieleinheit die Datendeduplizierung unterstützt und Sicherungen für diese Funktion optimiert werden sollen. Sie können diesen Parameter auf YES setzen, wenn Sie virtuelle Bandarchive (VTL, Virtual Tape Library) verwenden, die die Datendeduplizierung unterstützen.

#### COMPRESS

Gibt an, ob Datenträger, die mit dem Befehl BACKUP DB erstellt werden, komprimiert werden. Der Wert für COMPRESS wird für alle Typen der Datenbanksicherungen verwendet. Dieser Parameter ist wahlfrei. Der Standardwert ist situationsabhängig. Wird der Parameter COMPRESS im Befehl BACKUP DB angegeben, überschreibt er den Wert, der im Befehl SET DBRECOVERY definiert ist. Andernfalls ist der im Befehl SET DBRECOVERY definierte Wert der Standardwert. Sie können einen der folgenden Werte angeben:

No




Gibt an, dass die Datenträger, die mit dem Befehl BACKUP DB erstellt werden, nicht komprimiert werden.

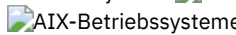

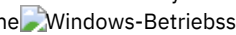
Yes

Gibt an, dass die Datenträger, die mit dem Befehl BACKUP DB erstellt werden, komprimiert werden.

Einschränkungen:

- Gehen Sie mit Vorsicht vor, wenn Sie den Parameter COMPRESS angeben. Bei Verwendung der Komprimierung während Datenbanksicherungen kann die Größe der Sicherungsdateien verringert werden. Die Komprimierung kann jedoch die Zeit verlängern, die für die Ausführung der Datenbanksicherungsverarbeitung erforderlich ist.
- Sichern Sie keine komprimierten Daten auf Band. Wenn in Ihrer Systemumgebung Datenbanksicherungen auf Band gespeichert werden, setzen Sie den Parameter COMPRESS in den Befehlen SET DBRECOVERY und BACKUP DB auf No.

   PROTECTKeys

   Gibt an, dass Datenbanksicherungen eine Kopie des Masterverschlüsselungsschlüssels des Servers enthalten, der zum Verschlüsseln von Speicherpooldaten verwendet wird. Dieser Parameter ist optional. Der Standardwert ist der für den Parameter PROTECTKEYS im Befehl SET DBRECOVERY angegebene Wert. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass Datenbanksicherungen keine Kopie des Masterverschlüsselungsschlüssels des Servers enthalten.


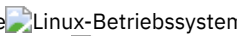
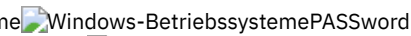
Achtung: Wenn Sie PROTECTKEYS=NO angeben, müssen Sie den Masterverschlüsselungsschlüssel für den Server manuell sichern und den Schlüssel verfügbar machen, wenn Sie die Wiederherstellung nach einem Katastrophenfall (Disaster



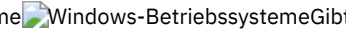


Recovery) implementieren.

Yes

Gibt an, dass Datenbanksicherungen eine Kopie des Masterverschlüsselungsschlüssels des Servers enthalten. Achtung: Wenn Sie PROTECTKEYS=YES angeben, müssen Sie auch den Parameter PASSWORD angeben.

   PASSWORD



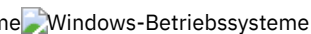
   Gibt das Kennwort an, das zum Schützen der Datenbanksicherung verwendet wird. Der Standardwert ist der für den Parameter PASSWORD im Befehl SET DBRECOVERY angegebene Wert.

Wichtig: Sie müssen sich dieses Kennwort merken. Wenn Sie ein Kennwort für Datenbanksicherungen angeben, müssen Sie dasselbe Kennwort im Befehl RESTORE DB zum Zurückschreiben der Datenbank angeben.

## Beispiel: Eine Teilsicherung unter Verwendung eines Arbeitsdatenträgers ausführen

Eine Teilsicherung der Datenbank unter Verwendung eines Arbeitsdatenträgers ausführen. Eine Einheitenklasse FILE für die Sicherung verwenden.

```
backup db devclass=file type=incremental
```

## Beispiel: Speicherpooldaten in Datenbanksicherungen verschlüsseln

Speicherpooldaten verschlüsseln, indem angegeben wird, dass Datenbanksicherungen eine Kopie des Masterverschlüsselungsschlüssels des Servers enthalten. Den folgenden Befehl ausgeben:

```
backup db protectkeys=yes password=Kennwortname
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für BACKUP DB

| Befehl                     | Beschreibung   |
|----------------------------|--|
| BACKUP DEVCONFIG           | Sichert IBM Spectrum Protect-Einheitendaten in einer Datei.                          |
| BACKUP VOLHISTORY          | Zeichnet Datenträger-History-Daten in externen Dateien auf.                          |
| CANCEL PROCESS             | Bricht einen Serverhintergrundprozess ab.  |
| DELETE VOLHISTORY          | Löscht History-Daten sequenzieller Datenträger aus der Datenträger-History-Datei.    |
| EXPIRE INVENTORY           | Startet die Verfallsverarbeitung für den Datenträgerbestandsverfall manuell.         |
| MOVE DRMEDIA               | Versetzt DRM-Datenträger vor Ort und lagert sie aus.                                 |
| PREPARE                    | Erstellt eine Wiederherstellungsplandatei.   |
| QUERY DB                   | Zeigt Zuordnungsinformationen zu der Datenbank an.                                   |
| QUERY PROCESS              | Zeigt Informationen über Hintergrundprozesse an.                                     |
| QUERY VOLHISTORY           | Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.   |
| SET DBRECOVERY             | Gibt die Einheitenklasse an, die für automatische Sicherungen verwendet werden soll. |
| SET DRMDBBACKUPEXPIREDDAYS | Gibt die Kriterien für den Verfall von Datenbanksicherungsreihen an.                 |



## BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)


Mit diesem Befehl können Sie Informationen zur Einheitenkonfiguration für den Server sichern.

Achtung: Um eine Datenbank zurückzuschreiben, muss der Server Informationen aus der Datenträgerhistorydatei und der Einheitenkonfigurationsdatei verwenden. Sie müssen Kopien der Datenträgerhistorydatei und der Einheitenkonfigurationsdatei erstellen und speichern. Diese Dateien können nicht erneut erstellt werden.

Mit diesem Befehl werden die folgenden Informationen in mindestens einer Datei gesichert:

- Einheitenklassendefinitionen
- Kassettenarchivdefinitionen
- Laufwerkdefinitionen
- Pfaddefinitionen bei SRCTYPE=SERVER
- Serverdefinitionen
- Servername
- Serverkennwort
- Informationen zur Datenträgerposition für Kassettenarchive mit LIBTYPE=SCSI

  Mit der Serveroption DEVCONFIG können eine oder mehrere Dateien angegeben werden, in denen Einheitenkonfigurationsinformationen gespeichert werden sollen. IBM Spectrum Protect aktualisiert die Dateien, wenn eine Einheitenklasse, ein Kassettenarchiv oder ein Laufwerk definiert, aktualisiert oder gelöscht wird.

 Bei der Installation enthält die Serveroptionsdatei eine Option DEVCONFIG, die eine Einheitenkonfigurationsdatei mit dem Namen devcnfg.out angibt. IBM Spectrum Protect aktualisiert diese Datei, wenn eine Einheitenklasse, ein Kassettenarchiv oder ein Laufwerk definiert, aktualisiert oder gelöscht wird.

Um sicherzustellen, dass die Aktualisierungen abgeschlossen sind, bevor der Server angehalten wird, ist Folgendes zu beachten:

- Halten Sie den Server nicht einige Minuten an, nachdem der Befehl BACKUP DEVCONFIG ausgegeben wurde.
- Geben Sie mehrere DEVCONFIG-Optionen in der Serveroptionsdatei an.
- Überprüfen Sie die Einheitenkonfigurationsdatei und stellen Sie fest, ob die Datei aktualisiert wurde.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben, es sei denn, der Befehl enthält den Parameter FILENAMES. Wird der Parameter FILENAMES angegeben und ist die Serveroption REQSYSAUTHOUTFILE auf YES gesetzt, muss der Administrator die Systemberechtigung haben. Wird der Parameter FILENAMES angegeben und ist die Serveroption REQSYSAUTHOUTFILE auf NO gesetzt, muss der Administrator die Bedienerberechtigung, die Maßnahmenberechtigung, die Speicherberechtigung oder die Systemberechtigung haben.

## Syntax

```
>>-Backup DEVCONFig--+-+-----+-----+-----><
|               .,-----.|
|               v         |
|'-Filenames-----Dateiname-----'|
```

## Parameter

### Filenames

Gibt die Dateien an, in denen Einheitenkonfigurationsinformationen gespeichert werden sollen. Es können mehrere Dateien angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden. Dieser Parameter ist wahlfrei.

Wird kein Dateiname angegeben, speichert IBM Spectrum Protect die Informationen in allen Dateien, die mit der Option DEVCONFIG in der Serveroptionsdatei angegeben wurden.

## Beispiel: Einheitenkonfigurationsdaten in einer Datei sichern


Einheitenkonfigurationsdaten in einer Datei mit dem Namen DEVICE sichern.

```
backup devconfig filenames=device
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für BACKUP DEVCONFIG

| Befehl             | Beschreibung   |
|--------------------|--|
| CHECKIN LIBVOLUME  | Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.   |
| CHECKOUT LIBVOLUME | Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv. |
| DEFINE DEVCLASS    | Definiert eine Einheitenklasse.  |

| Befehl  | Beschreibung   |
|---|--|
|   DEFINE DEVCLASS (z/OS Media-Server) |   Definiert eine Einheitenklasse für die Verwendung von Speicher, der von einem z/OS Media-Server verwaltet wird. |
| DEFINE DRIVE  | Ordnet ein Laufwerk einem Kassettenarchiv zu.  |
| DEFINE LIBRARY  | Definiert ein automatisiertes oder manuelles Kassettenarchiv.  |
| DEFINE PATH   | Definiert einen Pfad von einer Quelle zu einem Ziel.   |
| DEFINE SERVER   | Definiert einen Server für die Übertragung zwischen Servern.   |
| LABEL LIBVOLUME   | Kennzeichnet Datenträger in manuellen oder automatisierten Kassettenarchiven.  |
| QUERY LIBVOLUME   | Zeigt Informationen zu einem Datenträger im Kassettenarchiv an.  |
| SET SERVERNAME  | Gibt den Namen an, unter dem der Server registriert ist.   |
| SET SERVERPASSWORD  | Gibt das Serverkennwort an.  |
| UPDATE DEVCLASS   | Ändert die Attribute einer Einheitenklasse.  |
|   UPDATE DEVCLASS (z/OS Media-Server) |   Ändert die Attribute einer Einheitenklasse für Speicher, der von einem z/OS Media-Server verwaltet wird.        |
| UPDATE DRIVE  | Ändert die Attribute eines Laufwerks.  |
| UPDATE LIBRARY  | Ändert die Attribute eines Kassettenarchivs.   |
| UPDATE LIBVOLUME  | Ändert den Status eines Speicherdatenträgers.  |
| UPDATE PATH   | Ändert die zu einem Pfad gehörigen Attribute.  |
| UPDATE SERVER   | Aktualisiert Informationen über einen Server.  |

## BACKUP NODE (NAS-Knoten sichern)

Verwenden Sie diesen Befehl, um eine Sicherungsoperation für einen NAS-Knoten (NAS = Network Attached Storage) zu starten.

Sicherungen, die für NAS-Knoten mit diesem Befehl BACKUP NODE erstellt werden, sind funktional äquivalent zu Sicherungen, die mit dem Befehl BACKUP NAS auf einem IBM Spectrum Protect-Client erstellt werden. Sie können diese Sicherungen entweder mit dem Serverbefehl RESTORE NODE oder dem Clientbefehl RESTORE NAS zurückschreiben.

## Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie die Systemberechtigung, die Maßnahmenberechtigung für die Domäne, der der Knoten zugeordnet ist, oder die Clienteignerberechtigung für den Knoten haben.

## Syntax

```
>>-Backup Node--Knotenname-----+----->
      | .- ,----- . |
      | v             | |
      |-----Dateisystemname---+-'
>+-----+----->
  '-Mgmtclass----Verwaltungs-klasse-'
  .-TOC-----Preferred----- .-Wait-----No-----
>+-----+-----+-----+-----+----->
  '-TOC-----+No-----+-' '-Wait-----+No--+-'
      +-Preferred+           '-Yes-'
      '-Yes-----'
  .-MODE-----DIFFerential-----
>+-----+-----+----->
  '-MODE-----+FULL-----+-'
      '-DIFFerential-'
  .-TYPE-----BACKUPImage-----
```

```
>-----<
'-TYPE--==--+-BACKUPImage--+'
      '-SNAPMirror--'
```

## Parameter

---

### Knotenname (Erforderlich)

Gibt den Knoten an, für den die Sicherung ausgeführt wird. Sie können keine Platzhalterzeichen verwenden und keine Liste mit Namen angeben.

### Dateisystemname

Gibt den Namen eines oder mehrerer Dateisysteme an, die gesichert werden sollen. Sie können auch Namen von virtuellen Dateibereichen angeben, die für den NAS-Knoten definiert wurden. Der angegebene Dateisystemname darf keine Platzhalterzeichen enthalten. Sie können mehrere Dateisysteme angeben, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden.

Wird kein Dateisystem angegeben, werden alle Dateisysteme gesichert. Alle virtuellen Dateibereiche, die für den NAS-Knoten definiert wurden, werden als Teil des Dateisystemimages und nicht separat gesichert.

Ist auf der NAS-Einheit ein Dateisystem mit demselben Namen wie der angegebene virtuelle Dateibereich vorhanden, wird der vorhandene virtuelle Dateibereich automatisch von IBM Spectrum Protect in der Serverdatenbank umbenannt, und das NAS-Dateisystem, das mit dem angegebenen Namen übereinstimmt, wird gesichert. Verfügt der virtuelle Dateibereich über Sicherungsdaten, wird die Dateibereichsdefinition, die dem virtuellen Dateibereich zugeordnet ist, ebenfalls umbenannt.

Tipp: Weitere Überlegungen zur Benennung finden Sie unter dem Parameter für den Namen des virtuellen Dateibereichs im Befehl DEFINE VIRTUALFSMAPPING.

Bei der Bestimmung der zu verarbeitenden Dateisysteme verwendet der Server keine Anweisungen DOMAIN.NAS, INCLUDE.FS.NAS oder EXCLUDE.FS.NAS in der Clientoptionsdatei oder der Clientoptionsgruppe. Werden mehrere Dateisysteme gesichert, ist die Sicherung jedes Dateisystems ein separater Serverprozess.

### MGmtclass

Gibt den Namen der Verwaltungsklasse an, an die diese Sicherungsdaten gebunden werden. Wird keine Verwaltungsklasse angegeben, werden die Sicherungsdaten an die Standardverwaltungsklasse der Maßnahmendomäne gebunden, der der Knoten zugeordnet ist. Bei der Bestimmung der Verwaltungsklasse verwendet der Server *keine* Anweisungen INCLUDE.FS.NAS in der Clientoptionsdatei oder der Clientoptionsgruppe. Die Zielverwaltungsklasse kann auf einen nativen IBM Spectrum Protect-Pool verweisen. In diesem Fall werden NDMP-Daten (NDMP = Network Data Management Protocol) an die native IBM Spectrum Protect-Hierarchie gesendet. Danach verbleiben die Daten in der IBM Spectrum Protect-Hierarchie. Daten, die in native IBM Spectrum Protect-Pools fließen, werden über das LAN gesendet, und Daten, die in NAS-Pools fließen, können direkt angehängt werden oder über ein SAN gesendet werden.

Wenn Sie eine Verwaltungsklasse mit dem Befehl BACKUP NODE angeben, werden alle Versionen der Sicherungsdaten, die zu dem NAS-Knoten gehören, erneut an die neue Verwaltungsklasse gebunden.

### TOC

Gibt an, ob für jede Dateisystemsicherung ein Inhaltsverzeichnis gesichert wird. Sie sollten bei der Festlegung, ob ein Inhaltsverzeichnis gesichert werden soll, Folgendes berücksichtigen:

- Wird ein Inhaltsverzeichnis gesichert, können Sie den Befehl QUERY TOC zur Bestimmung des Inhalts einer Dateisystemsicherung zusammen mit dem Befehl RESTORE NODE zur Zurückschreibung von einzelnen Dateien oder Verzeichnisstrukturen verwenden. Sie können auch den IBM Spectrum Protect-Webclient für Sichern/Archivieren verwenden, um die gesamte Dateisystemstruktur zu untersuchen und Dateien und Verzeichnisse zum Zurückschreiben auszuwählen. Für die Erstellung eines Inhaltsverzeichnisses müssen Sie das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die Verwaltungsklasse definieren, an die dieses Sicherungsimage gebunden ist. Die Erstellung eines Inhaltsverzeichnisses erfordert zusätzliche Verarbeitung, zusätzliche Netzressourcen, zusätzlichen Speicherpoolplatz und möglicherweise einen Mountpunkt während der Sicherungsoperation.
- Ein Inhaltsverzeichnis für ein NAS-Dateisystem darf keinen Verzeichnispfad haben, der größer als 1024 Zeichen ist.
- Wird ein Inhaltsverzeichnis für eine Dateisystemsicherung nicht gesichert, können Sie dennoch einzelne Dateien oder Verzeichnisstrukturen mit dem Befehl RESTORE NODE zurückschreiben, vorausgesetzt, dass Sie den vollständig qualifizierten Namen jeder Datei oder jedes Verzeichnisses kennen, die bzw. das zurückgeschrieben werden soll, und das Image, in dem dieses Objekt gesichert wurde.

Dieser Parameter ist wahlfrei. Der Standardwert ist Preferred. Gültige Werte:

No

Gibt an, dass keine Inhaltsverzeichnisinformationen für Dateisystemsicherungen gesichert werden.

Preferred

Gibt an, dass Inhaltsverzeichnisinformationen für Dateisystemsicherungen gesichert werden sollen. Eine Sicherung schlägt jedoch nicht fehl, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt. Dies ist der Standardwert.

Yes

Gibt an, dass Inhaltsverzeichnisinformationen für jede Dateisystemsicherung gesichert werden müssen. Eine Sicherung schlägt fehl, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt.

Achtung: Wird MODE=DIFFERENTIAL angegeben und ein Inhaltsverzeichnis angefordert (TOC=PREFERRED oder TOC=YES), aber verfügt das letzte vollständige Image über kein Inhaltsverzeichnis, wird eine Gesamtsicherung ausgeführt und ein Inhaltsverzeichnis für diese Gesamtsicherung erstellt.

Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Mit dem Befehl QUERY PROCESS kann die Hintergrundverarbeitung dieses Befehls überwacht werden.

Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Der Befehl muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist. Werden mehrere Dateisysteme gesichert, müssen alle Sicherungsprozesse vor Beendigung des Befehls abgeschlossen sein.

Achtung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

MODE

Gibt an, ob es sich bei den Dateisystemsicherungen um Gesamt- oder Teilsicherungen handelt. Der Standardwert ist DIFFERENTIAL.

FULL

Gibt an, dass das vollständige Dateisystem gesichert wird.

DIFFerential

Gibt an, dass nur die Dateien gesichert werden sollen, die sich seit der letzten Gesamtsicherung geändert haben. Wird eine Sicherung der geänderten Teile ausgewählt und wird keine Gesamtsicherung gefunden, wird eine Gesamtsicherung ausgeführt. Sie können nicht TYPE=SNAPMIRROR angeben, wenn der Parameter MODE auf DIFFERENTIAL gesetzt ist.

TYPE

Gibt die Sicherungsmethode an, die zur Ausführung der NDMP-Sicherungsoperation verwendet wird. Der Standardwert für diesen Parameter ist BACKUPIIMAGE, und er sollte verwendet werden, um eine standardmäßige NDMP-Basis- oder -Differenzsicherung auszuführen. Andere Imagetypen stellen Sicherungsmethoden dar, die für einen bestimmten Dateiserver spezifisch sein können. Gültige Werte:

BACKUPIimage

Gibt an, dass das Dateisystem unter Verwendung einer NDMP-Speicherauszugsoperation gesichert werden soll. Dies ist die Standardmethode für die Ausführung einer NDMP-Sicherung. Die Operation des Typs BACKUPIIMAGE unterstützt Gesamt- und Differenzsicherungen, Zurückschreibungen auf Dateiebene und Sicherungen auf Verzeichnisebene.

SNAPMirror

Gibt an, dass das Dateisystem unter Verwendung der NetApp-Funktion 'SnapMirror-auf-Band' in einen IBM Spectrum Protect-Speicherpool kopiert werden soll. SnapMirror-Images sind Gesamtsicherungsimages auf Blockebene eines Dateisystems. Normalerweise wird für die Ausführung einer SnapMirror-Sicherung erheblich weniger Zeit als für die Ausführung einer traditionellen NDMP-Gesamtsicherung des Dateisystems benötigt. Es gibt jedoch Einschränkungen bezüglich der Verwendungsmöglichkeit von SnapMirror-Images. Die Funktion 'SnapMirror-auf-Band' sollte als Option für die Wiederherstellung nach einem Katastrophenfall zum Kopieren sehr großer NetApp-Dateisysteme in den Sekundärspeicher verwendet werden.

Für die meisten NetApp-Dateisysteme wird die standardmäßige NDMP-Gesamt- oder -Differenzsicherungsmethode verwendet. Weitere Informationen enthält die Dokumentation zu Ihrem NetApp-Dateiserver.

Die folgenden Einschränkungen gelten, wenn der Parameter TYPE auf SNAPMirror gesetzt wird:

Einschränkungen:

- Sie können nicht TOC=YES oder TOC=PREFERRED angeben.
- Der Dateisystemname kann kein Name eines virtuellen Dateibereichs sein.
- Die Momentaufnahme, die von dem Dateiserver während der SnapMirror-Kopieroperation automatisch erstellt wird, wird am Ende der Operation gelöscht.
- Dieser Parameter ist nur für NetApp- und IBM® N-Series-Dateiserver gültig.

## Beispiel: Eine Gesamtsicherung ausführen

Eine Gesamtsicherung für das Dateisystem /vol/vol10 des NAS-Knotens NAS1 ausführen.

```
backup node nas1 /vol/vol10 mode=full
```

## Beispiel: Eine Sicherung eines Verzeichnisses ausführen und ein Inhaltsverzeichnis erstellen

Das Verzeichnis /vol/vol2/mikes auf dem Knoten NAS1 sichern und ein Inhaltsverzeichnis für das Image erstellen. Für die folgenden beiden Beispiele wird angenommen, dass Tabelle 1 die Definitionen für virtuelle Dateibereiche enthält, die auf dem Server für den Knoten NAS1 vorhanden sind.

```
backup node nas1 /mikesdir
```

Tabelle 1. Definitionen für virtuelle Dateibereiche

| Name des virtuellen Dateibereichs | Dateisystem | Pfad           |
|-----------------------------------|-------------|----------------|
| /mikesdir                         | /vol/vol2   | /mikes         |
| /DataDirVol2                      | /vol/vol2   | /project1/data |
| /TestDirVol1                      | /vol/vol1   | /project1/test |

## Beispiel: Eine Sicherung für zwei Verzeichnisse ausführen

Die Verzeichnisse /vol/vol2/project1/data und /vol/vol1/project1/test des Knotens NAS1 sichern. In Tabelle 1 befinden sich die Definitionen für virtuelle Dateibereiche, die auf dem Server für den Knoten NAS1 vorhanden sind.

```
backup node nas1 /DataDirVol2,/testdirvoll mode=full toc=yes
```

## Zugehörige Befehle

Tabelle 2. Zugehörige Befehle für BACKUP NODE

| Befehl                     | Beschreibung  |
|----------------------------|---|
| BACKUP NAS (Clientbefehl)  | Erstellt eine Sicherung der NAS-Knotendaten.  |
| CANCEL PROCESS             | Bricht einen Serverhintergrundprozess ab.   |
| DEFINE COPYGROUP           | Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse. |
| DEFINE VIRTUALFSMAPPING    | Zuordnung eines virtuellen Dateibereichs definieren.  |
| QUERY NASBACKUP            | Zeigt Informationen zu NAS-Sicherungsimages an.   |
| QUERY TOC                  | Zeigt Details zum Inhaltsverzeichnis für ein angegebenes Sicherungsimage an.  |
| QUERY COPYGROUP            | Zeigt die Attribute einer Kopiengruppe an.  |
| RESTORE NAS (Clientbefehl) | Schreibt eine Sicherung der NAS-Knotendaten zurück.   |
| RESTORE NODE               | Schreibt einen NAS-Knoten (NAS = Network Attached Storage) zurück.  |
| UPDATE COPYGROUP           | Ändert ein oder mehrere Attribute einer Kopiengruppe.   |

### Zugehörige Konzepte:

Sichern und Zurückschreiben mit der NetApp-Funktion 'SnapMirror to Tape'

## BACKUP STGPOOL (Daten eines primären Speicherpools in einem Kopierspeicherpool sichern)

Mit diesem Befehl können Dateien aus dem primären Speicherpool in einem Kopierspeicherpool gesichert werden.

Sie können Daten aus einem primären Speicherpool sichern, der mit dem Format NATIVE, NONBLOCK oder einem der NDMP-Formate (NETAPPDUMP, CELERRADUMP oder NDMPDUMP) definiert ist. Der Kopierspeicherpool, in dem Daten gesichert werden sollen, muss dasselbe Datenformat wie der primäre Speicherpool haben. IBM Spectrum Protect unterstützt die Back-End-Datenversetzung für NDMP-Images.

Ist eine Datei in dem Kopierspeicherpool vorhanden, wird die Datei nicht gesichert, es sei denn, die Kopie der Datei in dem Kopierspeicherpool ist als beschädigt markiert. Es wird jedoch keine neue Kopie erstellt, wenn die Datei in dem primären Speicherpool auch als beschädigt markiert ist. In einem Speicherpool mit wahlfreiem Zugriff werden Cachekopien von umgelagerten Dateien und beschädigte Primärdateien nicht gesichert.

Tipp: Wird dieser Befehl für einen primären Speicherpool ausgegeben, der für die Deduplizierung von Daten definiert ist, werden doppelte Daten entfernt, wenn der Kopierspeicherpool ebenfalls für die Deduplizierung von Daten definiert ist.

Wenn die Umlagerung für einen Speicherpool während der Sicherung dieses Speicherpools startet, werden einige Dateien möglicherweise umgelagert, bevor sie gesichert werden. Speicherpools an einer höheren Position in der Umlagerungshierarchie sollen möglicherweise vor Speicherpools an einer niedrigeren Position gesichert werden.

Einschränkungen:

- Führen Sie die Befehle MOVE DRMEDIA und BACKUP STGPOOL nicht gleichzeitig aus. Stellen Sie sicher, dass die Speicherpoolsicherungsprozesse abgeschlossen wurden, bevor der Befehl MOVE DRMEDIA ausgegeben wird.
- Sie können keine Daten aus oder in Speicherpools sichern, die mit einer Einheitenklasse CENTERA definiert sind.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Kopierspeicherpool erforderlich, in dem Sicherungskopien erstellt werden sollen.

## Syntax

```
>>-Backup STGpool--Name_des_primären_Pools--Name_des_Kopienpools-->
. -MAXPRocess-----1----- .
>--+-----+----->
' -MAXPRocess-----Anzahl-'

. -Preview-----No----- .
>--+-----+----->
' -Preview-----+No-----+-'
      +-Yes-----+
      |                (1) |
      '-VOLumesonly-----'

. -SHREDTONoshred-----No----- .  . -Wait-----No----- .
>--+-----+-----+-----><
' -SHREDTONoshred-----+No--+-'  ' -Wait-----+No--+-'
      '-Yes-'                '-Yes-'
```

Anmerkungen:

1. Nur für Speicherpools gültig, die einer Einheitenklasse mit sequenziellem Zugriff zugeordnet sind.

## Parameter

Name\_des\_primären\_Pools (Erforderlich)

Gibt den primären Speicherpool an.

Name\_des\_Kopienpools (Erforderlich)

Gibt den Kopierspeicherpool an.

MAXPRocess

Gibt die maximale Anzahl der Parallelprozesse für die Sicherung von Dateien an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein. Der Standardwert ist 1.

Die Verwendung mehrerer paralleler Prozesse kann den Durchsatz der Sicherung verbessern. Die Erwartung ist die, dass die für die Ausführung der Speicherpoolsicherung benötigte Zeit verringert wird, indem mehrere Prozesse verwendet werden. Sind mehrere Prozesse aktiv, müssen jedoch in einigen Fällen ein oder mehrere Prozesse auf die Verwendung eines Datenträgers warten, der bereits von einem anderen Sicherungsprozess verwendet wird.

Bei der Bestimmung dieses Werts ist die Anzahl der logischen und physischen Laufwerke zu berücksichtigen, die dieser Operation zugeordnet werden kann. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl verfügbarer Mountpunkte und Laufwerke ist von anderen IBM Spectrum Protect-Aktivitäten und Systemaktivitäten sowie von den Mountlimits der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die von der Sicherung betroffen sind.

Jeder Prozess benötigt einen Mountpunkt für Datenträger aus dem Kopierspeicherpool und, falls der Einheitentyp nicht FILE lautet, außerdem ein Laufwerk. Wird ein sequenzieller Speicherpool gesichert, benötigt jeder Prozess einen zusätzlichen Mountpunkt für Datenträger des primären Speicherpools und, falls der Einheitentyp nicht FILE lautet, ein zusätzliches Laufwerk. Beispiel: Angenommen, es werden maximal drei Prozesse für die Zurückschreibung eines primären sequenziellen Speicherpools aus einem Kopierspeicherpool mit derselben Einheitenklasse angegeben. Jeder Prozess benötigt zwei Mountpunkte und zwei Laufwerke. Um alle drei Prozesse ausführen zu können, muss der Grenzwert für Ladeanforderungen für die Einheitenklasse mindestens 6 betragen, und es müssen mindestens sechs Mountpunkte und sechs Laufwerke verfügbar sein.

Für die Voranzeige einer Zurückschreibung wird nur ein Prozess verwendet und es werden keine Mountpunkte oder Laufwerke benötigt.

#### Preview

Gibt an, ob eine Voranzeige der Sicherung, nicht aber ihre Ausführung gewünscht wird. In der Voranzeige werden die Anzahl der Dateien und die Byte angezeigt, die gesichert werden sollen, sowie eine Liste der Datenträger des primären Speicherpools, die geladen werden müssen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können die folgenden Werte angeben:

No

Gibt an, daß die Sicherung ausgeführt wird.

Yes

Gibt an, daß eine Voranzeige der Sicherung, aber nicht die Ausführung der Sicherung gewünscht wird.

VOLUMESONLY

Gibt an, daß die Voranzeige der Sicherung nur als Liste der Datenträger gewünscht wird, die geladen werden müssen. Diese Auswahl erfordert die geringste Verarbeitungszeit. Die Option VOLUMESONLY ist nur für Speicherpools gültig, die einer Einheitenklasse mit sequenziellem Zugriff zugeordnet sind.

Die Option VOLUMESONLY kann verwendet werden, um eine Liste der Datenträger abzurufen, die vom Speicherpoolsicherungsprozess benötigt werden. Beispiel:

```
backup stgpool primary_pool copystg preview=volumesonly
```

Die Liste der Datenträger wird im Serveraktivitätenprotokoll mit der Nachricht ANR1228I protokolliert. Fragen Sie das Serveraktivitätenprotokoll ab, um die Liste der erforderlichen Datenträger abzurufen. Beispiel:

```
query actlog msg=1228
```

#### SHREDTONOshred

Gibt an, ob Daten aus einem primären Speicherpool, der das Schreddern erzwingt, in einem Kopierspeicherpool gesichert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können die folgenden Werte angeben:

No

Gibt an, dass der Server das Sichern von Daten aus einem primären Speicherpool, der das Schreddern erzwingt, in einem Kopierspeicherpool nicht zulässt. Wenn der primäre Speicherpool das Schreddern erzwingt, schlägt die Operation fehl.

Yes

Gibt an, dass der Server das Sichern von Daten aus einem primären Speicherpool, der das Schreddern erzwingt, in einem Kopierspeicherpool zulässt. Die Daten in dem Kopierspeicherpool werden nicht geschreddert, wenn er gelöscht wird.

#### Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können die folgenden Werte angeben:

No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet.

Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Nachrichten, die von dem Hintergrundprozess erstellt werden, werden entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird dieser Prozess abgebrochen, wurden möglicherweise einige Dateien bereits vor dem Abbruch gesichert.

Yes

Gibt an, dass der Server diese Operation im Vordergrund verarbeitet. Die Operation muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabennachrichten dem Verwaltungsclient an, wenn die Operation beendet ist.

Anmerkung: Sie können nicht WAIT=YES an der Serverkonsole angeben.

## Beispiel: Den primären Speicherpool sichern

Den primären Speicherpool mit dem Namen PRIMARY\_POOL im Kopierspeicherpool mit dem Namen COPYSTG sichern.



## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für BACKUP STGPOOL

| Befehl            | Beschreibung  |
|-------------------|---|
| CANCEL PROCESS    | Bricht einen Serverhintergrundprozess ab.   |
| MOVE DRMEDIA      | Versetzt DRM-Datenträger vor Ort und lagert sie aus.  |
| QUERY DRMEDIA     | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.                                       |
| QUERY PROCESS     | Zeigt Informationen über Hintergrundprozesse an.  |
| QUERY SHREDSTATUS | Zeigt Informationen zu Daten an, die auf das Schreddern warten.   |
| QUERY STGPOOL     | Zeigt Informationen zu Speicherpools an.  |
| RESTORE STGPOOL   | Schreibt Dateien aus Kopierspeicherpools in einen primären Speicherpool zurück.   |
| RESTORE VOLUME    | Schreibt Dateien, die auf angegebenen Datenträgern in einem primären Speicherpool gespeichert sind, aus Kopierspeicherpools zurück. |
| SHRED DATA        | Startet manuell den Prozess zum Schreddern gelöschter Daten.  |

## BACKUP VOLHISTORY (Protokolldaten sequenzieller Datenträger speichern)

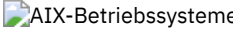
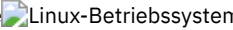
Mit diesem Befehl können Protokolldaten sequenzieller Datenträger in einer oder in mehreren Dateien gesichert werden.


Tipp: Datenträgerprotokolldaten müssen verwendet werden, wenn die Datenbank erneut geladen wird und betroffene Speicherpooldatenträger geprüft werden. Kann der Server nicht gestartet werden, kann die Protokolldatei für Datenträger verwendet werden, um die Datenbank nach diesen Datenträgern abzufragen.

Das Datenträgerprotokoll umfasst Informationen über die folgenden Datenträgertypen:

- Archivprotokolldatenträger
- Datenbanksicherungsdatenträger
- Exportdatenträger
- Sicherungsgruppendatenträger
- Datenbankmomentaufnahmedatenträger
- Datenträger mit Datenbankwiederherstellungsplandateien
- Datenträger mit Wiederherstellungsplandateien
- Datenträger mit Momentaufnahmen der Wiederherstellungsplandateien
- Die folgenden Speicherpooldatenträger mit sequenziellem Zugriff:
  - Datenträger, die Speicherpools hinzugefügt wurden
  - Datenträger, die aufgrund von Wiederherstellungsoperationen oder Operationen MOVE DATA wiederverwendet wurden
  - Datenträger, die mit dem Befehl DELETE VOLUME oder während der Wiederherstellung von Arbeitsdatenträgern entfernt wurden

**Achtung:** Um eine Datenbank zurückzuschreiben, muss der Server Informationen aus der Datenträgerhistorydatei und der Einheitenkonfigurationsdatei verwenden. Sie müssen Kopien der Datenträgerhistorydatei und der Einheitenkonfigurationsdatei erstellen und speichern. Diese Dateien können nicht erneut erstellt werden.

  Sie müssen die Serveroption VOLUMEHISTORY verwenden, um eine oder mehrere Protokolldateien für Datenträger anzugeben. IBM Spectrum Protect aktualisiert Protokolldateien für Datenträger, wenn sich Protokolldaten des Servers zu sequenziellen Datenträgern ändern.

 Bei der Installation enthält die Serveroptionsdatei eine Option VOLUMEHISTORY, die eine Standardprotokolldatei für Datenträger mit dem Namen volhist.out angibt. IBM Spectrum Protect aktualisiert Protokolldateien für Datenträger, wenn sich Protokolldaten des Servers zu sequenziellen Datenträgern ändern.

Um sicherzustellen, dass die Aktualisierungen abgeschlossen sind, bevor der Server angehalten wird, führen Sie diese Schritte aus:

- Halten Sie den Server nicht einige Minuten an, nachdem der Befehl BACKUP VOLHISTORY ausgegeben wurde.
- Geben Sie mehrere Optionen VOLUMEHISTORY in der Serveroptionsdatei an.
- Überprüfen Sie die Protokolldatei für Datenträger, um zu bestimmen, ob die Datei aktualisiert wurde.



```

>>-BEGIN Eventlogging----->>
| .,-----|
| v         |
'-----+-----'
+--CONSOLE-----+
+--ACTLOG-----+
+--EVENTSERVER----+
+--FILE-----+
+--FILETEXT-----+
|               (1) |
+--NTEVENTLOG-----+
|               (2) |
+--SYSLOG-----+
+--TIVOLI-----+
+'-USEREXIT-----'

```

Anmerkungen:

1. Dieser Parameter ist nur für das Windows-Betriebssystem verfügbar.
2. Dieser Parameter ist nur für das Linux-Betriebssystem verfügbar.

## Parameter

Einen oder mehrere Empfänger angeben. Es können mehrere Empfänger angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird ALL angegeben, beginnt das Protokollieren für alle konfigurierten Empfänger. Standardwert ist ALL.

ALL

Gibt alle Empfänger an, die für die Ereignisprotokollierung konfiguriert sind.

CONSOLE

Gibt die Server-Konsole als Empfänger an.

ACTLOG

Gibt das IBM Spectrum Protect-Aktivitätenprotokoll als Empfänger an.

EVENTSERVER


Gibt den Ereignisserver als Empfänger an.


FILE


Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist ein Satz in der Datei, und eine Person kann jedes protokollierte Ereignis nicht einfach lesen.


FILETEXT

Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.

 Windows-BetriebssystemeNTEVENTLOG

 Windows-BetriebssystemeGibt das Windows-Anwendungsprotokoll als Empfänger an.

 Linux-BetriebssystemeSYSLOG

 Linux-BetriebssystemeGibt das Linux-Systemprotokoll als Empfänger an.

TIVOLI

Gibt Tivoli Management Environment (TME) als Empfänger an.

USEREXIT

Gibt eine benutzerdefinierte Routine, in die IBM Spectrum Protect Informationen schreibt, als Empfänger an.

## Beispiel: Das Protokollieren von Ereignissen beginnen

Das Protokollieren von Ereignissen im IBM Spectrum Protect-Aktivitätenprotokoll beginnen.

```
begin eventlogging actlog
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für BEGIN EVENTLOGGING

| Befehl           | Beschreibung   |
|------------------|--|
| DISABLE EVENTS   | Inaktiviert bestimmte Ereignisse für Empfänger.                                  |
| ENABLE EVENTS    | Aktiviert bestimmte Ereignisse für Empfänger.                                    |
| END EVENTLOGGING | Beendet das Ereignisprotokoll für einen bestimmten Empfänger.                    |
| QUERY ENABLED    | Zeigt aktivierte bzw. inaktivierte Ereignisse für einen bestimmten Empfänger an. |
| QUERY EVENTRULES | Zeigt Informationen über Regeln für Server- und Clientereignisse an.             |

| Befehl       | Beschreibung   |
|--------------|--|
| QUERY STATUS | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## CANCEL-Befehle

Mit den CANCEL-Befehlen kann eine Task oder ein Prozess vor der Beendigung abgebrochen werden.

- CANCEL EXPIRATION (Verfallsprozess abbrechen)
- CANCEL EXPORT (Ausgesetzte Exportoperation löschen)
- CANCEL PROCESS (Verwaltungsprozess abbrechen)
- CANCEL REPLICATION (Knotenreplikationsprozesse abbrechen)
- CANCEL REQUEST (Ladeanforderungen abbrechen)
- CANCEL RESTORE (Wiederanlauffähige Zurückschreibungssitzung abbrechen)
- CANCEL SESSION (Clientsitzungen abbrechen)

## CANCEL EXPIRATION (Verfallsprozess abbrechen)

Verwenden Sie diesen Befehl, um einen Prozess mit einer unbekanntem Prozessnummer abzubreaken, der infolge einer Bestandsverfallsoperation ausgeführt wird.

Verwenden Sie den Befehl CANCEL EXPIRATION, wenn die Verfallsprozessnummer nicht bekannt ist; verwenden Sie in allen anderen Fällen den Befehl CANCEL PROCESS und geben Sie die Prozessnummer des Verfallsprozesses an. Mit beiden Befehlen wird derselbe Code zum Beenden des Verfallsprozesses aufgerufen.

Mithilfe des Befehls CANCEL EXPIRATION kann der Abbruch eines Verfallsprozesses automatisiert werden. Wenn Sie beispielsweise den Bestandsverfall um Mitternacht starten und der Prozess aufgrund des Wartungsaufwands auf dem Server um 03:00 Uhr enden muss, können Sie die Ausführung eines Befehls CANCEL EXPIRATION um 03:00 Uhr planen, ohne die Prozessnummer kennen zu müssen.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-CANcel EXPIration----->>
```

## Beispiel: Einen Bestandsverfallsprozess abbrechen

Den Prozess abbrechen, der durch eine Bestandsverfallsoperation generiert wurde.

```
cancel expiration
```

## Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für CANCEL EXPIRATION

| Befehl           | Beschreibung   |
|------------------|--|
| QUERY PROCESS    | Zeigt Informationen über Hintergrundprozesse an.                             |
| EXPIRE INVENTORY | Startet die Verfallsverarbeitung für den Datenträgerbestandsverfall manuell. |

## CANCEL EXPORT (Ausgesetzte Exportoperation löschen)

Mit diesem Befehl kann eine ausgesetzte Exportoperation zwischen Servern gelöscht werden. Nach Ausgabe des Befehls CANCEL EXPORT können Sie die Exportoperation nicht erneut starten. Soll eine momentan aktive Exportoperation gelöscht werden, verwenden Sie den Befehl CANCEL PROCESS.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung erforderlich.

## Syntax

```
>>-CANcel EXPort .-*-----.  
+-----+-----><  
'---Export-ID---'
```

## Parameter

### Export-ID

Die eindeutige ID der ausgesetzten Exportoperation, die Sie löschen wollen. Für die ID können auch Platzhalterzeichen eingegeben werden. Mit dem Befehl QUERY EXPORT können Sie die momentan ausgesetzten Exportoperationen auflisten.

## Beispiel: Eine bestimmte ausgesetzte Exportoperation löschen

Die ausgesetzte Exportoperation zwischen Servern EXPORTALLACCTNODES abbrechen.

```
cancel export exportallacctnodes
```

## Beispiel: Alle ausgesetzten Exportoperation zwischen Servern löschen

Brechen Sie alle ausgesetzten Exportoperationen zwischen Servern ab.

```
cancel export *
```

## Zugehörige Befehle




Tabelle 1. Zugehörige Befehle für CANCEL EXPORT

| Befehl         | Beschreibung  |
|----------------|---|
| CANCEL PROCESS | Bricht einen Serverhintergrundprozess ab.   |
| EXPORT NODE    | Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.                       |
| EXPORT SERVER  | Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server. |
| QUERY EXPORT   | Zeigt die Exportoperationen an, die gerade aktiv oder ausgesetzt sind.  |
| RESTART EXPORT | Startet eine ausgesetzte Exportoperation erneut.  |
| SUSPEND EXPORT | Setzt eine aktive Exportoperation aus.  |

## CANCEL PROCESS (Verwaltungsprozess abbrechen)

Mit diesem Befehl kann ein Hintergrundprozess abgebrochen werden, der durch einen Verwaltungsbefehl oder durch einen Prozess, wie beispielsweise eine Speicherpoolumlagerung, gestartet wurde.

Folgende Befehle generieren Hintergrundprozesse:

- AUDIT CONTAINER
- AUDIT LIBRARY
- AUDIT LICENSES
- AUDIT VOLUME
- BACKUP DB
- BACKUP NODE
- BACKUP STGPOOL
- CHECKIN LIBVOLUME
- CHECKOUT LIBVOLUME
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme CONVERT STGPOOL
- DELETE FILESPACE
- DELETE VOLUME
- EXPIRE INVENTORY

- EXPORT ADMIN
- EXPORT NODE
- EXPORT POLICY
- EXPORT SERVER
- GENERATE BACKUPSET
- IMPORT ADMIN
- IMPORT NODE
- IMPORT POLICY
- IMPORT SERVER
- MIGRATE STGPOOL
- MOVE DATA
- MOVE DRMEDIA
- MOVE MEDIA
- PREPARE
- PROTECT STGPOOL
- RECLAIM STGPOOL
- REPLICATE NODE
- RESTORE NODE
- RESTORE STGPOOL
- RESTORE VOLUME
- VARY

Folgende interne Serveroperationen generieren Hintergrundprozesse:

- Datenträgerbestandsverfall
- Umlagerung
- Wiederherstellung

Zum Abbrechen eines Prozesses benötigen Sie die Prozessnummer, die Sie durch Ausgabe des Befehls QUERY PROCESS abrufen können.

Einige Prozesse, wie beispielsweise die Wiederherstellung, generieren Ladeanforderungen, um die Verarbeitung abzuschließen. Hat ein Prozess eine anstehende Ladeanforderung, antwortet der Prozess möglicherweise erst dann auf einen Befehl CANCEL PROCESS, wenn unter Verwendung des Befehls REPLY oder CANCEL REQUEST auf die Ladeanforderung geantwortet bzw. die Ladeanforderung abgebrochen wurde, oder wenn eine Zeitlimitüberschreitung aufgetreten ist.

Geben Sie den Befehl QUERY REQUEST aus, um offene Anforderungen aufzulisten, oder fragen Sie das Aktivitätenprotokoll ab, um zu bestimmen, ob ein Prozess eine anstehende Ladeanforderung hat. Eine Ladeanforderung gibt an, dass ein Datenträger für den aktuellen Prozess erforderlich ist, der Datenträger aber in dem Kassettenarchiv nicht verfügbar ist. Der Datenträger ist möglicherweise nicht verfügbar, wenn der Administrator den Befehl MOVE MEDIA oder CHECKOUT LIBVOLUME ausgibt oder den Datenträger manuell aus dem Kassettenarchiv entfernt.

Nachdem Sie einen Befehl CANCEL PROCESS für eine Exportoperation ausgegeben haben, kann der Prozess nicht erneut gestartet werden. Um eine serverübergreifende Exportoperation zu stoppen und die Operation zu einem späteren Zeitpunkt erneut zu starten, geben Sie den Befehl SUSPEND EXPORT aus.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-CANcel PProcess--Prozessnummer-----<<
```

## Parameter

---

Prozessnummer (Erforderlich)

Gibt die Nummer des Hintergrundprozesses an, der abgebrochen werden soll.

## Beispiel: Einen Hintergrundprozess unter Verwendung seiner Prozessnummer abbrechen


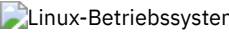


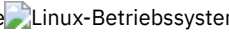
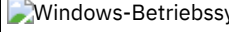

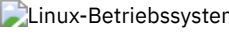



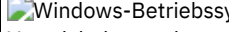
---

Hintergrundprozess Nummer 3 abbrechen.

```
cancel process 3
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für CANCEL PROCESS

| Befehl   | Beschreibung   |
|--|--|
| CANCEL EXPORT  | Löscht eine ausgesetzte Exportoperation.   |
| CANCEL REQUEST   | Bricht anstehende Datenträgerladeanforderungen ab.   |
|  <br> CONVERT STGPOOL |  <br> Konvertiert einen Speicherpool in einen Verzeichniscontainerspeicherpool. |
|  <br> PROTECT STGPOOL |  <br> Schützt einen Verzeichniscontainerspeicherpool.                           |
| QUERY EXPORT   | Zeigt die Exportoperationen an, die gerade aktiv oder ausgesetzt sind.   |
| QUERY PROCESS  | Zeigt Informationen über Hintergrundprozesse an.   |
| REPLICATE NODE   | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |
| REPLY  | Erlaubt einer Anforderung, die Verarbeitung fortzusetzen.  |
| RESTART EXPORT   | Startet eine ausgesetzte Exportoperation erneut.   |
| SUSPEND EXPORT   | Setzt eine aktive Exportoperation aus.   |

## CANCEL REPLICATION (Knotenreplikationsprozesse abbrechen)

Verwenden Sie diesen Befehl, um alle Knotenreplikationsprozesse abzubrechen.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-CANcel REPLication-----><
```

### Parameter

Keine.

### Beispiel: Knotenreplikationsprozesse abbrechen

Alle Knotenreplikationsprozesse abbrechen.

```
cancel replication
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für CANCEL REPLICATION

| Befehl            | Beschreibung   |
|-------------------|--|
| QUERY PROCESS     | Zeigt Informationen über Hintergrundprozesse an.       |
| QUERY REPLICATION | Zeigt Informationen zu Knotenreplikationsprozessen an. |

## CANCEL REQUEST (Ladeanforderungen abbrechen)

Mit diesem Befehl können eine oder mehrere anstehende Anforderungen zum Laden von Datenträgern abgebrochen werden. Um eine Ladeanforderung abbrechen, muss die Anforderungsnummer bekannt sein, die der Anforderung zugeordnet ist. Diese Nummer ist in der Ladeanforderungsnachricht enthalten und kann auch mit dem Befehl QUERY REQUEST angezeigt werden.

## Berechtigungsklasse

---

Für diesen Befehl ist die System- oder die Bedienerberechtigung erforderlich.

## Syntax

---

```
>>-CAnCel REQuest---Anforderungsnummer-+-+-----+-----><
      '-All-----' '-PERManent-'
```

## Parameter

---

Anforderungsnummer

Gibt die Anforderungsnummer der Ladeanforderung an, die abgebrochen werden soll.

ALL

Gibt an, daß alle anstehenden Ladeanforderungen abgebrochen werden sollen.

PERManent

Gibt an, daß der Server die Datenträger, für die eine Ladeanforderung abgebrochen wird, als nicht verfügbar markieren soll. Dieser Parameter ist wahlfrei.

## Beispiel: Eine Ladeanforderung abbrechen

---

Anforderungsnummer 2 abbrechen.

```
cancel request 2
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für CANCEL REQUEST

| Befehl        | Beschreibung  |
|---------------|---|
| QUERY REQUEST | Zeigt Informationen über alle anstehenden Ladeanforderungen an. |
| UPDATE VOLUME | Aktualisiert die Attribute der Speicherpooldatenträger.         |

## CANCEL RESTORE (Wiederanlauffähige Zurückschreibungssitzung abbrechen)

---

Mit diesem Befehl kann eine wiederanlauffähige Zurückschreibungssitzung abgebrochen werden. Zurückschreibungssitzungen können im aktiven oder im wiederanlauffähigen Status abgebrochen werden. Alle ausstehenden Ladeanforderungen, die zu dieser Sitzung gehören, werden automatisch abgebrochen.

Zum Anzeigen wiederanlauffähiger Zurückschreibungssitzungen den Befehl QUERY RESTORE verwenden.

## Berechtigungsklasse

---

Für diesen Befehl ist die System- oder Bedienerberechtigung erforderlich.

## Syntax

---

```
>>-CAnCel--REStoRe---Sitzungsnummer-+-----+-----><
      '-All-----'
```

## Parameter

---

Sitzungsnummer

Gibt die Nummer der wiederanlauffähigen Zurückschreibungssitzung an. Eine aktive Sitzung hat eine positive Nummer und eine wiederanlauffähige Sitzung eine negative Nummer.



ALL

Gibt an, dass alle wiederanlauffähigen Zurückschreibungssitzungen abgebrochen werden sollen.

## Beispiel: Zurückschreibungsoperationen abbrechen

Alle Operationen zum Zurückschreiben abbrechen.

```
cancel restore all
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für CANCEL RESTORE

| Befehl        | Beschreibung   |
|---------------|--|
| QUERY RESTORE | Zeigt Informationen über wiederanlauffähige Zurückschreibungssitzungen an. |

## CANCEL SESSION (Clientsitzungen abbrechen)

Verwenden Sie diesen Befehl, um vorhandene Verwaltungssitzungen oder Clientknotensitzungen abzubreaken und den Abbruch einer Verwaltungssitzung oder Clientknotensitzung mit dem Server zu erzwingen. Alle ausstehenden Ladeanforderungen, die zu dieser Sitzung gehören, werden automatisch abgebrochen. Der Clientknoten muss eine neue Sitzung starten, um die Aktivitäten wiederaufzunehmen.

Wird eine Sitzung abgebrochen, die sich im inaktiven Status (IdleW) befindet, wird die Client-Sitzung automatisch wieder mit dem Server verbunden, wenn sie mit dem erneuten Senden von Daten beginnt.

Wenn dieser Befehl einen Prozess unterbricht, wie beispielsweise Sicherung oder Archivierung, werden die Ergebnisse der Verarbeitung, die zum Zeitpunkt der Unterbrechung aktiv ist, rückgängig gemacht und nicht in der Datenbank festgeschrieben.

## Berechtigungsklasse

Für diesen Befehl ist die System- oder Bedienerberechtigung erforderlich.

## Syntax

```
>>-CANcel SEssion--+-Sitzungsnummer-+-----<<  
                '-ALL-----'
```

## Parameter

Sitzungsnummer

Gibt die Nummer der Verwaltungs-, Server- oder Clientknotensitzung an, die abgebrochen werden soll.

ALL

Gibt an, dass alle Clientknotensitzungen abgebrochen werden. Sie können diesen Parameter nicht verwenden, um Verwaltungsclient- oder Serversitzungen abzubreaken.

## Beispiel: Eine bestimmte Clientknotensitzung abbrechen

Die Clientknotensitzung mit NODEP (Sitzung 3) abbrechen.

```
cancel session 3
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für CANCEL SESSION

| Befehl           | Beschreibung   |
|------------------|--|
| DISABLE SESSIONS | Verhindert, dass neue Sitzungen auf IBM Spectrum Protect zugreifen, lässt jedoch zu, dass bestehende Sitzungen fortgesetzt werden. |
| LOCK ADMIN       | Verweigert einem Administrator den Zugriff auf IBM Spectrum Protect.   |

| Befehl        | Beschreibung   |
|---------------|--|
| LOCK NODE     | Verhindert, dass ein Client auf den Server zugreift.   |
| QUERY SESSION | Zeigt Informationen zu allen aktiven Administrator- und Clientsitzungen mit IBM Spectrum Protect an. |

## CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)


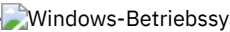

Mit diesem Befehl kann ein Speicherdatenträger mit sequenziellem Zugriff oder ein Reinigungsband dem Serverdatenträgerbestand für ein automatisiertes Speicherarchiv hinzugefügt werden. Der Server kann einen Datenträger, der sich physisch in einem automatisierten Speicherarchiv befindet, erst verwenden, wenn dieser Datenträger zurückgestellt wurde.

Wichtig:

1. Die Verarbeitung des Befehls CHECKIN LIBVOLUME wartet nicht darauf, dass ein Laufwerk verfügbar wird, auch wenn sich das Laufwerk nur im Status IDLE (Freizustand) befindet. Falls erforderlich, kann ein Speicherarchivlaufwerk verfügbar gemacht werden, indem der Befehl DISMOUNT VOLUME ausgegeben wird, um die Bereitstellung des Datenträgers aufzuheben. Ist ein Speicherarchivlaufwerk verfügbar, geben Sie den Befehl CHECKIN LIBVOLUME erneut aus.
2. In einem externen Speicherarchiv definieren Sie keine Laufwerke, stellen Sie keine Datenträger zurück und kennzeichnen Sie keine Datenträger. Der Server stellt eine Schnittstelle zur Verfügung, die von externen Datenträgerverwaltungssystemen verwendet wird, um mit dem Server zu arbeiten.
3. Werden andere WORM-Bänder als 3592-Bänder zurückgestellt, müssen Sie CHECKLABEL=YES verwenden. Andernfalls werden sie als normale Bänder mit Lese-/Schreibzugriff zurückgestellt.

Dieser Befehl erstellt einen Hintergrundprozess, den Sie mit dem Befehl CANCEL PROCESS abbrechen können. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Ausführliche und aktuelle Informationen zur Laufwerk- und Speicherarchivunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

-   Supported devices for AIX and Windows
-  Supported devices for Linux

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax für SCSI-Speicherarchive

```
>>-CHECKIn LIBVolume--Speicherarchivname----->
                                     .-SEARCH----No-.
>---+-Datenträgername-+-----+----->
+-SEARCH----Yes-+-----+-----+
|               '-| A |-|               |
'-SEARCH----Bulk-+-----+-----'
                '| A |-|

                                     .-OWNER----"-".-----
>--STATUS---+-PRiVate-+-----+----->
+-SCRatch-+   '-OWNER----Servername-'
'-CLEaner-'

                                     .-CHECKLabel----Yes----- .-SWAP----No-----
>--+-----+-----+-----+----->
'-CHECKLabel----+-Yes-----+-'   '-SWAP----+-No--+-'
                +-No-----+   '-Yes-'
                '-Barcode-'

                                     .-WAITTime----60---.
>--+-----+-----+-----+-----><
'-WAITTime----Wert-'   '-CLEanings-----Anzahl---'

A (SEARCH=Yes, SEARCH=Bulk)

|---+VOLRange---+-----Datenträgername1,Datenträgername2-----|
|               .-,-----|
```

```

|          V          |
'-VOLList-----Datenträgername-----'
'-FILE:--Dateiname----'

```

## Syntax für 349X-Speicherarchive

```

>>-CHECKIn LIBVolume--Speicherarchivname----->
. -SEARCH-----No-.
>-----Datenträgername----->
'-SEARCH-----Yes-----'
'-| A |- '
. -OWNER-----"-----.
>--STATus-----PRIVate----->
'-SCRatch-' '-OWNER-----Servername-'
. -CHECKLabel-----Yes-----.
>----->
'-CHECKLabel-----Yes+-' '-DEVType-----+3590+-'
'-No--' '-3592-'
. -SWAP-----No-----. . -WAITTime-----60---.
>----->
'-SWAP-----+No--+-' '-WAITTime-----Wert-'
'-Yes-'
A (SEARCH=Yes)
|---VOLRange-----Datenträgername1,Datenträgername2---|
|          .,-----|
|          V          |
'-VOLList-----Datenträgername-----'
'-FILE:--Dateiname----'

```

## Syntax für ACSLS-Speicherarchive

```

>>-CHECKIn LIBVolume--Speicherarchivname----->
. -SEARCH-----No-.
>-----Datenträgername----->
'-SEARCH-----Yes-----'
'-| A |- '
. -OWNER-----"-----.
>--STATus-----PRIVate----->
'-SCRatch-' '-OWNER-----Servername-'
. -CHECKLabel-----Yes-----. . -SWAP-----No-----.
>----->
'-CHECKLabel-----Yes+-' '-SWAP-----+No--+-'
'-No--' '-Yes-'
. -WAITTime-----60---.
>----->
'-WAITTime-----Wert-'
A (SEARCH=Yes)
|---VOLRange-----Datenträgername1,Datenträgername2---|
|          .,-----|
|          V          |
'-VOLList-----Datenträgername-----'
'-FILE:--Dateiname----'

```

## Parameter

Speicherarchivname (Erforderlich)  
Gibt den Namen des Kassettenarchivs an.

Datenträgername

Gibt den Datenträgernamen des Speicherdatenträgers an, der zurückgestellt wird. Dieser Parameter ist erforderlich, wenn SEARCH gleich NO ist. Diesen Parameter nicht eingeben, wenn der Parameter SEARCH den Wert YES oder BULK hat. Wird ein Datenträger in ein SCSI-Speicherarchiv mit mehreren Eingangs-/Ausgangsanschlüssen zurückgestellt, wird der Datenträger in dem Schacht mit der niedrigsten Nummer zurückgestellt.

#### STATus (Erforderlich)

Gibt den Datenträgerstatus an. Gültige Werte:

##### PRIVate

Gibt an, dass der Datenträger ein privater Datenträger ist, der nur geladen wird, wenn er mit seinem Namen angefordert wird.

##### SCRatch

Gibt an, dass der Datenträger ein neuer Arbeitsdatenträger ist. Dieser Datenträger kann geladen werden, um Anforderungen zum Laden eines Arbeitsdatenträgers während Datenspeicheroperationen oder Exportoperationen zu erfüllen.

Hat ein Datenträger einen Eintrag in der Datenträger-History, können Sie den Datenträger nicht als Arbeitsdatenträger zurückstellen.

##### CLEaner

Gibt an, dass der Datenträger eine Reinigungskassette und keine Datenkassette ist. Für eine Reinigungskassette ist der Parameter CLEANINGS erforderlich, der auf die Anzahl der Verwendungen der Reinigungskassette gesetzt werden muss.

Die Angabe CHECKLABEL=YES ist für das Zurückstellen einer Reinigungskassette ungültig. Verwenden Sie STATUS=CLEANER, um eine Reinigungskassette separat von einer Datenkassette zurückzustellen.

#### OWNer

Gibt an, welcher Speicherarchivclient der Eigner eines privaten Datenträgers in einem Speicherarchiv ist, das in einem SAN gemeinsam genutzt wird. Der Datenträger, für den das Eigentumsrecht angegeben wird, muss ein privater Datenträger sein. Für einen Arbeitsdatenträger können Sie kein Eigentumsrecht angeben. Außerdem können Sie keinen Eigner angeben, wenn Sie SEARCH=YES oder SEARCH=BULK verwenden.

Wird der Befehl CHECKIN LIBVOLUME ausgegeben, überprüft der Server den Eigner. Wurde dieser Parameter nicht angegeben, verwendet der Server den Standardwert und übergibt das Datenträgereigentumsrecht an den Speicherarchivclient als Eigner, wie in der Protokolldatei für Datenträger auf dem Speicherarchivmanager aufgezeichnet ist. Hat der Datenträger keinen Speicherarchivclient als Eigner, übergibt der Server das Eigentumsrecht an den Speicherarchivmanager.

#### SEARCH

Gibt an, ob der Server das Speicherarchiv nach Datenträgern durchsucht, die nicht zurückgestellt wurden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

Gültige Werte:

##### No

Gibt an, dass nur der angegebene Datenträger in das Speicherarchiv zurückgestellt wird.

**Für SCSI-Speicherarchive:** Der Server gibt die Anforderung aus, den Datenträger in einen Kassettenschacht in dem Speicherarchiv oder, falls verfügbar, in einen Eingangsanschluss einzulegen. Der Kassettenschacht oder Eingangsanschluss wird durch die Elementadresse identifiziert. **Für 349X-Speicherarchive:** Der Datenträger befindet sich möglicherweise bereits in dem Speicherarchiv oder Sie können ihn bei Aufforderung in die E/A-Station einlegen.

##### Yes

Gibt an, dass der Server das Speicherarchiv nach Datenträgern durchsucht, die zurückgestellt werden sollen. Sie können den Parameter VOLRANGE oder VOLLIST verwenden, um die Suche zu begrenzen. Bei Verwendung dieses Parameters sind die folgenden Einschränkungen zu berücksichtigen:

- Wird das Speicherarchiv von Anwendungen gemeinsam genutzt, kann der Server einen Datenträger untersuchen, der von einer anderen Anwendung benötigt wird. Bei 349X-Speicherarchiven fragt der Server den Speicherarchivmanager nach allen Datenträgern ab, die der Kategorie SCRATCH oder PRIVATE und der Kategorie INSERT zugeordnet sind.
- Für SCSI-Speicherarchive dürfen Sie nicht SEARCH=YES und CHECKLABEL=NO in demselben Befehl angeben.

##### Bulk

Gibt an, dass der Server die Eingangs-/Ausgangsanschlüsse des Speicherarchivs nach Datenträgern durchsucht, die automatisch zurückgestellt werden können. Diese Option gilt nur für SCSI-Speicherarchive.

Wichtig:

1. Sie dürfen CHECKLABEL=NO und SEARCH=BULK nicht gleichzeitig angeben.
2. Sie können den Parameter VOLRANGE oder VOLLIST verwenden, um die Suche zu begrenzen.

## VOLRange

Gibt einen Bereich von Datenträgernamen an, die durch Kommas voneinander getrennt sind. Sie können diesen Parameter verwenden, um die Suche nach Datenträgern zu begrenzen, die zurückgestellt werden sollen, wenn SEARCH=YES (349X-, ACSLS- und SCSI-Speicherarchive) oder SEARCH=BULK (nur SCSI-Speicherarchive) angegeben wird. Sind keine Datenträger in dem Speicherarchiv vorhanden, die sich in dem angegebenen Bereich befinden, wird der Befehl ohne Fehler beendet.

Geben Sie nur Datenträgernamen an, die numerisch erhöht werden können. Neben dem Bereich für den Erhöhungswert kann ein Datenträgername ein alphanumerisches Präfix und ein alphanumerisches Suffix enthalten.

| Parameter                           | Beschreibung  |
|-------------------------------------|---|
| <code>volrange=bar110,bar130</code> | Die 21 Datenträger werden zurückgestellt: bar110, bar111, bar112,...bar129, bar130. |
| <code>volrange=bar11a,bar13a</code> | Die 3 Datenträger werden zurückgestellt: bar11a, bar12a, bar13a.                    |
| <code>volrange=123400,123410</code> | Die 11 Datenträger werden zurückgestellt: 123400, 123401, ...123409, 123410.        |

## VOLList

Gibt eine Liste mit Datenträgern an. Sie können diesen Parameter verwenden, um die Suche nach Datenträgern zu begrenzen, die zurückgestellt werden sollen, wenn SEARCH=YES (349X-, ACSLS- und SCSI-Speicherarchive) oder SEARCH=BULK (nur SCSI-Speicherarchive) angegeben wird. Sind in dem Speicherarchiv keine Datenträger vorhanden, die sich in der Liste befinden, wird der Befehl ohne Fehler beendet.

Gültige Werte:

### Datenträgername

Gibt einen oder mehrere Datenträgernamen an, die durch Kommas und ohne Leerzeichen voneinander getrennt sind.

Beispiel: `VOLLIST=TAPE01,TAPE02`.

### FILE:Dateiname

Gibt den Namen einer Datei an, die eine Liste der Datenträger für den Befehl enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert. Um beispielsweise die Datenträger TAPE01, TAPE02 und TAPE03 zu verwenden, erstellen Sie die Datei TAPEVOL, die die folgenden Zeilen enthält:

```
TAPE01
TAPE02
TAPE03
```

Die Datenträger können für den Befehl wie folgt angegeben werden: `VOLLIST=FILE:TAPEVOL`.

Achtung: Bei dem Dateinamen muss die Groß-/Kleinschreibung beachtet werden.

## CHECKLabel

Gibt an, wie oder ob der Server Kennsätze sequenzieller Datenträger lesen soll. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Gültige Werte:

### Yes

Gibt an, dass während des Zurückstellens versucht wird, den Datenträgerkennsatz zu lesen.

Achtung:

1. Für SCSI-Speicherarchive dürfen Sie nicht SEARCH=YES und CHECKLABEL=NO in demselben Befehl angeben.
2. Für andere WORM-Datenträger als 3592 müssen Sie YES angeben.

### No

Gibt an, dass der Datenträgerkennsatz während des Zurückstellens nicht gelesen wird. Das Unterdrücken der Kennsatzprüfung kann jedoch später zu Fehlern führen (z. B. kann ein falscher Kennsatz oder ein nicht richtig gekennzeichnete Datenträger Fehler verursachen). Geben Sie für 349X- und ACSLS-Speicherarchive NO an, um das Laden von Kassetten in ein Laufwerk zum Lesen des Datenträgerkennsatzes zu vermeiden. Diese Speicherarchive geben immer die Informationen zu externen Kennsätzen für Kassetten zurück. Diese Informationen werden von IBM Spectrum Protect verwendet.

### Barcode

Gibt an, dass der Server das Barcodeetikett liest, wenn das Speicherarchiv über einen Barcodeleser verfügt und die Datenträger externe Barcodeetikett haben. Die Zeit für das Zurückstellen kann durch die Verwendung des Barcodes verkürzt werden. Dieser Parameter gilt nur für SCSI-Speicherarchive.

Kann der Barcodeleser das Barcodeetikett nicht lesen oder verfügt das Band über kein Barcodeetikett, lädt der Server das Band und liest den internen Kennsatz.

## DEVType

Gibt den Einheitentyp des Datenträgers an, der zurückgestellt wird. Dieser Parameter ist erforderlich, wenn keines der Laufwerke in diesem Speicherarchiv über definierte Pfade verfügt.

3590

Gibt an, dass der Einheitentyp des Datenträgers, der zurückgestellt wird, 3590 ist.

3592

Gibt an, dass der Einheitentyp des Datenträgers, der zurückgestellt wird, 3592 ist.

## SWAP

Gibt an, ob der Server Datenträger auslagert, wenn kein leerer Speicherarchivschacht verfügbar ist. Der für die Auslagerungsoperation ausgewählte Datenträger (Zielauslagerungsdaträger) wird aus dem Speicherarchiv ausgegeben und durch den zurückgestellten Datenträger ersetzt. Der Server identifiziert einen Zielauslagerungsdaträger, indem nach einem verfügbaren Arbeitsdatenträger gesucht wird. Ist keiner vorhanden, identifiziert der Server den am wenigsten geladenen Datenträger.

Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Dieser Parameter ist nur gültig, wenn in dem Befehl ein Datenträgername angegeben ist. Gültige Werte:

No

Gibt an, dass der Server den Datenträger nur zurückstellt, wenn ein leerer Schacht verfügbar ist.

Yes

Gibt an, dass der Server Kassetten auslagert, um den Datenträger zurückzustellen, wenn kein leerer Schacht verfügbar ist.

## WAITTime

Gibt die Anzahl Minuten an, die der Server auf Ihre Antwort auf eine Anforderung wartet. Geben Sie einen Wert im Bereich 0-9999 an. Möchten Sie vom Server zur Eingabe aufgefordert werden, geben Sie eine Wartezeit größer als Null an. Der Standardwert ist 60 Minuten. Angenommen, Sie werden vom Server aufgefordert, ein Band in den Eingangs-/Ausgangsanschluss eines Speicherarchivs einzulegen. Haben Sie eine Wartezeit von 60 Minuten angegeben, gibt der Server eine Anforderung aus und wartet 60 Minuten auf Ihre Antwort. Angenommen, Sie haben dagegen eine Wartezeit von 0 angegeben. Wenn Sie bereits ein Band eingelegt haben, hat eine Wartezeit mit dem Wert Null zur Folge, dass die Operation ohne Aufforderung fortgesetzt wird. Haben Sie *kein* Band eingelegt, hat eine Wartezeit mit dem Wert Null zur Folge, dass die Operation fehlschlägt.

## CLEAnings

Den empfohlenen Wert für die einzelne Reinigungskassette eingeben (ist normalerweise auf der Kassette angegeben). Reinigungen gelten nur für SCSI-Speicherarchive. Dieser Parameter ist bei der Angabe von STATUS=CLEANER erforderlich.

Werden mehrere Reinigungskassetten in das Speicherarchiv zurückgestellt, wird nur eine Reinigungskassette verwendet, bis ihr Wert für den Parameter CLEANINGS den Wert Null erreicht hat. Anschließend wird eine andere Reinigungskassette ausgewählt, und die erste Reinigungskassette kann entnommen und entsorgt werden.

## Beispiel: Einen Datenträger in ein SCSI-Speicherarchiv zurückstellen

---

Stellen Sie den Datenträger WPDV00 in das SCSI-Speicherarchiv AUTO zurück.

```
checkin libvolume auto wpdv00 status=scratch
```

## Beispiel: Einen Barcodeleser verwenden, um ein Speicherarchiv nach einer Reinigungskassette zu durchsuchen

---

Durchsuchen Sie das SCSI-Speicherarchiv AUTOLIB1 und suchen Sie unter Verwendung des Barcodelesers nach der Reinigungskassette CLNV. SEARCH=YES verwenden, aber die Suche mit dem Parameter VOLLIST eingrenzen.

```
checkin libvolume autolib1 search=yes vollist=cleanv status=cleaner  
cleanings=10 checklabel=barcode
```

## Beispiel: Ein Speicherarchiv durchsuchen, um nicht verwendete Datenträger in einem bestimmten Bereich in den Arbeitsdatenträgerstatus (SCRATCH) zu versetzen

---

Durchsuchen Sie das 349X-Speicherarchiv ABC und begrenzen Sie die Suche auf einen Bereich nicht verwendeter Datenträger BAR110 bis BAR130 und versetzen Sie die Datenträger in den Arbeitsdatenträgerstatus (SCRATCH).

```
checkin libvolume abc search=yes volrange=bar110,bar130  
status=scratch
```

## Beispiel: Ein Speicherarchiv durchsuchen, um einen bestimmten Datenträger in den Arbeitsdatenträgerstatus (SCRATCH) zu versetzen

---

Verwenden Sie den Barcodeleser, um das SCSI-Speicherarchiv MYLIB nach VOL1 zu durchsuchen, und versetzen Sie den Datenträger in den Arbeitsdatenträgerstatus (SCRATCH).

```
checkin libvolume mylib search=yes vollist=voll status=scratch  
checklabel=barcode
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für CHECKIN LIBVOLUME

| Befehl             | Beschreibung   |
|--------------------|--|
| AUDIT LIBRARY      | Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet.            |
| CANCEL PROCESS     | Bricht einen Serverhintergrundprozess ab.  |
| CHECKOUT LIBVOLUME | Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.                                     |
| DEFINE LIBRARY     | Definiert ein automatisiertes oder manuelles Kassettenarchiv.  |
| DEFINE VOLUME      | Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll. |
| DISMOUNT VOLUME    | Entlädt einen sequenziellen entfernbarer Datenträger anhand des Datenträgernamens.                             |
| LABEL LIBVOLUME    | Kennzeichnet Datenträger in manuellen oder automatisierten Kassettenarchiven.                                  |
| QUERY LIBRARY      | Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.  |
| QUERY LIBVOLUME    | Zeigt Informationen zu einem Datenträger im Kassettenarchiv an.  |
| QUERY PROCESS      | Zeigt Informationen über Hintergrundprozesse an.   |
| REPLY              | Erlaubt einer Anforderung, die Verarbeitung fortzusetzen.  |
| UPDATE LIBVOLUME   | Ändert den Status eines Speicherdatenträgers.  |

## CHECKOUT LIBVOLUME (Speicherdatenträger aus Kassettenarchiv entnehmen)

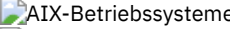
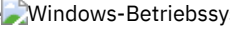
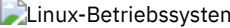
Mit diesem Befehl kann ein Speicherdatenträger mit sequenziellem Zugriff aus dem Serverdatenträgerbestand für ein automatisiertes Kassettenarchiv entfernt werden. Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Einschränkungen:

1. Bei der Entnahmeverarbeitung wird nicht darauf gewartet, dass ein Laufwerk verfügbar wird, auch wenn sich das Laufwerk im Status IDLE befindet. Falls erforderlich, können Sie ein Kassettenarchivlaufwerk verfügbar machen, indem der Datenträger mit dem Befehl DISMOUNT VOLUME entladen wird. Sobald ein Laufwerk verfügbar ist, kann der Befehl CHECKOUT LIBVOLUME erneut ausgegeben werden.

2. Bevor Datenträger aus einem 349X-Kassettenarchiv entnommen werden, stellen Sie sicher, dass die 349x-Kassetteneingabe- und -ausgabeeinrichtung über genügend leere Schächte für die Datenträger verfügt, die entnommen werden sollen. Der 3494-Kassettenarchivmanager (Library Manager) teilt einer Anwendung nicht mit, dass die Kassetteneingabe- und -ausgabeeinrichtung voll ist. Er akzeptiert Anforderungen zur Ausgabe einer Kassette und wartet, bis die Kassetteneingabe- und -ausgabeeinrichtung geleert wurde, bevor zum Server zurückgekehrt wird. IBM Spectrum Protect scheint in diesem Fall zu blockieren. Überprüfen Sie das Kassettenarchiv und löschen Sie alle Aufforderungen zum Eingriff.
3. Bevor Datenträger aus einem ACSLS-Kassettenarchiv entnommen werden, stellen Sie sicher, dass die CAP-Priorität in ACSLS größer als Null ist. Ist die CAP-Priorität Null, müssen Sie in dem Befehl CHECKOUT LIBVOLUME einen Wert für den CAP-Parameter angeben.

Ausführliche und aktuelle Informationen zur Laufwerk- und Speicherarchivunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

-   Supported devices for AIX and Windows
-  Supported devices for Linux

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax für SCSI-Speicherarchiv

```
>>-CHECKOut LIBVolume--Speicherarchivname----->
                                     .-REMove-----Bulk-----.
>----+-Datenträgername-+-----+-----+-----+----->
      '-| A |-----'      '-REMove-----+Yes--+-'
                                     +-No----+
                                     '-Bulk-'

      .-CHECKLabel-----Yes----- . -FORCE-----No----- .
>----+-+-----+-----+-----+-----><
      '-CHECKLabel-----+Yes--+-' '-FORCE-----+No--+-'
                                     '-No--'      '-Yes-'

A

|---+VOLRange-----Datenträgername1,Datenträgername2---+-----|
|           .-,-----|
|           V           |
'-VOLList-----+Datenträgername-+-----+-----'
      '-FILE:--Dateiname----'
```

## Syntax für 349X-Kassettenarchiv

```
>>-CHECKOut LIBVolume--Speicherarchivname----->
                                     .-REMove-----Bulk-----.
>----+-Datenträgername-+-----+-----+-----+-----><
      '-| A |-----'      '-REMove-----+Yes--+-'
                                     +-No----+
                                     '-Bulk-'

A

|---+VOLRange-----Datenträgername1,Datenträgername2---+-----|
|           .-,-----|
|           V           |
'-VOLList-----+Datenträgername-+-----+-----'
      '-FILE:--Dateiname----'
```

## Syntax für ACSLS-Kassettenarchiv

```
>>-CHECKOut LIBVolume--Speicherarchivname----->
                                     .-REMove-----Yes----- .
>----+-Datenträgername-+-----+-----+-----+----->
```



```

'-| A |-----'      '-REMove-----+Yes--+-'
                        +-No----+
                        '-Bulk-'

>-----<
'-CAP-----x,y,z---'

A

|---VOLRange-----Datenträgername1,Datenträgername2---|
|               v               |
'-VOLList-----+---Datenträgername-+-----'
                '-FILE:--Dateiname----'

```

## Parameter

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an.

Datenträgername

Gibt den Datenträgernamen an.

VOLRange

Gibt zwei Datenträgernamen an, die durch ein Komma voneinander getrennt sind. Dieser Parameter gibt einen Bereich von Datenträgern an, die entnommen werden sollen. Sind keine Datenträger in dem Kassettenarchiv vorhanden, die sich in dem angegebenen Bereich befinden, wird der Befehl ohne Fehler beendet.

Geben Sie nur Datenträgernamen an, die numerisch erhöht werden können. Neben dem Bereich für den Erhöhungswert kann ein Datenträgername ein alphanumerisches Präfix und ein alphanumerisches Suffix enthalten.

| Parameter              | Beschreibung   |
|------------------------|--|
| volrange=bar110,bar130 | Die 21 Datenträger werden entnommen: bar110, bar111, bar112,...bar129, bar130. |
| volrange=bar11a,bar13a | Die 3 Datenträger werden entnommen: bar11a, bar12a, bar13a.                    |
| volrange=123400,123410 | Die 11 Datenträger werden entnommen: 123400, 123401, ...123409, 123410.        |

VOLList

Gibt eine Liste mit Datenträgern an, die entnommen werden sollen. Sind keine Datenträger in dem Kassettenarchiv vorhanden, die sich in der Liste befinden, wird der Befehl ohne Fehler beendet.

Gültige Werte:

Datenträgername

Gibt die Namen der Datenträger an, die für den Befehl verwendet werden. Beispiel: VOLLIST=TAPE01,TAPE02.

FILE: Dateiname

Gibt den Namen einer Datei an, die eine Liste der Datenträger für den Befehl enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert. Um beispielsweise die Datenträger TAPE01, TAPE02 und TAPE03 zu verwenden, erstellen Sie die Datei TAPEVOL, die die folgenden Zeilen enthält:

```

TAPE01
TAPE02
TAPE03

```

Die Datenträger können für den Befehl wie folgt angegeben werden: VOLLIST=FILE:TAPEVOL.

Achtung: Bei dem Dateinamen muss die Groß-/Kleinschreibung beachtet werden.

REMove

Gibt an, dass der Server versucht, den Datenträger aus dem Kassettenarchiv in die Serviceein-/ausgabestation oder die Eingangs-/Ausgangsanschlüsse zu versetzen. Dieser Parameter ist wahlfrei. Abhängig vom Kassettenarchivtyp sind die gültigen Werte YES, BULK und NO. Die Antwort des Servers auf jede dieser Optionen und die Standardwerte werden in den folgenden Abschnitten beschrieben.

**349X-Kassettenarchive:** Der Standardwert ist BULK. Die folgende Tabelle zeigt, wie der Server für 349X-Kassettenarchive antwortet.

Tabelle 1. Antwort des Servers für 349X-Kassettenarchive

| <b>REMOVE=YES</b>  | <b>REMOVE=BULK</b>   | <b>REMOVE=NO</b>   |
|--|--|--|
| Der 3494-Kassettenarchivmanager (Library Manager) gibt die Kassette an die Serviceein-/ausgabestation aus. | Der 3494-Kassettenarchivmanager (Library Manager) gibt die Kassette an die Ausgabeeinrichtung mit hoher Speicherkapazität aus. | Der 3494-Kassettenarchivmanager (Library Manager) gibt den Datenträger nicht aus.<br><br>Der Server lässt die Kassette für die Verwendung durch andere Anwendungen in dem Kassettenarchiv in der Kategorie INSERT. |

**SCSI-Kassettenarchive:** Der Standardwert ist BULK. Die folgende Tabelle zeigt, wie der Server für ein SCSI-Kassettenarchiv antwortet.

Tabelle 2. Antwort des Servers für SCSI-Kassettenarchive

| <b>Wenn ein Kassettenarchiv ...</b>   | <b>Und REMOVE=YES, dann...</b>  | <b>Und REMOVE=BULK, dann...</b>   | <b>Und REMOVE=NO, dann...</b>   |
|---|---|---|---|
| <i>Keine</i><br>Eingangs-/Ausgangsanschlüsse hat  | Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben.     | Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.     | Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. |
| Eingangs-/Ausgangsanschlüsse hat und ein <i>Eingangs-/Ausgangsanschluss verfügbar ist</i> | Versetzt der Server die Kassette in den verfügbaren Eingangs-/Ausgangsanschluss und gibt die Anschlussadresse in einer Nachricht an.<br><br>Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben. | Versetzt der Server die Kassette in den verfügbaren Eingangs-/Ausgangsanschluss und gibt die Anschlussadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. | Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. |
| Eingangs-/Ausgangsanschlüsse hat, aber <i>keine Anschlüsse verfügbar sind</i>             | Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben.     | Wartet der Server auf einen verfügbaren Eingangs-/Ausgangsanschluss.  | Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. |

**ACSLs-Kassettenarchive:** Der Standardwert ist YES. Wenn der Parameter auf YES gesetzt wird und der Kassettenzugriffsport (CAP, Cartridge Access Port) den Prioritätswert 0 für die automatische Auswahl hat, müssen Sie eine CAP-ID angeben. Die folgende Tabelle zeigt, wie der Server für ACSLS-Kassettenarchive antwortet.

Tabelle 3. Antwort des Servers für ACSLS-Kassettenarchive

| <b>REMOVE=YES oder REMOVE=BULK</b>  | <b>REMOVE=NO</b>  |
|---|---|
| Der Server gibt die Kassette an die Serviceein-/ausgabestation aus und löscht den Datenträgereintrag aus dem Datenträgerbestand im Kassettenarchiv des Servers. | Der Server gibt die Kassette nicht aus. Der Server löscht den Datenträgereintrag aus dem Kassettenarchivbestand des Servers und lässt den Datenträger in dem Kassettenarchiv. |

## CHECKLabel

Gibt an, wie oder ob der Server Kennsätze sequenzieller Datenträger liest.

Achtung: Dieser Parameter gilt nicht für Kassettenarchive IBM® 349X oder ACSLS.

Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Gültige Werte:

### Yes

Gibt an, daß der Server versucht, den Datenträgerkennsatz zu lesen, um sicherzustellen, daß der korrekte Datenträger entnommen wird.

### No

Gibt an, daß der Datenträgerkennsatz während der Entnahme nicht gelesen wird. Da der Lesevorgang entfällt, verbessert sich die Leistung.

## FORCE

Gibt an, ob der Server einen Datenträger entnimmt, wenn beim Lesen des Kennsatzes ein Ein-/Ausgabefehler auftritt.

Achtung: Dieser Parameter gilt nicht für Kassettenarchive IBM 349X oder ACSLS.

Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

### No

Der Server entnimmt keinen Speicherdatenträger, wenn beim Lesen des Kennsatzes ein E/A-Fehler auftritt.

### Yes

Der Server entnimmt den Speicherdatenträger, auch wenn ein E/A-Fehler auftritt.

## CAP

Gibt an, welcher Cartridge Access Port (CAP) für die Ausgabe von Datenträgern verwendet werden soll, wenn REMOVE=YES angegeben wird. Dieser Parameter gilt nur für Datenträger in ACSLS-Kassettenarchiven. Wenn der CAP-Prioritätswert in dem Kassettenarchiv auf 0 gesetzt wird, ist dieser Parameter erforderlich. Ist ein CAP-Prioritätswert größer als Null in dem Kassettenarchiv definiert, ist dieser Parameter optional. Standardmäßig haben alle CAPs anfänglich den Prioritätswert 0, der bedeutet, dass ACSLS nicht automatisch den Kassettenzugriffsport auswählt.

Zum Anzeigen der gültigen CAP-Kennungen (x,y,z) geben Sie den Befehl QUERY CAP mit der Option ALL von der ACSA-Konsole (ACSA = Automated Cartridge System System Administrator) auf dem ACSLS-Server-Host aus. Die Kennungen sind:

### x

Die ACS-ID (ACS = Automated Cartridge System). Diese Kennung kann eine Zahl im Bereich von 0 bis 126 sein.

### y

Die LSM-ID (LSM = Library Storage Module). Diese Kennung kann eine Zahl im Bereich von 0 bis 23 sein.

### z

Die CAP-ID. Diese Kennung kann eine Zahl im Bereich von 0 bis 11 sein.

Weitere Informationen enthält die StorageTek-Dokumentation.

## Beispiel: Einen Datenträger entnehmen und den Kennsatz prüfen

Den Datenträger mit dem Namen EXB004 aus dem Kassettenarchiv FOREST entnehmen. Den Kennsatz lesen, um den Datenträgernamen zu prüfen, den Datenträger aber nicht aus dem Kassettenarchiv entfernen.

```
checkout libvolume forest exb004 checklabel=yes remove=no
```

## Zugehörige Befehle

Tabelle 4. Zugehörige Befehle für CHECKOUT LIBVOLUME

| Befehl            | Beschreibung   |
|-------------------|--|
| AUDIT LIBRARY     | Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet.            |
| CANCEL PROCESS    | Bricht einen Serverhintergrundprozess ab.  |
| CHECKIN LIBVOLUME | Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.                                       |
| DEFINE LIBRARY    | Definiert ein automatisiertes oder manuelles Kassettenarchiv.  |
| DEFINE VOLUME     | Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll. |
| LABEL LIBVOLUME   | Kennzeichnet Datenträger in manuellen oder automatisierten Kassettenarchiven.                                  |

| Befehl           | Beschreibung  |
|------------------|---|
| QUERY LIBRARY    | Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an. |
| QUERY LIBVOLUME  | Zeigt Informationen zu einem Datenträger im Kassettenarchiv an.     |
| QUERY PROCESS    | Zeigt Informationen über Hintergrundprozesse an.                    |
| REPLY            | Erlaubt einer Anforderung, die Verarbeitung fortzusetzen.           |
| UPDATE LIBVOLUME | Ändert den Status eines Speicherdatenträgers.                       |

## CLEAN DRIVE (Laufwerk reinigen)

Verwenden Sie diesen Befehl, wenn IBM Spectrum Protect unabhängig von der Reinigungshäufigkeit sofort eine Reinigungskassette in ein Laufwerk laden soll.

Es gibt einige Besonderheiten, die beachtet werden müssen, wenn dieser Befehl für ein SCSI-Kassettenarchiv verwendet werden soll, das eine automatische Laufwerkreinigung in seiner Einheitenhardware zur Verfügung stellt.

Einschränkung: Sie können den Befehl CLEAN DRIVE nicht für ein Laufwerk ausführen, dessen einzige Pfadquelle ein NAS-Dateiserver ist.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-CLEAN DRIVE--Kassettenarchivname--Laufwerkname-----<<
```

### Parameter

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, dem das Laufwerk zugeordnet ist.

Laufwerkname (Erforderlich)

Gibt den Namen des Laufwerks an.

### Beispiel: Ein bestimmtes Bandlaufwerk reinigen

Sie haben bereits mit dem Befehl DEFINE LIBRARY ein Kassettenarchiv mit dem Namen AUTOLIB definiert und mit dem Befehl CHECKIN LIBVOL eine Reinigungskassette in das Kassettenarchiv zurückgestellt. Dem Server mitteilen, daß TAPEDRIVE3 in diesem Kassettenarchiv gereinigt werden muß.

```
clean drive autolib tapedrive3
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für CLEAN DRIVE

| Befehl             | Beschreibung   |
|--------------------|--|
| CHECKIN LIBVOLUME  | Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.   |
| CHECKOUT LIBVOLUME | Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv. |
| DEFINE DRIVE       | Ordnet ein Laufwerk einem Kassettenarchiv zu.                              |
| DEFINE LIBRARY     | Definiert ein automatisiertes oder manuelles Kassettenarchiv.              |
| DELETE DRIVE       | Löscht ein Laufwerk aus einem Kassettenarchiv.                             |
| QUERY DRIVE        | Zeigt Informationen zu Laufwerken an.                                      |
| UPDATE DRIVE       | Ändert die Attribute eines Laufwerks.                                      |

## COMMIT (Festschreiben von Befehlen in einem Makro steuern)

Mit diesem Befehl kann das Festschreiben eines Befehls in einem Makro gesteuert und die Datenbank nach der Verarbeitung von Befehlen aktualisiert werden. Wird dieser Befehl im Konsolenmodus des Verwaltungsclients ausgegeben, wird keine Nachricht generiert.

Tritt während der Verarbeitung der Befehle in einem Makro ein Fehler auf, stoppt der Server die Verarbeitung des Makros und macht alle Änderungen (seit dem letzten COMMIT) rückgängig. Wenn ein Befehl festgeschrieben worden ist, kann er nicht rückgängig gemacht werden.

Wenn die Befehlsverarbeitung gesteuert werden soll, ist sicherzustellen, dass in der Verwaltungsclientsitzung nicht die Option ITEMCOMMIT verwendet wird. Mit der Option ITEMCOMMIT werden Befehle innerhalb eines Scripts oder eines Makros festgeschrieben, während *jeder* Befehl verarbeitet wird.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-COMMIT-----<<
```

### Parameter

Keine.

### Beispiel: Festschreiben von Befehlen in einem Makro steuern

Im interaktiven Modus des Verwaltungs-Clients mit dem Makro REG.ADM neue Administratoren registrieren und eine Berechtigung erteilen. Die Änderungen werden festgeschrieben, nachdem die Administratoren registriert worden sind und ihnen eine Berechtigung erteilt worden ist.

Makroinhalt:

```
/* REG.ADM-Maßnahmenadmin. registrieren & Berechtigung erteilen*/  
REGister Admin sara hobby  
GRant AUTHority sara CLasses=Policy  
COMMIT /* Änderungen festschreiben */REGister Admin ken plane  
GRant AUTHority ken CLasses=Policy  
COMMIT /* Änderungen festschreiben */
```

Befehl

```
macro reg.adm
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COMMIT

| Befehl   | Beschreibung   |
|----------|--|
| MACRO    | Führt eine angegebene Makrodatei aus.  |
| ROLLBACK | Löscht alle Änderungen, die seit dem letzten COMMIT nicht in der Datenbank festgeschrieben wurden. |

#### Zugehörige Konzepte:

Makros des Verwaltungsclients

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## CONVERT STGPOOL (Speicherpool in einen Containerspeicherpool konvertieren)

Mit diesem Befehl können Sie einen primären Speicherpool, der eine Einheitenklasse FILE, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet, in einen Verzeichniscontainerspeicherpool oder einen Cloud-Containerspeicherpool konvertieren. Sie können Containerspeicherpools sowohl für die Inline-Dateneduplizierung als auch für die clientseitige Dateneduplizierung verwenden.

Einschränkungen: Die folgenden Einschränkungen gelten für die Speicherpoolkonvertierung:

- Sie können einen Speicherpool nur einmal konvertieren.
- Sie können den Speicherpool während der Konvertierungsverarbeitung nicht aktualisieren. Umlagerungs- und Datenversetzungsprozesse sind nicht verfügbar.
- Sie müssen alle Maßnahmen aktualisieren, um sicherzustellen, dass das Ziel einen Speicherpool angibt, der nicht konvertiert ist oder gerade konvertiert wird.

Während der Konvertierungsverarbeitung werden alle Daten aus dem Quellenspeicherpool in den Zielspeicherpool versetzt. Wenn der Prozess abgeschlossen ist, ist der Quellenspeicherpool nicht mehr verfügbar. Wenn ein Speicherpool nicht verfügbar ist, können Sie keine Daten in den Speicherpool schreiben. Der Quellenspeicherpool kann für das Löschen ausgewählt werden, aber er wird nicht automatisch gelöscht. Bei Bedarf können Sie Daten aus dem Quellenspeicherpool zurückschreiben.

Achtung: Während der Speicherpoolkonvertierung werden Daten aus Kopierspeicherpools und Speicherpools für aktive Daten gelöscht. Diese Aktion wird auch dann ausgeführt, wenn Sie die Anzahl der Tage angegeben haben, die nach dem Löschen aller Dateien von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerpool zurückgestellt werden kann.

## Berechtigungsklasse

---

Für diesen Befehl ist die eingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
>>-CONvert STGpool--Quellenspeicherpool--Zielspeicherpool----->
. -MAXPRocess-----8----- .
>-+-----+-----+-----+-----><
' -MAXPRocess-----Anzahl---' ' -DUration---Minuten-'
```

## Parameter

---

### Quellenspeicherpool (Erforderlich)

Geben Sie einen primären Speicherpool an, der eine Dateieinheitenklasse, eine Bändeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) für die Sicherungs- und Archivierungsverarbeitung verwendet. Dieser Parameter ist erforderlich.

### Zielspeicherpool (Erforderlich)

Geben Sie den Namen eines vorhandenen Verzeichniscontainerspeicherpools oder Cloud-Containerspeicherpools an, in den der Speicherpool konvertiert wird. Dieser Parameter ist erforderlich, wenn Sie zum ersten Mal diesen Befehl ausgeben. Tipp: Wenn Sie die Speicherpoolkonvertierung erneut starten und der Zielspeicherpool von dem Wert abweicht, der bei der ersten Ausgabe des Befehls CONVERT STGPOOL angegeben wurde, schlägt der Befehl fehl.

### MAXPRocess

Gibt die maximale Anzahl paralleler Prozesse für die Konvertierung von Daten in dem Speicherpool an. Dieser Parameter ist wahlfrei. Sie können eine Zahl im Bereich von 1 bis 99 angeben. Der Standardwert ist 8. Tipp: Änderungen des Standardwerts werden automatisch gespeichert. Wenn Sie die Speicherpoolkonvertierung erneut starten und der Parameterwert von dem Wert abweicht, der bei der ersten Ausgabe des Befehls CONVERT STGPOOL angegeben wurde, wird der zuletzt angegebene Wert verwendet.

### DUration

Gibt die maximale Anzahl Minuten an, die eine Konvertierung ausgeführt wird, bevor sie abgebrochen wird. Wenn die angegebene Anzahl Minuten verstrichen ist, bricht der Server alle Konvertierungsprozesse für den Speicherpool ab. Sie können eine Zahl im Bereich von 1 bis 9999 angeben. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, wird die Konvertierung bis zum Abschluss ausgeführt.

Tipp: Die Ausführung der Speicherpoolkonvertierung für große Speicherpools kann Tage dauern. Verwenden Sie diesen Parameter, um die Zeit für die Speicherpoolkonvertierung täglich zu begrenzen. Als Best Practice sollten Sie die Konvertierung für mindestens 2 Stunden für einen Speicherpool, der eine Einheitenklasse FILE verwendet, und für mindestens 4 Stunden für ein VTL planen.

## Beispiel: Einen Speicherpool konvertieren und eine maximale Anzahl Prozesse angeben

---

Konvertieren Sie einen Speicherpool mit dem Namen DEDUPPOOL1, versetzen Sie die Daten in einen Containerspeicherpool mit dem Namen DIRPOOL1 und geben Sie 25 als maximale Anzahl Prozesse an.

```
convert stgpool deduppool1 dirpool1 maxprocess=25
```

Tabelle 1. Zugehörige Befehle für CONVERT STGPOOL

| Befehl           | Beschreibung  |
|------------------|---|
| CANCEL PROCESS   | Bricht einen Serverhintergrundprozess ab.                   |
| QUERY CLEANUP    | Fragt den Bereinigungsstatus eines Quellenspeicherpools ab. |
| QUERY CONVERSION | Fragt den Konvertierungsstatus eines Speicherpools ab.      |
| PROTECT STGPOOL  | Schützt einen Verzeichniscontainerspeicherpool.             |
| REMOVE DAMAGED   | Entfernt beschädigte Daten aus einem Quellenspeicherpool.   |

## COPY-Befehle

Mit den COPY-Befehlen kann eine Kopie von IBM Spectrum Protect-Objekten oder -Daten erstellt werden.

- COPY ACTIVEdata (Aktive Sicherungsdaten aus einem primären Speicherpool in einen Pool für aktive Daten kopieren)
- COPY CLOPTSET (Clientoptionsgruppe kopieren)
- COPY DOMAIN (Maßnahmendomäne kopieren)
- COPY MGMTCLASS (Verwaltungsklasse kopieren)
- COPY POLICYSET (Maßnahmengruppe kopieren)
- COPY PROFILE (Profil kopieren)
- COPY SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl kopieren)
- COPY SCRIPT (IBM Spectrum Protect-Prozedur kopieren)
- COPY SERVERGROUP (Server-Gruppe kopieren)

## COPY ACTIVEdata (Aktive Sicherungsdaten aus einem primären Speicherpool in einen Pool für aktive Daten kopieren)

Mit diesem Befehl können aktive Versionen von Sicherungsdaten aus einem primären Speicherpool in einen Pool für aktive Daten kopiert werden. Der primäre Vorteil von Pools für aktive Daten sind schnelle Clientzurückschreibungen. Kopieren Sie Ihre aktiven Daten regelmäßig, um sicherzustellen, dass die Daten in einem Katastrophenfall geschützt sind.

Ist eine Datei bereits in dem Pool für aktive Daten vorhanden, wird die Datei nicht kopiert, es sei denn, die Kopie der Datei in dem Pool für aktive Daten ist als beschädigt markiert. Es wird jedoch keine neue Kopie erstellt, wenn die Datei in dem primären Speicherpool auch als beschädigt markiert ist. In einem Speicherpool mit wahlfreiem Zugriff werden weder Cache-Kopien von umgelagerten Dateien noch beschädigte Primärdateien kopiert.

Wenn die Umlagerung für einen Speicherpool beginnt, während aktive Daten kopiert werden, werden einige Dateien möglicherweise umgelagert, bevor sie kopiert werden. Aus diesem Grund sollten Sie aktive Daten aus Speicherpools, die sich an einer höheren Position in der Umlagerungshierarchie befinden, vor den aktiven Daten aus Speicherpools kopieren, die sich an einer niedrigeren Position befinden. Stellen Sie sicher, dass ein Kopierprozess beendet ist, bevor ein anderer Kopierprozess beginnt.

Hinweis:

- Sie können nur aktive Daten aus Speicherpools kopieren, die das Datenformat NATIVE oder NONBLOCK haben.
- Wird dieser Befehl für einen primären Speicherpool ausgegeben, der für die Deduplizierung von Daten definiert ist, werden doppelte Daten entfernt, wenn der Pool für aktive Daten ebenfalls für die Deduplizierung von Daten definiert ist.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Pool für aktive Daten erforderlich, aus dem aktive Versionen von Sicherungsdaten kopiert werden.

## Syntax

```
>>-COPY ACTIVEdata--Name_des_primären_Pools--Name_des_Pools_für_aktive_Daten-->
. -MAXProcess-----1-----
>--+-----+----->
' -MAXProcess-----Anzahl-- '

. -Preview-----No----- . -Wait-----No-----
>--+-----+-----+-----+----->
' -Preview-----+No-----+ ' ' -Wait-----+No-----+ '
      +-Yes-----+                '-Yes-'
```





Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird dieser Prozess abgebrochen, wurden möglicherweise bereits einige Dateien vor dem Abbruch kopiert.

Yes

Gibt an, dass der Server diese Operation im Vordergrund ausführt. Die Operation muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dem Verwaltungsclient an, wenn die Operation beendet ist.

Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

SHREDTONOshred

Gibt an, ob Daten aus einem primären Speicherpool, der das Schreddern erzwingt, in einen Pool für aktive Daten, der das Schreddern nicht erzwingt, kopiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, dass der Server das Kopieren von Daten aus einem primären Speicherpool, der das Schreddern erzwingt, in einen Pool für aktive Daten, der das Schreddern nicht erzwingt, nicht zulässt. Wenn der primäre Speicherpool das Schreddern erzwingt und der Pool für aktive Daten das Schreddern nicht erzwingt, schlägt die Operation fehl.

Yes

Gibt an, dass der Server das Kopieren von Daten aus einem primären Speicherpool, der das Schreddern erzwingt, in einen Pool für aktive Daten, der das Schreddern nicht erzwingt, zulässt. Die Daten in dem Pool für aktive Daten werden nicht geschreddert, wenn er gelöscht wird.

## Beispiel: Daten aus einem primären Speicherpool in einen Pool für aktive Daten kopieren

Die aktiven Daten aus dem primären Speicherpool PRIMARY\_POOL in den Pool für aktive Daten mit dem Namen ACTIVEPOOL kopieren. Den folgenden Befehl ausgeben:

```
copy activedata primary_pool activepool
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COPY ACTIVEDATA

| Befehl          | Beschreibung  |
|-----------------|---|
| DEFINE DOMAIN   | Definiert eine Maßnahmendomäne, der Clients zugeordnet werden können.   |
| DEFINE STGPOOL  | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.                                    |
| EXPORT NODE     | Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.                       |
| EXPORT SERVER   | Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server. |
| IMPORT NODE     | Schreibt Clientknotendaten von externen Datenträgern zurück.  |
| IMPORT SERVER   | Schreibt den gesamten Server oder einen Teil davon von externen Datenträgern zurück.                                  |
| MOVE NODEDATA   | Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen.         |
| QUERY CONTENT   | Zeigt Informationen über Dateien in einem Speicherpooldatenträger an.   |
| QUERY DOMAIN    | Zeigt Informationen über Maßnahmendomänen an.   |
| QUERY NODE      | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.                                     |
| QUERY NODEDATA  | Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.                                       |
| QUERY STGPOOL   | Zeigt Informationen zu Speicherpools an.  |
| RESTORE STGPOOL | Schreibt Dateien aus Kopierspeicherpools in einen primären Speicherpool zurück.                                       |

| Befehl         | Beschreibung  |
|----------------|---|
| RESTORE VOLUME | Schreibt Dateien, die auf angegebenen Datenträgern in einem primären Speicherpool gespeichert sind, aus Kopierspeicherpools zurück. |
| UPDATE DOMAIN  | Ändert die Attribute einer Maßnahmendomäne.   |
| UPDATE STGPOOL | Ändert die Attribute eines Speicherpools.   |

## COPY CLOPTSET (Clientoptionsgruppe kopieren)

Mit diesem Befehl kann eine Clientoptionsgruppe kopiert werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, der der Clientknoten zugeordnet ist.

### Syntax

```
>>-COPY CLOptset--aktueller_Optionsgruppenname--neuer_Optionsgruppenname-><
```

### Parameter

aktueller\_Optionsgruppenname (Erforderlich)

Gibt den Namen der zu kopierenden Client-Optionsgruppe an.

neuer\_Optionsgruppenname (Erforderlich)

Gibt den Namen der neuen Client-Optionsgruppe an. Die maximale Länge des Namens beträgt 64 Zeichen.

### Beispiel: Eine Clientoptionsgruppe kopieren

Die Clientoptionsgruppe ENG in die neue Clientoptionsgruppe ENG2 kopieren.

```
copy cloptset eng eng2
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COPY CLOPTSET

| Befehl           | Beschreibung  |
|------------------|---|
| DEFINE CLIENTOPT | Fügt einer Clientoptionsgruppe eine Clientoption hinzu.                       |
| DEFINE CLOPTSET  | Definiert eine Clientoptionsgruppe.   |
| DELETE CLIENTOPT | Löscht eine Clientoption aus einer Clientoptionsgruppe.                       |
| DELETE CLOPTSET  | Löscht eine Clientoptionsgruppe.  |
| QUERY CLOPTSET   | Zeigt Informationen über eine Clientoptionsgruppe an.                         |
| UPDATE CLIENTOPT | Aktualisiert die Folgenummer einer Clientoption in einer Clientoptionsgruppe. |
| UPDATE CLOPTSET  | Aktualisiert die Beschreibung einer Clientoptionsgruppe.                      |

## COPY DOMAIN (Maßnahmendomäne kopieren)

Mit diesem Befehl kann eine Kopie einer Maßnahmendomäne erstellt werden.

Der Server kopiert die folgenden Informationen in die neue Domäne:

- Beschreibung der Maßnahmendomäne
- Maßnahmengruppen in der Maßnahmendomäne (einschließlich der AKTIVEN Maßnahmengruppe, wenn eine Maßnahmengruppe aktiviert ist)
- Verwaltungsklassen in jeder Maßnahmengruppe (einschließlich der Standardverwaltungsklasse, falls zugeordnet)

- Kopiengruppen in jeder Verwaltungsklasse

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-COpy Domain--aktueller_Domänenname--neuer_Domänenname-----<<
```

## Parameter

aktueller\_Domänenname (Erforderlich)

Gibt die Maßnahmendomäne an, die kopiert werden soll.

neuer\_Domänenname (Erforderlich)

Gibt den Namen der neuen Maßnahmendomäne an. Die maximale Länge dieses Namens beträgt 30 Zeichen.

## Beispiel: Eine Maßnahmendomäne in eine neue Maßnahmendomäne kopieren

Die Maßnahmendomäne STANDARD in die neue Maßnahmendomäne ENGPOLDOM kopieren, indem der folgende Befehl eingegeben wird:

```
copy domain standard engpoldom
```

ENGPOLDOM enthält jetzt die Standardmaßnahmengruppe, die Verwaltungsklasse, die Sicherungskopiengruppe und die Archivierungskopiengruppe.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COPY DOMAIN

| Befehl             | Beschreibung  |
|--------------------|---|
| ACTIVATE POLICYSET | Wertet eine Maßnahmengruppe aus und aktiviert sie.  |
| COPY MGMTCLASS     | Erstellt eine Kopie einer Verwaltungsklasse.  |
| DEFINE COPYGROUP   | Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse. |
| DEFINE DOMAIN      | Definiert eine Maßnahmendomäne, der Clients zugeordnet werden können.   |
| DEFINE MGMTCLASS   | Definiert eine Verwaltungsklasse.   |
| DEFINE POLICYSET   | Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.   |
| DELETE COPYGROUP   | Löscht eine Sicherungs- oder Archivierungskopiengruppe aus einer Maßnahmendomäne und Maßnahmengruppe.                         |
| DELETE DOMAIN      | Löscht eine Maßnahmendomäne und, falls vorhanden, Maßnahmenobjekte in der Maßnahmendomäne.                                    |
| DELETE MGMTCLASS   | Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe.                     |
| QUERY COPYGROUP    | Zeigt die Attribute einer Kopiengruppe an.  |
| QUERY DOMAIN       | Zeigt Informationen über Maßnahmendomänen an.   |
| QUERY MGMTCLASS    | Zeigt Informationen zu Verwaltungsklassen an.   |
| QUERY POLICYSET    | Zeigt Informationen über Maßnahmengruppen an.   |
| REGISTER NODE      | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.                                       |
| UPDATE COPYGROUP   | Ändert ein oder mehrere Attribute einer Kopiengruppe.   |
| UPDATE DOMAIN      | Ändert die Attribute einer Maßnahmendomäne.   |

| Befehl             | Beschreibung  |
|--------------------|---|
| UPDATE MGMTCLASS   | Ändert die Attribute einer Verwaltungsklasse.   |
| UPDATE POLICYSET   | Ändert die Beschreibung einer Maßnahmengruppe.  |
| VALIDATE POLICYSET | Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert. |

## COPY MGMTCLASS (Verwaltungsklasse kopieren)

Mit diesem Befehl kann eine Kopie einer Verwaltungsklasse innerhalb derselben Maßnahmengruppe erstellt werden.

Der Server kopiert die folgenden Informationen in die neue Verwaltungsklasse:

- Beschreibung der Verwaltungsklasse
- Für die Verwaltungsklasse definierte Kopiengruppen
- Alle Attribute für die Verwaltung von Dateien für IBM Spectrum Protect for Space Management-Clients

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die neue Verwaltungsklasse gehört.

### Syntax

```
>>-COpy MGMTclass--Domänenname--Name_der_Maßnahmengruppe----->
>--aktueller_Klassenname--neuer_Klassenname-----<<
```

### Parameter

Domänenname (Erforderlich)

Gibt die Maßnahmendomäne an, zu der die Verwaltungsklasse gehört.

Name\_der\_Maßnahmengruppe (Erforderlich)

Gibt die Maßnahmengruppe an, zu der die Verwaltungsklasse gehört.

aktueller\_Klassenname (Erforderlich)

Gibt die Verwaltungsklasse an, die kopiert werden soll.

neuer\_Klassenname (Erforderlich)

Gibt den Namen der neuen Verwaltungsklasse an. Die maximale Länge dieses Namens beträgt 30 Zeichen.

### Beispiel: Eine Verwaltungsklasse in eine neue Verwaltungsklasse kopieren

Die Verwaltungsklasse ACTIVEFILES in die neue Verwaltungsklasse FILEHISTORY kopieren. Die Verwaltungsklasse befindet sich in Maßnahmengruppe VACATION in der Maßnahmendomäne EMPLOYEE\_RECORDS.

```
copy mgmtclass employee_records vacation
activefiles filehistory
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COPY MGMTCLASS

| Befehl           | Beschreibung  |
|------------------|---|
| DEFINE COPYGROUP | Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse. |
| DELETE MGMTCLASS | Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe.                     |
| QUERY COPYGROUP  | Zeigt die Attribute einer Kopiengruppe an.  |
| QUERY MGMTCLASS  | Zeigt Informationen zu Verwaltungsklassen an.   |
| QUERY POLICYSET  | Zeigt Informationen über Maßnahmengruppen an.   |

| Befehl           | Beschreibung  |
|------------------|---|
| UPDATE COPYGROUP | Ändert ein oder mehrere Attribute einer Kopiengruppe. |
| UPDATE MGMTCLASS | Ändert die Attribute einer Verwaltungsklasse.         |

## COPY POLICYSET (Maßnahmengruppe kopieren)

Mit diesem Befehl kann eine Maßnahmengruppe (einschließlich der AKTIVEN Maßnahmengruppe) innerhalb derselben Maßnahmendomäne kopiert werden.

Der Server kopiert die folgenden Informationen in die neue Maßnahmengruppe:

- Beschreibung der Maßnahmengruppe
- Verwaltungsklassen in der Maßnahmengruppe (einschließlich der Standardverwaltungsklasse, falls zugeordnet)
- Kopiengruppen in jeder Verwaltungsklasse

Die Maßnahmen in der neuen Maßnahmengruppe werden erst wirksam, wenn Sie die neue Gruppe als Maßnahmengruppe ACTIVE definieren.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die neue Maßnahmengruppe gehört.

### Syntax

```
>>-COPY Policyset--Domänenname--aktueller_Gruppenname--neuer_Gruppenname-><
```

### Parameter

Domänenname (Erforderlich)

Gibt die Maßnahmendomäne an, zu der die Maßnahmengruppe gehört.

aktueller\_Gruppenname (Erforderlich)

Gibt die Maßnahmengruppe an, die kopiert werden soll.

neuer\_Gruppenname (Erforderlich)

Gibt den Namen der neuen Maßnahmengruppe an. Die maximale Länge dieses Namens beträgt 30 Zeichen.

### Beispiel: Eine Maßnahmengruppe in eine neue Maßnahmengruppe kopieren

Die Maßnahmengruppe VACATION in die neue Maßnahmengruppe HOLIDAY in der Maßnahmendomäne EMPLOYEE\_RECORDS kopieren.

```
copy policyset employee_records vacation holiday
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COPY POLICYSET

| Befehl             | Beschreibung  |
|--------------------|---|
| ACTIVATE POLICYSET | Wertet eine Maßnahmengruppe aus und aktiviert sie.  |
| COPY MGMTCLASS     | Erstellt eine Kopie einer Verwaltungsklasse.  |
| DEFINE MGMTCLASS   | Definiert eine Verwaltungsklasse.   |
| DELETE POLICYSET   | Löscht eine Maßnahmengruppe einschließlich ihrer Verwaltungsklassen und Kopiengruppen aus einer Maßnahmendomäne.        |
| QUERY POLICYSET    | Zeigt Informationen über Maßnahmengruppen an.   |
| UPDATE POLICYSET   | Ändert die Beschreibung einer Maßnahmengruppe.  |
| VALIDATE POLICYSET | Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert. |

## COPY PROFILE (Profil kopieren)

Mit diesem Befehl können auf einem Konfigurationsmanager ein Profil und alle zugeordneten Objektnamen in ein neues Profil kopiert werden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-COPY PROFILE--aktueller_Profilname--neuer_Profilname-----<<
```

### Parameter

aktueller\_Profilname (Erforderlich)

Gibt das Profil an, das kopiert werden soll.

neuer\_Profilname (Erforderlich)

Gibt den Namen des neuen Profils an. Die maximale Länge des Profilenames beträgt 30 Zeichen.

### Beispiel: Eine Kopie eines Profils erstellen

Das Profil VAL in das neue Profil VAL2 kopieren.

```
copy profile val val2
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COPY PROFILE

| Befehl                 | Beschreibung   |
|------------------------|--|
| DEFINE PROFASSOCIATION | Ordnet Objekte einem Profil zu.  |
| DEFINE PROFILE         | Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.  |
| DEFINE SUBSCRIPTION    | Subskribiert einen verwalteten Server für ein Profil.                            |
| DELETE PROFASSOCIATION | Löscht die Zuordnung zwischen einem Objekt und einem Profil.                     |
| DELETE PROFILE         | Löscht ein Profil aus einem Konfigurationsmanager.                               |
| DELETE SUBSCRIBER      | Löscht veraltete Subskriptionen verwalteter Server.                              |
| DELETE SUBSCRIPTION    | Löscht eine angegebene Profilsubskription.                                       |
| LOCK PROFILE           | Verhindert die Verteilung eines Konfigurationsprofils.                           |
| NOTIFY SUBSCRIBERS     | Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin. |
| QUERY PROFILE          | Zeigt Informationen über Konfigurationsprofile an.                               |
| QUERY SUBSCRIBER       | Zeigt Informationen über Subskribenten und ihre Subskriptionen für Profile an.   |
| QUERY SUBSCRIPTION     | Zeigt Informationen über Profilsubskriptionen an.                                |
| SET CONFIGMANAGER      | Gibt an, ob ein Server ein Konfigurationsmanager ist.                            |
| UNLOCK PROFILE         | Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server.         |
| UPDATE PROFILE         | Ändert die Beschreibung eines Profils.   |

## COPY SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl kopieren)

Mit diesem Befehl kann eine Kopie eines Zeitplans erstellt werden.

Der Befehl COPY SCHEDULE kann zwei Formen haben, je nachdem, ob der Zeitplan Client-Operationen oder Verwaltungsbefehle betrifft. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für COPY SCHEDULE

| Befehl             | Beschreibung  |
|--------------------|---|
| DEFINE ASSOCIATION | Ordnet Clients einem Zeitplan zu.   |
| DEFINE SCHEDULE    | Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl. |
| DELETE SCHEDULE    | Löscht einen Zeitplan aus der Datenbank.  |
| QUERY SCHEDULE     | Zeigt Informationen über Zeitpläne an.  |
| UPDATE SCHEDULE    | Ändert die Attribute eines Zeitplans.   |

- COPY SCHEDULE (Kopie eines Zeitplans für Clientoperationen erstellen)  
Mit dem Befehl COPY SCHEDULE kann eine Kopie eines Zeitplans für Clientoperationen erstellt werden. Ein Zeitplan kann innerhalb einer Maßnahmendomäne oder von einer Maßnahmendomäne in eine andere Maßnahmendomäne kopiert werden. Mit dem Befehl DEFINE ASSOCIATION kann der neue Zeitplan den Clientknoten zugeordnet werden.
- COPY SCHEDULE (Kopie eines Zeitplans für Verwaltungsoperationen erstellen)  
Mit dem Befehl COPY SCHEDULE kann eine Kopie eines Zeitplans für Verwaltungsbefehle erstellt werden.

## COPY SCHEDULE (Kopie eines Zeitplans für Clientoperationen erstellen)

Mit dem Befehl COPY SCHEDULE kann eine Kopie eines Zeitplans für Clientoperationen erstellt werden. Ein Zeitplan kann innerhalb einer Maßnahmendomäne oder von einer Maßnahmendomäne in eine andere Maßnahmendomäne kopiert werden. Mit dem Befehl DEFINE ASSOCIATION kann der neue Zeitplan den Clientknoten zugeordnet werden.

### Berechtigungsklasse

Zum Kopieren eines Clientzeitplans ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, in die der Zeitplan kopiert wird.

### Syntax

```
>>-COpy SChedule--aktueller_Domänenname----->
>--aktueller_Zeitplanname--neuer_Domänenname----->
  .-aktueller_Zeitplanname-. .-REPlace===-No-----
>-----+-----+-----+-----+-----><
  '-neuer_Zeitplanname-----' '-REPlace===-+No--+-'
                                     '-Yes-'
```

### Parameter

aktueller\_Domänenname (Erforderlich)

Gibt den Namen der Maßnahmendomäne an, in der sich der Zeitplan befindet, der kopiert werden soll.

aktueller\_Zeitplanname (Erforderlich)

Gibt den Namen des Zeitplans an, der kopiert werden soll.

neuer\_Domänenname (Erforderlich)

Gibt den Namen einer Maßnahmendomäne an, in die der neue Zeitplan kopiert werden soll.

neuer\_Zeitplanname

Gibt den Namen des neuen Zeitplans an. Für den Namen können bis zu 30 Zeichen angegeben werden.

Wird dieser Name nicht angegeben, wird der Name des ursprünglichen Zeitplans verwendet.

Wenn der Zeitplanname bereits in der Maßnahmendomäne definiert ist, muß REPLACE=YES angegeben werden, damit der Befehl nicht fehlschlägt.

REPLace

Gibt an, ob ein Client-Zeitplan ersetzt werden soll. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, daß ein Client-Zeitplan nicht ersetzt wird.

Yes

Gibt an, daß ein Client-Zeitplan ersetzt wird.

## Beispiel: Einen Zeitplan aus einer Maßnahmendomäne in eine andere Maßnahmendomäne kopieren

---

Den Zeitplan WEEKLY\_BACKUP, der zur Maßnahmendomäne EMPLOYEE\_RECORDS gehört, in die Maßnahmendomäne PROG1 kopieren und den neuen Zeitplan WEEKLY\_BACK2 benennen. Ist bereits ein Zeitplan dieses Namens in der Maßnahmendomäne PROG1 definiert, darf er nicht ersetzt werden.

```
copy schedule employee_records weekly_backup  
prog1 weekly_back2
```

## COPY SCHEDULE (Kopie eines Zeitplans für Verwaltungsoperationen erstellen)

---

Mit dem Befehl COPY SCHEDULE kann eine Kopie eines Zeitplans für Verwaltungsbefehle erstellt werden.

### Berechtigungsklasse

---

Zum Kopieren eines Zeitplans für Verwaltungsbefehle ist die Systemberechtigung erforderlich.

### Syntax

---

```
>>-COpy SChedule--aktueller_Zeitplanname--neuer_Zeitplanname---->  
                                     .-REPlace----No-----.  
>--Type----Administrative--+-----+-----><  
                                     '-REPlace----+No--+-'  
                                     '-Yes-'
```

### Parameter

---

aktueller\_Zeitplanname (Erforderlich)

Gibt den Namen des Zeitplans an, der kopiert werden soll.

neuer\_Zeitplanname (Erforderlich)

Gibt den Namen des neuen Zeitplans an. Für den Namen können bis zu 30 Zeichen angegeben werden.

Wenn der Zeitplanname bereits definiert ist, muß REPLACE=YES angegeben werden, damit der Befehl nicht fehlschlägt.

Type=Administrative

Gibt an, daß ein Zeitplan für Verwaltungsbefehle kopiert werden soll.

REPlace

Gibt an, ob ein Zeitplan für Verwaltungsbefehle ersetzt werden soll. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, daß ein Zeitplan für Verwaltungsbefehle nicht ersetzt wird.

Yes

Gibt an, daß ein Zeitplan für Verwaltungsbefehle ersetzt wird.

## Beispiel: Einen Zeitplan für Verwaltungsbefehle in einen anderen Zeitplan kopieren

---

Den Zeitplan für Verwaltungsbefehle mit dem Namen DATA\_BACKUP kopieren und in DATA\_ENG umbenennen. Ist bereits ein Zeitplan mit diesem Namen vorhanden, den Zeitplan ersetzen.

```
copy schedule data_backup data_eng  
type=administrative replace=yes
```

## COPY SCRIPT (IBM Spectrum Protect-Prozedur kopieren)

---

Verwenden Sie diesen Befehl, um eine vorhandene IBM Spectrum Protect-Prozedur in eine neue Prozedur mit einem anderen Namen zu kopieren.



## Berechtigungsklasse

---

Für diesen Befehl ist die Bediener-, Maßnahmen-, Speicher- oder Systemberechtigung erforderlich.

## Syntax

---

```
>>-COpy SCRIPT--aktueller_Prozedurname--neuer_Prozedurname-----><
```

## Parameter

---

aktueller\_Prozedurname (Erforderlich)

Gibt den Namen der Prozedur an, die kopiert werden soll.

neuer\_Prozedurname (Erforderlich)

Gibt den Namen der neuen Prozedur an. Für den Namen können bis zu 30 Zeichen angegeben werden.

## Beispiel: Eine Kopie eines Scripts erstellen

---

Prozedur TESTDEV in eine neue Prozedur kopieren und in ENGDEV umbenennen.

```
copy script testdev engdev
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für COPY SCRIPT

| Befehl        | Beschreibung  |
|---------------|---|
| DEFINE SCRIPT | Definiert eine Prozedur für den IBM Spectrum Protect-Server.  |
| DELETE SCRIPT | Löscht eine Prozedur oder einzelne Zeilen aus einer Prozedur. |
| QUERY SCRIPT  | Zeigt Informationen über Prozeduren an.                       |
| RENAME SCRIPT | Vergibt einen neuen Namen für eine Prozedur.                  |
| RUN           | Führt ein Script aus.   |
| UPDATE SCRIPT | Ändert Zeilen oder fügt Zeilen in einer Prozedur hinzu.       |

## COPY SERVERGROUP (Server-Gruppe kopieren)

---

Mit diesem Befehl kann eine Kopie einer Server-Gruppe erstellt werden.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-COpy SERVERGroup--aktueller_Gruppenname--neuer_Gruppenname--><
```

## Parameter

---

aktueller\_Gruppenname (Erforderlich)

Gibt die Server-Gruppe an, die kopiert werden soll.

neuer\_Gruppenname (Erforderlich)

Gibt den Namen der neuen Server-Gruppe an. Die maximale Länge dieses Namens beträgt 64 Zeichen.

## Beispiel: Eine Kopie einer Servergruppe erstellen

---

Die Server-Gruppe GRP\_PAYROLL in die neue Gruppe HQ\_PAYROLL kopieren.

```
copy servergroup grp_payroll hq_payroll
```

Tabelle 1. Zugehörige Befehle für COPY SERVERGROUP

| Befehl             | Beschreibung   |
|--------------------|--|
| DEFINE GRPMEMBER   | Definiert einen Server als Teil einer Servergruppe.          |
| DEFINE SERVER      | Definiert einen Server für die Übertragung zwischen Servern. |
| DEFINE SERVERGROUP | Definiert eine neue Servergruppe.                            |
| DELETE GRPMEMBER   | Löscht einen Server aus einer Servergruppe.                  |
| DELETE SERVER      | Löscht die Definition eines Servers.                         |
| DELETE SERVERGROUP | Löscht eine Servergruppe.                                    |
| MOVE GRPMEMBER     | Versetzt einen Teil einer Servergruppe.                      |
| QUERY SERVER       | Zeigt Informationen über Server an.                          |
| QUERY SERVERGROUP  | Zeigt Informationen über Servergruppen an.                   |
| RENAME SERVERGROUP | Benennt eine Servergruppe um.                                |
| UPDATE SERVER      | Aktualisiert Informationen über einen Server.                |
| UPDATE SERVERGROUP | Aktualisiert eine Servergruppe.                              |

## DEACTIVATE DATA (Daten für einen Clientknoten inaktivieren)

Mit diesem Befehl können Sie angeben, dass aktive Daten, die für einen Anwendungsclientknoten vor einem angegebenen Datum gesichert wurden, nicht mehr benötigt werden. Der Befehl markiert die Daten als inaktiv, sodass sie gemäß Ihren Datenaufbewahrungsmaßnahmen gelöscht werden können.

Einschränkung: Der Befehl DEACTIVATE DATA gilt nur für Anwendungsclients, die Oracle-Datenbanken schützen.

Wenn Sie den Befehl DEACTIVATE DATA ausgeben, werden alle aktiven Sicherungsdaten, die vor dem angegebenen Datum gespeichert wurden, inaktiv. Die Daten können nicht mehr abgerufen werden und werden bei ihrem Verfall gelöscht.

Der Befehl DEACTIVATE DATA betrifft nur die Dateien, die vor dem angegebenen Datum und der angegebenen Zeit auf den Server kopiert wurden. Auf die Dateien, die nach dem angegebenen Datum kopiert wurden, kann noch zugegriffen werden, und der Client kann noch auf den Server zugreifen.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>DEACTivate DAta--Knotenname--TODate---Datum----->
      .-TOTime----23:59:59-.  .-Wait----No-----
>+-----+-----+-----+-----><
  '-TOTime----Zeit-----'  '-Wait-----No---'
                               '-Yes-'
```

## Parameter

Knotenname (Erforderlich)

Gibt den Namen eines Anwendungsclientknotens an, dessen Daten inaktiviert werden sollen.

TODate (Erforderlich)

Gibt das Datum an, das für die Auswahl der Sicherungsdateien, die inaktiviert werden sollen, verwendet werden soll. IBM Spectrum Protect inaktiviert nur die Dateien mit einem Datum bis zu dem angegebenen Datum (einschließlich). Sie können das Datum mit einem der folgenden Werte angeben:

| Wert       | Beschreibung         | Beispiel   |
|------------|----------------------|------------|
| MM/TT/JJJJ | Ein bestimmtes Datum | 01/23/2014 |

| Wert                         | Beschreibung   | Beispiel  |
|------------------------------|--|---|
| TODAY                        | Das aktuelle Datum   | TODAY   |
| TODAY-Tage <b>oder</b> -Tage | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY-30 <b>oder</b> -30.<br>Um Dateien zu inaktivieren, die mindestens 30 Tage alt sind, können Sie TODAY-30 oder -30 angeben. |
| EOLM                         | Ende des letzten Monats. Der letzte Tag des Vormonats.   | EOLM  |
| EOLM-Tage                    | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br>Um Dateien zu inaktivieren, die am Tag vor dem letzten Tag des Vormonats aktiv waren.                                 |
| BOTM                         | Anfang dieses Monats. Der erste Tag des aktuellen Monats.  | BOTM  |
| BOTM+Tage                    | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br>Um Dateien zu inaktivieren, die am zehnten Tag des aktuellen Monats aktiv waren.                                      |

#### TOTIME

Gibt an, dass Dateien inaktiviert werden sollen, die vor dieser Zeit am angegebenen Datum auf dem Server erstellt wurden. Dieser Parameter ist wahlfrei. Der Standardwert ist das Ende des Tages (23:59:59). Geben Sie die Uhrzeit mit einem der folgenden Werte an:

| Wert                         | Beschreibung  | Beispiel   |
|------------------------------|---|--|
| HH:MM:SS                     | Eine bestimmte Uhrzeit am angegebenen Datum                             | 12:30:22   |
| NOW                          | Die aktuelle Uhrzeit am angegebenen Datum                               | NOW  |
| NOW+HH:MM <b>oder</b> +HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Datum  | NOW+03:00 <b>oder</b> +03:00.<br>Wenn Sie den Befehl DEACTIVATE DATA um 9:00 Uhr mit TOTIME=NOW+03:00 oder TOTIME=+03:00 ausgeben, inaktiviert IBM Spectrum Protect Dateien, die um 12:00 Uhr oder früher am angegebenen Datum auf den Server gestellt wurden. |
| NOW-HH:MM <b>oder</b> -HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Datum | NOW-03:30 <b>oder</b> -03:30.<br>Wenn Sie den Befehl DEACTIVATE DATA um 9:00 Uhr mit TOTIME=NOW-3:30 oder TOTIME=-3:30 ausgeben, inaktiviert IBM Spectrum Protect Dateien, die um 5:30 Uhr oder früher am angegebenen Datum auf den Server gestellt wurden.    |

#### Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Geben Sie die folgenden Werte an:

##### No

Der Server verarbeitet diesen Befehl im Hintergrund und Sie können mit anderen Tasks fortfahren, während der Befehl verarbeitet wird. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden entweder in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, je nachdem, wo die Nachrichten protokolliert werden.

##### Yes

Der Server verarbeitet diesen Befehl im Vordergrund. Die Operation muss beendet sein, bevor mit anderen Tasks fortgeföhren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.

Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

## Beispiel: Daten für einen Data Protection-Clientknoten inaktivieren

Der Clientknoten BANDIT ist ein IBM Spectrum Protect for Databases: Data Protection for Oracle-Anwendungsclient. Alle Sicherungsdaten sind aktiv und somit werden alle Sicherungsdaten aufbewahrt. Mit dem folgenden Befehl werden Daten inaktiviert, die

vor dem 3. Januar 2014 gesichert wurden, sodass die Daten bei ihrem Verfall gelöscht werden können.

```
deactivate data bandit todate=01/23/2014
```

Um Daten regelmäßig zu inaktivieren, sodass sie bei ihrem Verfall gelöscht werden können, können Sie den folgenden Befehl in einem Clientzeitplan ausführen.

```
deactivate data bandit todate=today
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEACTIVATE DATA

| Befehl            | Beschreibung                                    |
|-------------------|---|
| DECOMMISSION NODE | Legt einen Anwendungs- oder Systemknoten still. |
| DECOMMISSION VM   | Legt eine virtuelle Maschine still.             |

## DECOMMISSION-Befehle

Verwenden Sie die DECOMMISSION-Befehle, um Clientknoten aus der Produktionsumgebung zu entfernen. Clientknoten umfassen Anwendungen, Systeme und virtuelle Maschinen.

- DECOMMISSION NODE (Anwendungs- oder Systemknoten stilllegen)
- DECOMMISSION VM (Virtuelle Maschine stilllegen)

## DECOMMISSION NODE (Anwendungs- oder Systemknoten stilllegen)

Verwenden Sie diesen Befehl, um einen Anwendungs- oder Systemclientknoten der Produktionsumgebung stillzulegen. Alle Sicherungsdaten, die für den Clientknoten gespeichert werden, verfallen gemäß den Maßnahmeneinstellungen, sofern Sie die Daten nicht explizit löschen.

Achtung: Diese Aktion kann nicht umgekehrt werden und hat das Löschen von Daten zur Folge. Obwohl dieser Befehl die Clientknotendefinition erst löscht, nachdem die Daten verfallen sind, kann die Stilllegung des Clientknotens nicht rückgängig gemacht werden. Nachdem Sie diesen Befehl ausgegeben haben, kann der Clientknoten nicht auf den Server zugreifen und seine Daten werden nicht gesichert. Der Clientknoten wird gesperrt und kann nur zum Zurückschreiben von Dateien entsperrt werden. Dateibereiche, die zu dem Clientknoten gehören, und der Clientknoten selbst werden schließlich entfernt.

Mit diesem Befehl können die folgenden Typen von Clientknoten stillgelegt werden:

### Anwendungsclientknoten

Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

### Systemclientknoten

Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

Wenn ein Clientknoten nicht mehr in der Produktionsumgebung benötigt wird, können Sie diesen Befehl ausgeben, um eine schrittweise, gesteuerte Stilllegungsoperation einzuleiten. Der Befehl führt die folgenden Aktionen aus:

- Löscht alle Zeitplanzuordnungen für den Clientknoten. Zeitpläne werden nicht mehr auf dem Clientknoten ausgeführt. Diese Aktion entspricht der Ausgabe des Befehls DELETE ASSOCIATION für jeden Zeitplan, dem der Clientknoten zugeordnet ist.
- Verhindert, dass der Client auf den Server zugreift. Diese Aktion entspricht der Ausgabe des Befehls LOCK NODE.

Nach der Ausführung des Befehls werden Clientknotendaten nicht mehr auf dem Server gesichert. Daten, die vor der Stilllegung des Clientknotens gesichert wurden, werden nicht sofort auf dem Server gelöscht. Alle Sicherungsdateiversionen, einschließlich der neuesten Sicherung, sind jedoch jetzt inaktive Kopien. Die Clientdateien werden auf dem Server gemäß ihren Speicherwaltungsmaßnahmen aufbewahrt.

Nach dem Ablauf aller Datenaufbewahrungszeiträume und dem Entfernen aller Clientsicherungs- und -archivierungsdateikopien aus dem Serverspeicher löscht IBM Spectrum Protect die Dateibereiche, die zu dem stillgelegten Knoten gehören. Diese Aktion entspricht der Ausgabe des Befehls DELETE FILESPACE.

Nach dem Löschen der Dateibereiche für den stillgelegten Knoten wird die Knotendefinition auf dem Server gelöscht. Diese Aktion entspricht der Ausgabe des Befehls REMOVE NODE.

Nach der Stilllegung eines Clientknotens, aber vor dem Entfernen des Knotens auf dem Server können Sie mithilfe des Befehls QUERY NODE überprüfen, ob der Clientknoten stillgelegt ist.

Einschränkung: Sie können keinen Clientknoten stilllegen, der für die Replikation konfiguriert ist. Sie können den Replikationsstatus eines Clientknotens mithilfe des Befehls QUERY NODE bestimmen. Wenn ein Clientknoten für die Replikation konfiguriert ist, können Sie den Clientknoten mit dem Befehl REMOVE REPLNODE aus der Replikation entfernen.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-DECommission Node--Knotenname--+-Wait-----No-----+-----><
                                     '-Wait-----+No--+'
                                     '-Yes-'
```

## Parameter

Knotenname (Erforderlich)

Gibt den Namen des Clientknotens an, der stillgelegt werden soll.

Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können die folgenden Werte angeben:

No

Der Server verarbeitet diesen Befehl im Hintergrund und Sie können mit anderen Tasks fortfahren, während der Befehl verarbeitet wird. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden entweder in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, je nachdem, wo die Nachrichten protokolliert werden.

Yes

Der Server verarbeitet diesen Befehl im Vordergrund. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.

Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

## Beispiel: Einen Clientknoten stilllegen

Den Clientknoten CODY stilllegen.

```
decommission node cody
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DECOMMISSION NODE

| Befehl          | Beschreibung                              |
|-----------------|---|
| DECOMMISSION VM | Legt eine virtuelle Maschine still.       |
| DEACTIVATE DATA | Inaktiviert Daten für einen Clientknoten. |

## DECOMMISSION VM (Virtuelle Maschine stilllegen)

Verwenden Sie diesen Befehl, um eine einzelne virtuelle Maschine innerhalb eines Datencenterknotens zu entfernen. Der Dateibereich, der die virtuelle Maschine darstellt, wird erst nach dem Verfall seiner Sicherungsdaten auf dem Server gelöscht.

Achtung: Dieser Befehl kann nicht umgekehrt werden und hat das Löschen von Daten zur Folge. Obwohl dieser Befehl den Dateibereich der virtuellen Maschine erst löscht, nachdem die Daten verfallen sind, kann die Stilllegung der virtuellen Maschine nicht rückgängig gemacht werden.



```
decommission vm dept06node cody
```

Legen Sie die virtuelle Maschine CODY 2 still.

```
decommission vm dept06node "cody 2"
```

Legen Sie eine virtuelle Maschine durch Angabe ihrer Dateibereichs-ID still.

```
decommission vm dept06node 7 nametype=fsid
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für DECOMMISSION VM

| Befehl            | Beschreibung                                    |
|-------------------|---|
| DECOMMISSION NODE | Legt einen Anwendungs- oder Systemknoten still. |
| DEACTIVATE DATA   | Inaktiviert Daten für einen Clientknoten.       |

## DEFINE-Befehle

---

Mit den DEFINE-Befehlen können IBM Spectrum Protect-Objekte erstellt werden.

- DEFINE ALERTTRIGGER (Alertauslöser definieren)
- DEFINE ASSOCIATION (Clientknoten einem Zeitplan zuordnen)
- DEFINE BACKUPSET (Sicherungsgruppe definieren)
- DEFINE CLIENTACTION (Einmalige Clientaktion definieren)
- DEFINE CLIENTOPT (Option für eine Optionsgruppe definieren)
- DEFINE CLOPTSET (Clientoptionsgruppennamen definieren)
- DEFINE COLLOGROUP (Kollokationsgruppe definieren)
- DEFINE COLLOCMEMBER (Kollokationsgruppenmitglied definieren)
- DEFINE COPYGROUP (Kopiengruppe definieren)
- DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren)
- DEFINE DEVCLASS (Einheitenklasse definieren)
- DEFINE DOMAIN (Neue Maßnahmendomäne definieren)
- DEFINE DRIVE (Laufwerk für Kassettenarchiv definieren)
- DEFINE EVENTSERVER (Server als Ereignissserver definieren)
- DEFINE GRPMEMBER (Server zu einer Servergruppe hinzufügen)
- DEFINE LIBRARY (Kassettenarchiv definieren)
- DEFINE MACHINE (Maschineninformationen für die Wiederherstellung nach einem Katastrophenfall definieren)
- DEFINE MACHNODEASSOCIATION (Knoten einer Maschine zuordnen)
- DEFINE MGMTCLASS (Verwaltungsklasse definieren)
- DEFINE NODEGROUP (Knotengruppe definieren)
- DEFINE NODEGROUPMEMBER (Eintrag in der Knotengruppe definieren)
- DEFINE PATH (Pfad definieren)
- DEFINE POLICYSET (Maßnahmengruppe definieren)
- DEFINE PROFASSOCIATION (Profilzuordnung definieren)
- DEFINE PROFILE (Profil definieren)
- DEFINE RECMEDMACHASSOCIATION (Wiederh.-Datenträger Maschine zuordnen)
- DEFINE RECOVERYMEDIA (Wiederherstellungsdatenträger definieren)
- DEFINE SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl definieren)
- DEFINE SCRIPT (IBM Spectrum Protect-Prozedur definieren)
- DEFINE SERVER (Server für Übertragung zwischen Servern definieren)
- DEFINE SERVERGROUP (Server-Gruppe definieren)
- DEFINE SPACETRIGGER (Speicherbereichsauslöser definieren)
- DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)
- DEFINE STGRULE (Speicherregel für Speicherpools definieren)
- DEFINE STGPOOL (Speicherpool definieren)
- DEFINE STGPOOLDIRECTORY (Speicherpoolverzeichnis definieren)
- DEFINE SUBSCRIPTION (Profilsubskription definieren)
- DEFINE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs definieren)
- DEFINE VOLUME (Datenträger in einem Speicherpool definieren)

## DEFINE ALERTTRIGGER (Alertauslöser definieren)

---

Verwenden Sie diesen Befehl, um einen Alert auszulösen, wenn ein Server eine bestimmte Fehlernachricht ausgibt. Sie können eine Nachrichtennummer als Alertauslöser definieren, die Nachrichtennummer einer Kategorie zuordnen oder Administratoren angeben, die über den Alert in einer E-Mail benachrichtigt werden können.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```

      .-,-----
      v          |
>>-Define ALERTTrigger---+--Nachrichtennummer+----->
      .-CAteGory---SErver-----
>--+-----+----->
      '-CAteGory---+APplication+-'
          +-INventory---+
          +-CLient-----+
          +-DEvice-----+
          +-SErver-----+
          +-STorage-----+
          +-SYstem-----+
          '-VMclient----'
>--+-----+-----><
      |          .-,-----
      |          v          |
      '-ADmin---+-----AdministratOrname+-'

```

## Parameter

### Nachrichtennummer (Erforderlich)

Gibt die Nachrichtennummer an, die dem Alertauslöser zugeordnet werden soll. Geben Sie mehrere Nachrichtennummern durch Kommas getrennt und ohne Leerzeichen an. Nachrichtennummern haben eine maximale Länge von acht Zeichen.

### CAteGory

Gibt den Kategorietyt für den Alert an, der durch die Nachrichtentypen bestimmt wird. Der Standardwert ist SERVER.

Anmerkung: Wenn Sie die Kategorie eines Alertauslösers ändern, wird die Kategorie von vorhandenen Alerts auf dem Server nicht geändert. Neue Alerts werden mit der neuen Kategorie kategorisiert.

Geben Sie einen der folgenden Werte an:

#### APplication

Der Alert wird als Anwendungskategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Anwendungsclients (TDP) zugeordnet sind.

#### INventory

Der Alert wird als Bestandskategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die der Datenbank, der aktiven Protokolldatei oder der Archivprotokolldatei zugeordnet sind.

#### CLient

Der Alert wird als Clientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die allgemeinen Clientaktivitäten zugeordnet sind.

#### DEvice

Der Alert wird als Einheitenkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Einheitenklassen, Kassettenarchiven, Laufwerken oder Pfaden zugeordnet sind.

#### SErver

Der Alert wird als allgemeine Serverkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die allgemeinen Serveraktivitäten oder -ereignissen zugeordnet sind.

#### STorage

Der Alert wird als Speicherkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Speicherpools zugeordnet sind.

#### SYstemS

Der Alert wird als Systemclientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Systemsicherungs- und -archivierungsclients oder HSM-Clients zugeordnet sind.

#### VMclient

Der Alert wird als VM-Clientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die VM-Clients zugeordnet sind.



ADmin

Dieser optionale Parameter gibt den Namen des Administrators an, der eine E-Mail-Benachrichtigung über diesen Alert empfängt. Der Alertauslöser wird erfolgreich definiert, auch wenn keine Administratornamen angegeben werden.

## Einem Alert zwei Nachrichtennummern zuordnen

Mit dem folgenden Befehl angeben, dass zwei Nachrichtennummern einen Alert auslösen sollen:

```
define alertrigger ANR1067E,ANR1073E
```

## Einem Alert eine Nachrichtennummer zuordnen und zwei Administratoren in einer E-Mail benachrichtigen

Den folgenden Befehl ausgeben, um die Nachrichtennummern anzugeben, die einen Alert auslösen sollen und in einer E-Mail an zwei Administratoren gesendet werden sollen:

```
define alertrigger ANR1067E,ANR1073E ADmin=BILL,DJADMIN
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE ALERTTRIGGER

| Befehl   | Beschreibung   |
|--|--|
| DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)  | Entfernt eine Nachrichtennummer, die einen Alert auslösen kann.                                  |
| QUERY ALERTSTATUS (Status eines Alert abfragen)  | Zeigt Informationen zu Alerts an, die auf dem Server ausgegeben wurden.                          |
| QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)  | Zeigt Nachrichtennummern an, die einen Alert auslösen.   |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen) | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an. |
| UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)  | Aktualisiert die Attribute eines oder mehrerer Alertauslöser.                                    |
| UPDATE ALERTSTATUS (Status eines Alert aktualisieren)  | Aktualisiert den Status eines zurückgemeldeten Alert.  |

## DEFINE ASSOCIATION (Clientknoten einem Zeitplan zuordnen)

Mit diesem Befehl können ein oder mehrere Clients einem Zeitplan zugeordnet werden. Sie müssen einen Clientknoten der Maßnahmendomäne zuordnen, zu der ein Zeitplan gehört. Client-Knoten verarbeiten Operationen gemäß den Zeitplänen, die den Knoten zugeordnet sind.

Anmerkung:

1. IBM Spectrum Protect kann nicht mehrere Zeitpläne gleichzeitig für denselben Clientknoten ausführen.
2. In einem Makro kann der Server blockieren, wenn einige Befehle (z. B. REGISTER NODE und DEFINE ASSOCIATION) nicht festgeschrieben werden, sobald sie ausgegeben werden. Hinter jedem Befehl in einem Makro könnte ein Befehl COMMIT angegeben werden. Einfacher ist es jedoch, die Option -ITEMCOMMIT im Befehl DSMADMC anzugeben.

## Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Systemberechtigung
- Uneingeschränkte Maßnahmenberechtigung
- Eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne, zu der der Zeitplan gehört

## Syntax

```
>>-DEFine ASSOCIation--Domänennamen--Zeitplannamen----->>
      .-,-----
      V          |
```

## Parameter

Domänenname (Erforderlich)

Gibt den Namen der Maßnahmendomäne an, zu der der Zeitplan gehört.

Zeitplanname (Erforderlich)

Gibt den Namen des Zeitplans an, der einem oder mehreren Clients zugeordnet werden soll.

Knotenname (Erforderlich)

Gibt den Namen eines Clientknotens oder eine Liste mit Clientknoten an, der bzw. die dem angegebenen Zeitplan zugeordnet werden soll(en). Verwenden Sie Kommas, um die Einträge in der Liste voneinander zu trennen. Lassen Sie keine Leerzeichen zwischen den Einträgen und den Kommas. Es kann ein Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Der Befehl ordnet einen aufgelisteten Client dem Zeitplan nicht zu, wenn:

- Der Client bereits dem angegebenen Zeitplan zugeordnet wurde.
- Der Client nicht der Maßnahmendomäne zugeordnet ist, zu der der Zeitplan gehört.
- Der Client ein NAS-Knotenname ist. Alle NAS-Knoten werden ignoriert.

## Beispiel: Clientknoten einem Zeitplan zuordnen

Die Clientknoten SMITH und JOHN dem Zeitplan WEEKLY\_BACKUP zuordnen. Die zugeordneten Clients sind der Maßnahmendomäne EMPLOYEE\_RECORDS zugeordnet.

```
define association employee_records  
weekly_backup smith*,john*
```

## Beispiel: Clientknoten einem Zeitplan zuordnen

Die Clientknoten JOE, TOM und LARRY dem Zeitplan WINTER zuordnen. Die zugeordneten Clients sind der Maßnahmendomäne EMPLOYEE\_RECORDS zugeordnet; der Client JOE ist jedoch bereits dem Zeitplan WINTER zugeordnet.

```
define association employee_records  
winter joe,tom,larry
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE ASSOCIATION

| Befehl             | Beschreibung  |
|--------------------|---|
| DEFINE SCHEDULE    | Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl.         |
| DELETE ASSOCIATION | Löscht die Zuordnung zwischen Clients und einem Zeitplan.                               |
| DELETE SCHEDULE    | Löscht einen Zeitplan aus der Datenbank.  |
| QUERY ASSOCIATION  | Zeigt die Clients an, die einem oder mehreren Zeitplänen zugeordnet sind.               |
| REGISTER NODE      | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest. |

## DEFINE BACKUPSET (Sicherungsgruppe definieren)

Mit diesem Befehl kann eine Clientsicherungsgruppe definiert werden, die zuvor auf einem Server generiert wurde, und die Sicherungsgruppe für den Server verfügbar gemacht werden, auf dem dieser Befehl ausgeführt wird. Der Clientknoten hat die Option, die Sicherungsgruppe von dem Server zurückzuschreiben, der diesen Befehl ausführt, und nicht von dem Server, auf dem die Sicherungsgruppe generiert wurde.

Jede Sicherungsgruppe, die auf einem Server generiert wurde, kann für einen anderen Server definiert werden, wenn die Server einen Einheitentyp gemeinsam benutzen. Die Stufe des Servers, für die die Sicherungsgruppe definiert wird, muss mindestens so hoch sein wie die Stufe des Servers, der die Sicherungsgruppe generiert hat.

Der Befehl DEFINE BACKUPSET kann auch verwendet werden, um eine Sicherungsgruppe erneut zu definieren, die auf einem Server gelöscht wurde.

## Berechtigungsklasse

Wird die Serveroption REQSYSAUTHOUTFILE auf YES (Standardwert) gesetzt, muss der Administrator die Systemberechtigung haben. Ist die Serveroption REQSYSAUTHOUTFILE auf NO gesetzt, muss der Administrator über Systemberechtigung oder Maßnahmenberechtigung für die Domäne verfügen, der der Clientknoten zugeordnet ist.

## Syntax

```

      .-,-----
      v          |
>>-DEFine BACKUPSET-----+--Knotenname-----+----->
      '-Knotengruppenname-'

>--Präfix_des_Sicherungsgruppennamens----->

>--DEVclass-----Einheitenklassenname----->

      .-,-----
      v          |
>>-VOLumes-----Datenträgernamen----->

      .-RETention-----365-----
>+-----+----->
      '-RETention-----+Tage-----+'
      '-NOLimit-'

>+-----+----->
      '-DESCRiption-----Beschreibung-'

      .-WHEREDATAType-----ALL-----
>+-----+----->
      |          .-,-----
      |          v          | |
      |'-WHEREDATAType-----+FILE-----+'
      |          '-IMAGE-'

>+-----+----->
      '-TOC-----+PREFERRED+-'
      '+-YES-----+'
      '-NO-----+'

>+-----+-----><
      '-TOCMgmtclass-----Klassenname-'

```

## Parameter

### Knotenname oder Knotengruppenname (Erforderlich)

Gibt den Namen der Clientknoten oder Knotengruppen an, deren Daten in den angegebenen Sicherungsgruppenträgern enthalten sind. Sollen mehrere Knoten- und Knotengruppenamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Knotennamen können Platzhalterzeichen enthalten, Knotengruppenamen dagegen nicht. Wenn die Sicherungsgruppenträger Sicherungsgruppen von mehreren Knoten enthalten, wird jede Sicherungsgruppe, deren Knotenname mit einem der angegebenen Knotennamen übereinstimmt, definiert. Enthalten die Datenträger eine Sicherungsgruppe für einen Knoten, der gegenwärtig nicht registriert ist, wird mit dem Befehl DEFINE BACKUPSET die Sicherungsgruppe für diesen Knoten nicht definiert.

### Präfix\_des\_Sicherungsgruppennamens (Erforderlich)

Gibt den Namen der Sicherungsgruppe an, die für diesen Server definiert werden soll. Die maximale Länge des Namens beträgt 30 Zeichen.

Wird ein Name ausgewählt, fügt IBM Spectrum Protect ein Suffix hinzu, um den Sicherungsgruppennamen zu erstellen. Wird die Sicherungsgruppe beispielsweise *mybackupset* genannt, fügt IBM Spectrum Protect eine eindeutige Zahl wie beispielsweise 3099 zum Namen hinzu. Der Sicherungsgruppennamen wird dann als *mybackupset.3099* identifiziert. Sollen später Informationen über diese Sicherungsgruppe angezeigt werden, kann in den Namen ein Platzhalterzeichen wie beispielsweise *mybackupset\** eingefügt oder der vollständig qualifizierte Name wie beispielsweise *mybackupset.3099* angegeben werden.

Enthalten die Sicherungsgruppenträger Sicherungsgruppen für mehrere Knoten, werden Sicherungsgruppen für jeden der Knoten unter Verwendung desselben Präfix und Suffix des Sicherungsgruppennamens definiert.

### DEVclass (Erforderlich)

Gibt den Namen der Einheitenklasse für die Datenträger an, von denen die Sicherungsgruppe gelesen wird.

Anmerkung: Der Einheitentyp, der der angegebenen Einheitenklasse zugeordnet ist, muss mit der Einheitenklasse übereinstimmen, mit der die Sicherungsgruppe ursprünglich generiert wurde.

#### VOLumes (Erforderlich)

Gibt die Namen der Datenträger an, die zum Speichern der Sicherungsgruppe verwendet werden. Es können mehrere Datenträger angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Die angegebenen Datenträger müssen für den Server verfügbar sein, der die Sicherungsgruppe definiert.

Anmerkung: Die angegebenen Datenträger müssen in der Reihenfolge ihrer Erstellung aufgelistet sein; andernfalls schlägt der Befehl DEFINE BACKUPSET fehl.

Der Server prüft nicht, ob jeder Datenträger, der für eine Sicherungsgruppe mit mehreren Datenträgern angegeben ist, einen Teil der Sicherungsgruppe enthält. Der erste Datenträger wird immer überprüft, und in einigen Fällen werden auch zusätzliche Datenträger überprüft. Sind diese Datenträger korrekt, wird die Sicherungsgruppe definiert, und es werden alle im Befehl aufgelisteten Datenträger vor dem Überschreiben geschützt. Ist ein Datenträger, der einen Teil der Sicherungsgruppe enthält, nicht in dem Befehl aufgelistet, wird der Datenträger nicht geschützt und kann während der normalen Serveroperationen überschrieben werden.

Anmerkung: Standardmäßig versucht der Server, ein Inhaltsverzeichnis zu erstellen, wenn eine Sicherungsgruppe definiert wird. Wird ein falscher Datenträger angegeben oder sind Datenträger nicht in der korrekten Reihenfolge aufgelistet, schlägt die Erstellung des Inhaltsverzeichnisses fehl. Tritt dieser Fehler auf, überprüfen Sie die Datenträgerliste in dem Befehl und ziehen Sie die Verwendung des Befehls QUERY BACKUPSETCONTENTS in Betracht, um den Inhalt der Sicherungsgruppe zu prüfen.

#### RETention

Gibt die Anzahl Tage an, die die Sicherungsgruppe auf dem Server aufbewahrt wird. Sie können eine ganze Zahl von 0 bis 30000 angeben. Der Standardwert ist 365 Tage. Gültige Werte:

##### Tage

Gibt die Anzahl der Tage an, die die Sicherungsgruppe auf dem Server aufbewahrt werden soll.

##### NOLimit

Gibt an, dass die Sicherungsgruppe auf dem Server unbegrenzt aufbewahrt werden muss.

Wird NOLIMIT angegeben, werden die Datenträger mit der Sicherungsgruppe von IBM Spectrum Protect unbegrenzt aufbewahrt, es sei denn, ein Benutzer oder Administrator löscht die Datenträger aus dem Serverspeicher.

#### DESCription

Gibt die Beschreibung an, die der Sicherungsgruppe zugeordnet werden soll, die zu dem Client-Knoten gehört. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

#### WHEREDATAType

Gibt an, dass die Sicherungsgruppen mit den angegebenen Typen von Daten definiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert gibt an, dass Sicherungsgruppen für alle Typen von Daten (Dateiebene, Image und Anwendung) definiert werden sollen. Bei der Angabe mehrerer Datentypen müssen die Datentypen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Gültige Werte:

##### ALL

Gibt an, dass Sicherungsgruppen für alle Typen von Daten (Dateiebene, Image und Anwendung) definiert werden sollen. ALL ist der Standardwert.

##### FILE

Gibt an, dass eine Sicherungsgruppe auf Dateiebene definiert werden soll. Sicherungsgruppen auf Dateiebene enthalten Dateien und Verzeichnisse, die vom Sicherungsclient gesichert werden.

##### IMAGE

Gibt an, dass eine Imagesicherungsgruppe definiert werden soll. Imagesicherungsgruppen enthalten Images, die mit dem Befehl BACKUP IMAGE des Clients für Sichern/Archivieren erstellt wurden.

#### TOC

Gibt an, ob ein Inhaltsverzeichnis (Table of contents - TOC) für die Sicherungsgruppe auf Dateiebene erstellt werden muss, wenn sie definiert wird. Der Parameter TOC wird ignoriert, wenn Image- und Anwendungssicherungsgruppen definiert werden, da für diese Sicherungsgruppen immer ein Inhaltsverzeichnis erstellt wird.

Sie sollten bei der Festlegung, ob ein Inhaltsverzeichnis erstellt werden soll, Folgendes berücksichtigen:

- Wird ein Inhaltsverzeichnis erstellt, können Sie den IBM Spectrum Protect-Webclient für Sichern/Archivieren verwenden, um die gesamte Dateisystemstruktur zu untersuchen und Dateien und Verzeichnisse zum Zurückschreiben auszuwählen. Für die Erstellung eines Inhaltsverzeichnisses müssen Sie das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die Verwaltungsklasse definieren, die mit dem Parameter TOCMGMTCLASS angegeben wird. Die Erstellung eines Inhaltsverzeichnisses erfordert zusätzliche Verarbeitung, zusätzlichen Speicherpoolbereich und möglicherweise einen Mountpunkt während der Sicherungsgruppenoperation.
- Wird ein Inhaltsverzeichnis für eine Sicherungsgruppe nicht gesichert, können Sie dennoch einzelne Dateien oder Verzeichnisstrukturen mit dem Befehl RESTORE BACKUPSET des Clients für Sichern/Archivieren zurückschreiben, wenn Sie den vollständig qualifizierten Namen jeder Datei oder jedes Verzeichnisses kennen, die bzw. das zurückgeschrieben werden soll.

Dieser Parameter ist wahlfrei. Der Standardwert ist Preferred. Gültige Werte:

No

Gibt an, dass keine Inhaltsverzeichnisinformationen für Sicherungsgruppen auf Dateiebene gesichert werden.

Preferred

Gibt an, dass Inhaltsverzeichnisinformationen für Sicherungsgruppen auf Dateiebene gesichert werden müssen. Eine Sicherungsgruppe ist jedoch nicht fehlerhaft, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt.

Yes

Gibt an, dass Inhaltsverzeichnisinformationen für jede Sicherungsgruppe auf Dateiebene gesichert werden müssen. Eine Sicherungsgruppe ist fehlerhaft, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt.

TOCMgmtclass

Gibt den Namen der Verwaltungsklasse an, an die das Inhaltsverzeichnis gebunden werden muss. Wird keine Verwaltungsklasse angegeben, wird das Inhaltsverzeichnis an die Standardverwaltungsklasse für die Maßnahmendomäne gebunden, der der Knoten zugeordnet ist. In diesem Fall müssen Sie für die Erstellung des Inhaltsverzeichnisses das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die angegebene Verwaltungsklasse definieren.

## Beispiel: Eine Sicherungsgruppe definieren

Die Sicherungsgruppe PERS\_DATA, die zum Clientknoten JANE gehört, für den Server definieren, der diesen Befehl ausführt. Die Sicherungsgruppe auf dem Server 50 Tage aufbewahren. Angeben, dass die Datenträger VOL001 und VOL002 die Daten für die Sicherungsgruppe enthalten. Die Datenträger sollen von einer Einheit gelesen werden, die der Einheitenklasse AGADM zugeordnet ist. Eine Beschreibung einschließen.

```
define backupset jane pers_data devclass=agadm
volumes=voll,vol2 retention=50
description="Basisimage Sektor 7"
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE BACKUPSET

| Befehl                  | Beschreibung  |
|-------------------------|---|
| DEFINE NODEGROUP        | Definiert eine Gruppe von Knoten.   |
| DEFINE NODEGROUPMEMBER  | Fügt einer Knotengruppe einen Clientknoten hinzu.                           |
| DELETE NODEGROUP        | Löscht eine Knotengruppe.   |
| DELETE BACKUPSET        | Löscht eine Sicherungsgruppe.   |
| DELETE NODEGROUPMEMBER  | Löscht einen Clientknoten aus einer Knotengruppe.                           |
| GENERATE BACKUPSET      | Generiert eine Sicherungsgruppe mit den Daten eines Clients.                |
| GENERATE BACKUPSETTOC   | Generiert ein Inhaltsverzeichnis für eine Sicherungsgruppe.                 |
| QUERY BACKUPSET         | Zeigt Sicherungsgruppen an.   |
| QUERY BACKUPSETCONTENTS | Zeigt den Inhalt in Sicherungsgruppen an.                                   |
| QUERY NODEGROUP         | Zeigt Informationen zu Knotengruppen an.                                    |
| UPDATE BACKUPSET        | Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum. |
| UPDATE NODEGROUP        | Aktualisiert die Beschreibung einer Knotengruppe.                           |

## DEFINE CLIENTACTION (Einmalige Clientaktion definieren)

Mit diesem Befehl können ein oder mehrere Clients für die Verarbeitung eines Befehls für eine einmalige Aktion geplant werden.

Der Server definiert automatisch einen Zeitplan und ordnet dem Zeitplan den Clientknoten zu. Der Server ordnet dem Zeitplan Priorität 1 zu, setzt PERUNITS auf ONETIME und bestimmt die Anzahl der Tage, die der Zeitplan aktiv bleiben soll. Die Anzahl der Tage basiert auf dem Wert, der mit dem Befehl SET CLIENTACTDURATION definiert wird.

Wie schnell der Client diesen Befehl verarbeitet, ist davon abhängig, ob der Planungsmodus für den Client auf Serversystemanfrage (server-prompted) oder auf Clientsendeaufruf (client-polling) gesetzt ist. Der Client-Scheduler muss auf der Clientdatenstation gestartet werden, damit der Server den Zeitplan verarbeiten kann.



Gibt an, daß der Zeitplan alle Dateien sichert, die neu sind oder sich seit der letzten Teilsicherung geändert haben. Mit "Incremental" werden auch alle Dateien gesichert, für die alle vorhandenen Sicherungen möglicherweise verfallen sind.

#### Selective

Gibt an, daß der Zeitplan nur Dateien sichert, die mit dem Parameter OBJECTS angegeben werden.

#### Archive

Gibt an, daß der Zeitplan Dateien archiviert, die mit dem Parameter OBJECTS angegeben werden.

#### Backup

Gibt an, dass der Zeitplan Dateien sichert, die mit dem Parameter OBJECTS angegeben werden.

#### REStore

Gibt an, daß der Zeitplan Dateien zurückschreibt, die mit dem Parameter OBJECTS angegeben werden.

Wenn Sie ACTION=RESTORE für eine geplante Operation angeben, und ist die Option REPLACE auf PROMPT gesetzt, erfolgt keine Aufforderung. Wird die Option auf PROMPT gesetzt, werden die Dateien übersprungen.

Wenn Sie eine zweite Dateispezifikation angeben, agiert diese zweite Dateispezifikation als Zielort für die Zurückschreibung. Müssen mehrere Gruppen von Dateien zurückgeschrieben werden, planen Sie eine für jede Dateispezifikation, die zurückgeschrieben werden muss.

#### RETRieve

Gibt an, dass der Zeitplan Dateien abrufen, die mit dem Parameter OBJECTS angegeben werden.

Hinweis: Eine zweite Datei, die angegeben wird, dient als Abrufzielort. Müssen mehrere Gruppen von Dateien abgerufen werden, erstellen Sie einen separaten Zeitplan für jede Dateigruppe.

#### IMAGEBACKup

Gibt an, daß der Zeitplan logische Datenträger sichert, die mit dem Parameter OBJECTS angegeben werden.

#### IMAGERESTore

Gibt an, daß der Zeitplan logische Datenträger zurückschreibt, die mit dem Parameter OBJECTS angegeben werden.

#### Command

Gibt an, dass der Zeitplan einen Client-Betriebssystembefehl oder ein Script verarbeitet, der bzw. das mit dem Parameter OBJECTS angegeben wird.

#### Macro

Gibt an, daß ein Client ein Makro verarbeitet, dessen Dateiname im Parameter OBJECTS angegeben ist.

#### SUBACTion

Sie können einen der folgenden Werte angeben:

""

Wenn eine Nullzeichenfolge (zwei Anführungszeichen) mit ACTION=BACKUP angegeben wird, ist die Sicherung eine Teilsicherung.

#### FASTBBack

Gibt an, dass eine FastBack-Clientoperation, die durch den Parameter ACTION angegeben wird, für die Verarbeitung geplant werden soll. Der Wert des Parameters ACTION muss ARCHIVE oder BACKUP sein.

#### SYSTEMState

Gibt an, dass eine Clientsystemstatussicherung geplant ist.

#### VApp

Gibt an, dass eine vApp-Clientsicherung geplant ist. Eine vApp ist eine Sammlung von vorimplementierten virtuellen Maschinen.

#### VM


Gibt an, dass eine VMware-Clientsicherungsoperation geplant ist.

#### OPTions

Gibt die Clientoptionen an, die für den geplanten Befehl angegeben werden, wenn der Zeitplan verarbeitet wird. Dieser Parameter ist wahlfrei.

Für diesen Parameter können nur die Optionen angegeben werden, die für den geplanten Befehl gültig sind. Informationen zu den Optionen, die in der Befehlszeile gültig sind, befinden sich im entsprechenden Clienthandbuch. Alle Optionen, für die im Clienthandbuch angegeben ist, dass sie nur in der Anfangsbefehlszeile gültig sind, führen zu einem Fehler oder werden ignoriert, wenn der Zeitplan vom Server ausgeführt wird. Geben Sie beispielsweise die folgenden Optionen nicht an, da sie keinen Einfluss darauf haben, wann der Client den geplanten Befehl verarbeitet:

- MAXCMDRETRIES
- OPTFILE
- QUERYSCHEDPERIOD
- RETRYPERIOD
- SCHEDLOGNAME
- SCHEDMODE
- SERVERNAME
- TCPCLIENTADDRESS
- TCPCLIENTPORT

 Windows-Betriebssysteme Wenn Sie einen Scheduler-Service definieren, indem Sie den Befehl DSMCUTIL oder den Assistenten für die GUI des Clients für Sichern/Archivieren verwenden, geben Sie eine Optionsdatei an. Sie können die Optionen in dieser Optionsdatei nicht überschreiben, indem Sie den geplanten Befehl ausgeben. Sie müssen die Optionen in Ihrem Schedulerservice ändern.

Enthält die Optionszeichenfolge mehrere Optionen oder Optionen mit eingebetteten Leerzeichen, schließen Sie die gesamte Optionszeichenfolge in Hochkommas ein. Schließen Sie einzelne Optionen, die Leerzeichen enthalten, in Anführungszeichen ein. Vor der Option muss ein führendes Minuszeichen stehen. Fehler können auftreten, wenn die Optionszeichenfolge Leerzeichen enthält, die nicht korrekt in Anführungszeichen eingeschlossen sind.

Die folgenden Beispiele zeigen, wie einige Clientoptionen angegeben werden:

- Geben Sie Folgendes ein, um `subdir=yes` und `domain all-local -systemobject` anzugeben:
  - `options='-subdir=yes -domain="all-local -c: -systemobject"'`
- Geben Sie Folgendes ein, um `domain all-local -c: -d:` anzugeben:
  - `options='-domain="all-local -c: -d:"'`

 Windows-Betriebssysteme Tipp:

Für Windows-Clients, die im Stapelbetrieb ausgeführt werden: Ist die Verwendung von Anführungszeichen erforderlich, verwenden Sie den Dialogmodus oder Escapezeichen des Betriebssystems. Weitere Informationen liefern die folgenden Abschnitte:

- Eine Serie von Befehlen des Verwaltungsclients verarbeiten
- Einzelne Befehle mit dem Verwaltungsclient verarbeiten

## OBjects

Gibt die Objekte an, für die die angegebene Aktion ausgeführt wird. Verwenden Sie ein einzelnes Leerzeichen zwischen jedem Objekt. Außer bei `ACTION=INCREMENTAL` ist dieser Parameter erforderlich. Ist die Aktion eine Sicherungs-, Archivierungs-, Abruf- oder Zurückschreibungsoperation, sind die Objekte Dateibereiche, Verzeichnisse oder logische Datenträger. Dient die Aktion zur Ausführung eines Befehls oder Makros, ist das Objekt der Name des auszuführenden Befehls oder Makros.

Wenn `ACTION=INCREMENTAL` ohne Angabe eines Werts für diesen Parameter angegeben wird, wird der geplante Befehl ohne angegebene Objekte aufgerufen, und der Befehl versucht, die Objekte wie in der Clientoptionsdatei definiert zu verarbeiten. Um alle Dateibereiche oder Verzeichnisse für eine Aktion auszuwählen, müssen sie explizit in der Objektzeichenfolge aufgeführt werden. Wird nur ein Stern in die Objektzeichenfolge eingegeben, erfolgt die Sicherung nur für das Verzeichnis, bei dem der Scheduler gestartet wurde.

Wichtig:

- Wenn Sie eine zweite Dateispezifikation angeben, und handelt es sich nicht um einen gültigen Zielort, empfangen Sie diesen Fehler:


```
ANS1082E Ungültige
Zieldateispezifikation <Dateispezifikation> eingegeben.
```

- Geben Sie mehr als zwei Dateispezifikationen an, empfangen Sie diesen Fehler:


```
ANS1102E Zu viele Befehlszeilenparameter an das Programm übergeben!
```

Wird für diesen Parameter `ACTION=ARCHIVE, INCREMENTAL` oder `SELECTIVE` angegeben, können Sie maximal 20 Dateispezifikationen auflisten.

Schließen Sie die Objektzeichenfolge in Anführungszeichen ein, wenn sie Leerzeichen enthält, und schließen Sie dann die Anführungszeichen in Hochkommas ein. Enthält die Objektzeichenfolge mehrere Dateinamen, schließen Sie jeden Dateinamen in Anführungszeichen ein und schließen Sie dann die gesamte Zeichenfolge in Hochkommas ein. Fehler können auftreten, wenn Dateinamen ein Leerzeichen enthalten, das nicht korrekt in Anführungszeichen eingeschlossen ist.

 Windows-Betriebssysteme Wenn Sie Zeichen verwenden, die für Windows-Benutzer eine besondere Bedeutung haben, wie z. B. Kommas, schließen Sie das gesamte Argument in doppelte Anführungszeichen ein und schließen Sie dann die gesamte Zeichenfolge in Hochkommas ein. Die folgenden Beispiele zeigen, wie einige Dateinamen angegeben werden:

- Geben Sie Folgendes ein, um `C:\FILE 2, D:\GIF FILES` und `E:\MY TEST FILE` anzugeben:
  - `OBJECTS="\"C:\FILE 2" \"D:\GIF FILES" \"E:\MY TEST FILE"'`
- Geben Sie Folgendes ein, um `D:\TEST FILE` anzugeben:
  - `OBJECTS="\"D:\TEST FILE"'`
- Geben Sie Folgendes ein, um `D:TEST,FILE` anzugeben:
  - `OBJECTS="\"D:\TEST,FILE"'`

 AIX-Betriebssysteme  Linux-Betriebssysteme Die folgenden Beispiele zeigen, wie einige Dateinamen angegeben werden:



- Geben Sie Folgendes ein, um /home/file 2, /home/gif files und /home/my test file anzugeben:
  - OBJECTS="/home/file 2" "/home/gif files" "/home/my test file"
- Geben Sie Folgendes ein, um /home/test file anzugeben:
  - OBJECTS="/home/test file"



Für Windows-Clients, die im Stapelbetrieb ausgeführt werden: Ist die Verwendung von Anführungszeichen erforderlich, verwenden Sie den Dialogmodus oder Escapezeichen des Betriebssystems. Weitere Informationen liefern die folgenden Abschnitte:

- Eine Serie von Befehlen des Verwaltungsclients verarbeiten
- Einzelne Befehle mit dem Verwaltungsclient verarbeiten

#### Wait

Gibt an, ob auf die Beendigung einer geplanten Clientoperation gewartet werden soll. Dieser Parameter ist nützlich, wenn Clientaktionen aus einer Befehlsprozedur oder einem Makro definiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

#### No

Gibt an, dass nicht auf die Beendigung der geplanten Clientoperation gewartet wird. Wird dieser Wert angegeben und hat der Parameter ACTION den Wert COMMAND, gibt der Rückkehrcode an, ob die Clientaktion definiert wurde.

#### Yes

Gibt an, dass auf die Beendigung der geplanten Clientoperation gewartet wird. Wird dieser Wert angegeben und hat der Parameter ACTION den Wert COMMAND, gibt der Rückkehrcode den Status der Clientoperation an.

Der Befehl DEFINE CLIENTACTION mit WAIT=YES kann nicht von der Serverkonsole ausgegeben werden. Der Administrator kann jedoch von der Serverkonsole:

- WAIT=YES mit DEFINE CLIENTACTION als Befehlszeile eines Befehls DEFINE SCRIPT angeben.
- WAIT=YES mit DEFINE CLIENTACTION als Befehlszeile einer Datei angeben, deren Inhalt in die Prozedur eingelesen wird, die durch einen Befehl DEFINE SCRIPT definiert wird.

Einschränkung: Wird der Befehl DEFINE CLIENTACTION mit WAIT=YES in einem Makro angegeben, werden die mit dem Befehl definierten sofortigen Zeitpläne nicht zurückgesetzt, wenn das Makro nicht erfolgreich ausgeführt wird.

## Beispiel: Eine einmalige Teilsicherung ausführen

Einen Teilsicherungsbefehl für Clientknoten TOM ausgeben, der der Maßnahmendomäne EMPLOYEE\_RECORDS zugeordnet ist. IBM Spectrum Protect definiert einen Zeitplan und ordnet ihn dem Clientknoten TOM zu (vorausgesetzt, der Client-Scheduler ist aktiv).

```
define clientaction tom domain=employee_records
action=incremental
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE CLIENTACTION

| Befehl                | Beschreibung  |
|-----------------------|---|
| DELETE SCHEDULE       | Löscht einen Zeitplan aus der Datenbank.  |
| QUERY ASSOCIATION     | Zeigt die Clients an, die einem oder mehreren Zeitplänen zugeordnet sind.                   |
| QUERY EVENT           | Zeigt Informationen über geplante und abgeschlossene Ereignisse für ausgewählte Clients an. |
| QUERY SCHEDULE        | Zeigt Informationen über Zeitpläne an.  |
| SET CLIENTACTDURATION | Gibt die Dauer eines mit dem Befehl DEFINE CLIENTACTION definierten Zeitplans an.           |

## DEFINE CLIENTOPT (Option für eine Optionsgruppe definieren)

Mit diesem Befehl kann eine Clientoption einer Optionsgruppe hinzugefügt werden.

## Berechtigungsklasse



Dateispezifikation in Hochkommas und die gesamte Option in Anführungszeichen ein.

```
define clientopt winspec inclexcl "exclude.dir '*:\..\Temporary  
Internet Files'"
```

## Beispiel: Eine Option hinzufügen, um Dateien in angegebenen Verzeichnissen zu binden

Clientoptionen zur Optionsgruppe WINSPEC hinzufügen, um alle Dateien in den Verzeichnissen C:\Data und C:\Program Files\My Apps an die Verwaltungsklasse PRODCLASS zu binden.

```
define clientopt winspec inclexcl "include C:\Data\..\* prodclass"  
define clientopt winspec inclexcl "include 'C:\Program  
Files\My Apps\..\*' prodclass"
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE CLIENTOPT

| Befehl           | Beschreibung  |
|------------------|---|
| COPY CLOPTSET    | Kopiert eine Clientoptionsgruppe.   |
| DEFINE CLOPTSET  | Definiert eine Clientoptionsgruppe.   |
| DELETE CLIENTOPT | Löscht eine Clientoption aus einer Clientoptionsgruppe.                                 |
| DELETE CLOPTSET  | Löscht eine Clientoptionsgruppe.  |
| REGISTER NODE    | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest. |
| QUERY CLOPTSET   | Zeigt Informationen über eine Clientoptionsgruppe an.                                   |
| UPDATE CLIENTOPT | Aktualisiert die Folgenummer einer Clientoption in einer Clientoptionsgruppe.           |
| UPDATE CLOPTSET  | Aktualisiert die Beschreibung einer Clientoptionsgruppe.                                |
| UPDATE NODE      | Ändert die Attribute, die einem Clientknoten zugeordnet sind.                           |

## DEFINE CLOPTSET (Clientoptionsgruppenamen definieren)

Mit diesem Befehl kann ein Name für eine Gruppe von Optionen definiert werden, die den Clients für Archivierungs-, Sicherungs-, Zurückschreibungs- und Abrufoperationen zugeordnet werden können.

Sollen Optionen der neuen Gruppe hinzugefügt werden, den Befehl DEFINE CLIENTOPT ausgeben.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

## Syntax

```
>>-DEFine CLOptset--Optionsgruppenname----->  
>--+-----+-----><  
  '-DESCRiption----Beschreibung-'
```

## Parameter

Optionsgruppenname (Erforderlich)

Gibt den Namen der Clientoptionsgruppe an. Die maximale Länge des Namens beträgt 64 Zeichen.

DESCRiption

Gibt eine Beschreibung der Clientoptionsgruppe an. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Dieser Parameter ist wahlfrei.

## Beispiel: Eine Clientoptionsgruppe definieren

Um eine Clientoptionsgruppe mit dem Namen ENG zu definieren, den folgenden Befehl ausgeben:

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE CLOPTSET

| Befehl           | Beschreibung  |
|------------------|---|
| COPY CLOPTSET    | Kopiert eine Clientoptionsgruppe.   |
| DEFINE CLIENTOPT | Fügt einer Clientoptionsgruppe eine Clientoption hinzu.                       |
| DELETE CLIENTOPT | Löscht eine Clientoption aus einer Clientoptionsgruppe.                       |
| DELETE CLOPTSET  | Löscht eine Clientoptionsgruppe.  |
| QUERY CLOPTSET   | Zeigt Informationen über eine Clientoptionsgruppe an.                         |
| UPDATE CLIENTOPT | Aktualisiert die Folgenummer einer Clientoption in einer Clientoptionsgruppe. |
| UPDATE CLOPTSET  | Aktualisiert die Beschreibung einer Clientoptionsgruppe.                      |

## DEFINE COLLOGROUP (Kollokationsgruppe definieren)

Verwenden Sie diesen Befehl, um eine Kollokationsgruppe zu definieren. Eine *Kollokationsgruppe* ist eine Gruppe von Knoten oder Dateibereichen auf einem Knoten, deren Daten auf eine minimale Anzahl Datenträger mit sequenziellem Zugriff durch Kollokation zusammengefasst werden. Ihre Daten werden nur zusammengefasst, wenn in der Speicherpooldefinition die Kollokation nach Gruppe (COLLOCATE=GROUP) angegeben ist.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-DEFine COLLOCGroup--Gruppenname----->
>--+-----+-----><
  '-DESCription-----Beschreibung-'
```

### Parameter

#### Gruppenname

Gibt den Namen der Kollokationsgruppe an, die erstellt werden soll. Die maximale Länge des Namens beträgt 30 Zeichen.

#### DESCription

Gibt eine Beschreibung der Kollokationsgruppe an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

## Kollokationsgruppe definieren

Um eine Knoten- oder Dateibereichskollokationsgruppe mit dem Namen GROUP1 zu definieren, geben Sie den folgenden Befehl aus:

```
define collogroup group1
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE COLLOGROUP

| Befehl              | Beschreibung   |
|---------------------|--|
| DEFINE COLLOCMEMBER | Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.          |
| DEFINE STGPOOL      | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern. |
| DELETE COLLOGROUP   | Löscht eine Kollokationsgruppe.  |

| Befehl              | Beschreibung  |
|---------------------|---|
| DELETE COLLOCMEMBER | Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.                                     |
| MOVE NODEDATA       | Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen. |
| QUERY COLLOGROUP    | Zeigt Informationen zu Kollokationsgruppen an.  |
| QUERY NODE          | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.                             |
| QUERY NODEDATA      | Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.                               |
| QUERY STGPOOL       | Zeigt Informationen zu Speicherpools an.  |
| REMOVE NODE         | Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.              |
| UPDATE COLLOGROUP   | Aktualisiert die Beschreibung einer Kollokationsgruppe.   |
| UPDATE STGPOOL      | Ändert die Attribute eines Speicherpools.   |

## DEFINE COLLOCMEMBER (Kollokationsgruppenmitglied definieren)

Geben Sie diesen Befehl aus, um einen Clientknoten zu einer Kollokationsgruppe oder einen Dateibereich auf einem Knoten zu einer Kollokationsgruppe hinzuzufügen. Eine Kollokationsgruppe ist eine Gruppe von Knoten oder Dateibereichen auf einem Knoten, deren Daten auf eine minimale Anzahl Datenträger mit sequenziellem Zugriff durch Kollokation zusammengefasst werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

Knoten zu einer Kollokationsgruppe hinzufügen

```

      .-,------.
      v             |
>>-DEfine COLLOCMember--Gruppenname---Knotenname+-----<<

```

### Parameter

#### Gruppenname

Gibt den Namen der Kollokationsgruppe an, der ein Clientknoten hinzugefügt werden soll.

#### Knotenname

Gibt den Namen des Clientknotens an, der zur Kollokationsgruppe hinzugefügt werden soll. Sie können einen oder mehrere Namen angeben. Mehrere Namen sind durch Kommas voneinander zu trennen; verwenden Sie keine Leerzeichen zwischen den Namen. Sie können auch Platzhalterzeichen verwenden, um mehrere Namen anzugeben.

Dateibereich auf einem Knoten zu einer Kollokationsgruppe hinzufügen

```

>>-DEfine COLLOCMember--Gruppenname--Knotenname----->
      .-,------.
      v             |
>>-Filespace-----Dateibereichsname+----->
      .-NAMEType----SERVER----- .
>+-----+-----+-----+----->
  '-NAMEType----+-SERVER--+-'
      +-UNICODE+
      '-FSID----'
      .-CODEType----BOTH----- .
>+-----+-----+-----+-----<
  '-CODEType----+-BOTH-----+-'

```

+--UNICODE----+  
'-NONUNICODE-'

## Parameter

---

### Gruppenname

Gibt den Namen der Kollokationsgruppe an, der ein Dateibereich hinzugefügt werden soll.

### Knotenname

Gibt den Clientknoten an, auf dem sich der Dateibereich befindet.

### Filespace

Gibt den *Dateibereichsnamen* auf dem Clientknoten an, der der Kollokationsgruppe hinzugefügt werden soll. Sie können einen oder mehrere Dateibereichsnamen angeben, die sich auf einem bestimmten Clientknoten befinden. Wenn Sie mehrere Dateibereichsnamen angeben, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Sie können auch Platzhalterzeichen verwenden, um mehrere Dateibereichsnamen anzugeben. Beispiel:

```
define collocmember manufacturing linux237 filespace=*_linux_fs
```

Mit diesem Befehl werden alle Dateibereiche auf dem Knoten linux237 mit einem Namen, der mit `_linux_fs` endet, zur Kollokationsgruppe `manufacturing` hinzugefügt.

Die folgende Liste enthält Tipps zum Arbeiten mit Kollokationsgruppen:

- Wenn Sie einer neuen Kollokationsgruppe Mitglieder hinzufügen, bestimmt der Typ des ersten Kollokationsgruppenmitglieds den Typ der Kollokationsgruppe. Die Gruppe kann entweder eine Knotenkollokationsgruppe oder eine Dateibereichskollokationsgruppe sein.  
Einschränkung: Nachdem der Typ der Kollokationsgruppe definiert wurde, kann er nicht geändert werden.
- Typen von Kollokationsgruppenmitgliedern können nicht gemischt werden, wenn Sie einer Kollokationsgruppe (Knotengruppe oder Dateibereichsgruppe) Mitglieder hinzufügen.
- Für eine Dateibereichskollokationsgruppe können Sie Dateibereiche zur Gruppe hinzufügen. Die Dateibereiche müssen denselben Wert wie der Parameter *Knotenname* verwenden, der bei der Erstellung der Kollokationsgruppe angegeben wird.
- Ein Clientknoten kann in mehrere Dateibereichsgruppen eingeschlossen werden. Ist jedoch ein Knoten ein Mitglied einer Knotenkollokationsgruppe, kann er nicht ein Mitglied einer Dateibereichskollokationsgruppe sein.
- Ein Dateibereich kann nur ein Mitglied einer Dateibereichsgruppe sein.

### NAMETYPE

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Geben Sie diesen Parameter an, wenn der Server mit Clients kommuniziert, die über Unicode-Unterstützung verfügen. Ein Client für Sichern/Archivieren mit Unicode-Unterstützung ist nur für Windows-, Macintosh OS 9-, Macintosh OS X- und NetWare-Systeme verfügbar. Der Dateibereichsname kann kein Platzhalterzeichen sein, wenn NAMETYPE für eine Dateibereichskollokationsgruppe angegeben wird. Der Standardwert lautet SERVER. Sie können einen der folgenden Werte angeben:

#### SERVER

Der Server verwendet die Zeichenumsetzungstabelle des Servers, um die Dateibereichsnamen zu interpretieren.

#### UNICODE

Der Server konvertiert die Dateibereichsnamen aus der Server-Codepage in die Codepage UTF-8. Die Zeichen in den Namen und die Server-Codepage bestimmen, ob die Namen konvertiert werden können. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Server-Codepage nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

#### FSID

Der Server interpretiert die Dateibereichsnamen nach ihren Dateibereichs-IDs (FSIDs).

### CODETYPE

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Verwenden Sie diesen Parameter, wenn Sie ein Platzhalterzeichen für den Dateibereichsnamen verwenden. Beispiel:

```
define collocmember production Win_3419 filespace=* codetype=unicode
```

Mit diesem Beispielbefehl werden alle Dateibereiche auf dem Knoten Win\_3419 zur Kollokationsgruppe 'production' hinzugefügt. Der Standardwert lautet BOTH, d. h., die Dateibereiche werden unabhängig vom Codepagetyp eingeschlossen. Sie können einen der folgenden Werte angeben:

#### BOTH

Die Dateibereiche unabhängig vom Codepagetyp einschließen.

#### UNICODE

Nur Dateibereiche einschließen, die in Unicode sind.

NONUNICODE

Dateibereiche einschließen, die nicht in Unicode sind.

## Zwei Kollokationsgruppenmitglieder definieren

Die beiden Knoten NODE1 und NODE2 für die Kollokationsgruppe GROUP1 definieren.

```
define collocmember group1 node1,node2
```

## Ein Dateibereichsgruppenmitglied CNTR90524 auf dem Knoten clifton für die Kollokationsgruppe TSM\_alpha\_1 definieren

```
define collocmember TSM_alpha_1 clifton filespace=CNTR90524
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE COLLOCMEMBER

| Befehl              | Beschreibung   |
|---------------------|--|
| DEFINE COLLOGROUP   | Definiert eine Kollokationsgruppe.   |
| DEFINE STGPOOL      | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.   |
| DELETE COLLOGROUP   | Löscht eine Kollokationsgruppe.  |
| DELETE COLLOCMEMBER | Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.  |
| DELETE FILESPACE    | Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt. |
| MOVE NODEDATA       | Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen.  |
| QUERY COLLOGROUP    | Zeigt Informationen zu Kollokationsgruppen an.   |
| QUERY NODE          | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.  |
| QUERY NODEDATA      | Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.  |
| QUERY STGPOOL       | Zeigt Informationen zu Speicherpools an.   |
| REMOVE NODE         | Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.   |
| UPDATE COLLOGROUP   | Aktualisiert die Beschreibung einer Kollokationsgruppe.  |
| UPDATE STGPOOL      | Ändert die Attribute eines Speicherpools.  |

## DEFINE COPYGROUP (Kopiengruppe definieren)

Mit diesem Befehl kann eine neue Sicherungs- oder Archivierungskopiengruppe in einer bestimmten Verwaltungsklasse, Maßnahmengruppe und Maßnahmendomäne definiert werden. Der Server verwendet die Sicherungs- und Archivierungskopiengruppen, um zu steuern, wie Clients Dateien sichern und archivieren, und um die gesicherten und archivierten Dateien zu verwalten.

Um Clients die Verwendung der neuen Kopiengruppe zu ermöglichen, muss die Maßnahmengruppe aktiviert werden, die die neue Kopiengruppe enthält.

Für jede Verwaltungsklasse kann eine Sicherungskopiengruppe und eine Archivierungskopiengruppe definiert werden. Um sicherzustellen, dass Clientknoten Dateien sichern können, schließen Sie eine Sicherungskopiengruppe in der Standardverwaltungsklasse für eine Maßnahmengruppe ein.

Achtung: Der Befehl DEFINE COPYGROUP schlägt fehl, wenn ein Kopiespeicherpool als Ziel angegeben wird.

Der Befehl DEFINE COPYGROUP liegt in zwei Formen vor, eine zum Definieren einer Sicherungskopiengruppe und eine zum Definieren einer Archivierungskopiengruppe. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für DEFINE COPYGROUP

| Befehl                         | Beschreibung  |
|--------------------------------|---|
| ASSIGN DEFMGMTCLASS            | Ordnet eine Verwaltungsklasse als Standardklasse für eine angegebene Maßnahmengruppe zu.                  |
| BACKUP NODE                    | Sichert einen NAS-Knoten (NAS = Network Attached Storage).  |
| COPY MGMTCLASS                 | Erstellt eine Kopie einer Verwaltungsklasse.  |
| DEFINE MGMTCLASS               | Definiert eine Verwaltungsklasse.   |
| DEFINE STGPOOL                 | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.                        |
| DELETE COPYGROUP               | Löscht eine Sicherungs- oder Archivierungskopiengruppe aus einer Maßnahmendomäne und Maßnahmengruppe.     |
| DELETE MGMTCLASS               | Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe. |
| EXPIRE INVENTORY               | Startet die Verfallsverarbeitung für den Datenträgerbestandsverfall manuell.                              |
| QUERY COPYGROUP                | Zeigt die Attribute einer Kopiengruppe an.  |
| QUERY MGMTCLASS                | Zeigt Informationen zu Verwaltungsklassen an.   |
| SET ARCHIVERETENTIONPROTECTION | Gibt an, ob der Aufbewahrungsschutz für Daten aktiviert ist.  |
| UPDATE COPYGROUP               | Ändert ein oder mehrere Attribute einer Kopiengruppe.   |

- DEFINE COPYGROUP (Sicherungskopiengruppe definieren)  
Mit diesem Befehl kann eine neue Sicherungskopiengruppe innerhalb einer bestimmten Verwaltungsklasse, Maßnahmengruppe und Maßnahmendomäne definiert werden.
- DEFINE COPYGROUP (Archivierungskopiengruppe definieren)  
Mit diesem Befehl kann eine neue Archivierungskopiengruppe innerhalb einer bestimmten Verwaltungsklasse, Maßnahmengruppe und Maßnahmendomäne definiert werden.

## DEFINE COPYGROUP (Sicherungskopiengruppe definieren)

Mit diesem Befehl kann eine neue Sicherungskopiengruppe innerhalb einer bestimmten Verwaltungsklasse, Maßnahmengruppe und Maßnahmendomäne definiert werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Kopiengruppe gehört.

### Syntax

```
>>-DEFine Copygroup--Domänennamen--Name_der_Maßnahmengruppe--Klassennamen-->
    .-STANDARD-.    .-Type-----Backup-.
>-----+-----+-----+-----+----->
    '-STANDARD-'   '-Type-----Backup-'

                                .-FREquency-----0-----
>--DESTination-----Poolnamen-----+-----+----->
                                '-FREquency-----Tage-'

    .-VERExists-----2-----
>-----+-----+-----+-----+----->
    '-VERExists-----+Anzahl--+-'
                                '-NOLimit-'

    .-VERDeleted-----1-----
>-----+-----+-----+-----+----->
    '-VERDeleted-----+Anzahl--+-'
                                '-NOLimit-'

    .-RETEExtra-----30-----    .-RETOOnly-----60-----
```



```

>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
  '-RETEExtra--++-+Tage--++-' '-RETOOnly--++-+Tage--++-'
      '-NOLimit-'              '-NOLimit-'

  .-MODE--++-+MODified--++-+
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
  '-MODE--++-+MODified--++-'
      '-ABSolute-'

  .-SERialization--++-+SHRStatic--++-+
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
  '-SERialization--++-+SHRStatic--++-'
      +-Static--++-+
      +-SHRDYnamic--++-+
      '-DYnamic--++-'

>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----><
  '-TOCDestination--++-+PoolName--++-'

```

## Parameter

---

### Domänenname (Erforderlich)

Gibt die Maßnahmendomäne an, für die die Kopiengruppe definiert wird.

### Name\_der\_Maßnahmengruppe (Erforderlich)

Gibt die Maßnahmengruppe an, für die die Kopiengruppe definiert wird.

Für eine Verwaltungsklasse, die zu der aktiven Maßnahmengruppe (ACTIVE) gehört, kann keine Kopiengruppe definiert werden.

### Klassenname (Erforderlich)

Gibt die Verwaltungsklasse an, für die die Kopiengruppe definiert wird.

### STANDARD

Gibt den Namen der Kopiengruppe an, der STANDARD lauten muss. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD.

### Type=Backup

Gibt an, dass eine Sicherungskopiengruppe definiert werden soll. Der Standardparameter ist BACKUP. Dieser Parameter ist wahlfrei.

### DESTination (Erforderlich)

Gibt den primären Speicherpool an, in dem der Server anfänglich Sicherungsdaten speichert. Ein Kopiespeicherpool kann nicht als Zielort angegeben werden.

### FREQuency

Gibt an, wie oft IBM Spectrum Protect eine Datei sichern kann. Dieser Parameter ist wahlfrei. IBM Spectrum Protect sichert eine Datei nur, wenn die angegebene Anzahl Tage seit der letzten Sicherung verstrichen ist. Der Wert für den Parameter FREQUENCY wird nur bei einer vollständigen Teilsicherung verwendet. Dieser Wert wird bei einer selektiven Sicherung oder einer partiellen Teilsicherung ignoriert. Zulässige Werte sind ganze Zahlen von 0 bis 9999. Der Standardwert ist 0. Dieser Standardwert bedeutet, daß IBM Spectrum Protect eine Datei unabhängig vom Datum der letzten Sicherung sichern kann.

### VERExists

Gibt die maximale Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die sich momentan im Client-Dateisystem befinden. Dieser Parameter ist wahlfrei. Der Standardwert ist 2.

Wird der Grenzwert durch eine Teilsicherungsoperation überschritten, verfällt die älteste Sicherungsversion, die im Serverspeicher vorhanden ist. Gültige Werte:

#### Zahl

Gibt die Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die sich momentan im Client-Dateisystem befinden. Zulässige Werte sind ganze Zahlen von 1 bis 9999.

Tipp: Um sicherzustellen, dass Dateien nach einem Malwarevorfall, wie z. B. einer Ransomware-Attacke, wiederhergestellt werden können, geben Sie einen Wert von mindestens 2 an. Bevorzugte Werte sind 3, 4 oder höher.

#### NOLimit

Gibt an, daß der Server alle Sicherungsversionen aufbewahren soll.

Die Anzahl der Sicherungsversionen, die aufbewahrt werden sollen, wird so lange durch diesen Parameter gesteuert, bis Versionen den Aufbewahrungszeitraum überschreiten, der durch den Parameter RETEXTRA angegeben ist.

### VERDeleted

Gibt die maximale Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die aus dem Client-Dateisystem gelöscht wurden, nachdem sie mit IBM Spectrum Protect gesichert wurden. Dieser Parameter ist wahlfrei. Der Standardwert ist 1. Löscht ein Benutzer eine Datei aus dem Clientdateisystem, werden bei der nächsten Teilsicherung die ältesten Versionen der Datei, die diese Anzahl überschreiten, von dem Server als verfallen gekennzeichnet. Das Verfallsdatum der übrigen Versionen wird durch den Aufbewahrungszeitraum bestimmt, der mit dem Parameter RETEXTRA oder RETONLY angegeben wurde. Gültige Werte:

#### Anzahl

Gibt die Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die nach der Sicherung aus dem Client-Dateisystem gelöscht werden. Zulässige Werte sind ganze Zahlen von 0 bis 9999.

#### NOLimit

Gibt an, dass der Server alle Sicherungsversionen für Dateien, die nach der Sicherung aus dem Clientdateisystem gelöscht werden, aufbewahren soll.

#### RETEExtra

Gibt die Anzahl Tage an, die eine Sicherungsversion aufbewahrt werden soll, nachdem diese Version inaktiv wurde. Die Version einer Datei wird inaktiv, wenn der Client eine aktuellere Sicherungsversion speichert oder wenn der Client die Datei aus der Datenstation löscht und dann eine vollständige Teilsicherung durchführt. Der Server löscht inaktive Versionen auf der Basis des Aufbewahrungszeitraums, auch wenn die Anzahl der inaktiven Versionen die durch den Parameter VEREXISTS oder VERDELETED erlaubte Anzahl nicht überschreitet. Dieser Parameter ist wahlfrei. Der Standardwert ist 30 Tage. Gültige Werte:

#### Tage

Gibt die Anzahl Tage an, die inaktive Sicherungsversionen aufbewahrt werden sollen. Zulässige Werte sind ganze Zahlen von 0 bis 9999.

Tipp: Um sicherzustellen, dass Dateien nach einem Malwarevorfall, wie z. B. einer Ransomware-Attacke, wiederhergestellt werden können, geben Sie einen Wert von mindestens 14 Tagen an. Der bevorzugte Wert ist 30 oder mehr Tage.

#### NOLimit

Gibt an, dass inaktive Sicherungsversionen unbegrenzt aufbewahrt werden sollen.

Wird NOLIMIT angegeben, löscht der Server inaktive Sicherungsversionen auf der Basis des Parameters VEREXISTS (wenn die Datei noch im Clientdateisystem vorhanden ist) oder auf der Basis des Parameters VERDELETED (wenn die Datei nicht mehr im Clientdateisystem vorhanden ist).

#### RETOOnly

Gibt die Anzahl Tage an, die die letzte Sicherungsversion einer Datei aufbewahrt werden soll, die aus dem Client-Dateisystem gelöscht wurde. Dieser Parameter ist wahlfrei. Der Standardwert ist 60. Gültige Werte:

#### Tage

Gibt die Anzahl Tage an, die die letzte verbleibende inaktive Version einer Datei aufbewahrt werden soll. Zulässige Werte sind ganze Zahlen von 0 bis 9999.

Tipp: Um sicherzustellen, dass Dateien nach einem Malwarevorfall, wie z. B. einer Ransomware-Attacke, wiederhergestellt werden können, geben Sie einen Wert von mindestens 30 Tagen an.

#### NOLimit

Gibt an, dass die letzte verbleibende inaktive Version einer Datei unbegrenzt aufbewahrt werden soll.

Wird NOLIMIT angegeben, wird die letzte verbleibende Sicherungsversion unbegrenzt von dem Server aufbewahrt, es sei denn, ein Benutzer oder Administrator löscht die Datei aus dem Server-Speicher.

#### MODE

Gibt an, ob IBM Spectrum Protect eine Datei nur sichert, wenn sich die Datei seit der letzten Sicherung geändert hat oder wenn ein Client eine Sicherung anfordert. Dieser Parameter ist wahlfrei. Der Standardwert ist MODIFIED. Gültige Werte:

#### MODified

Gibt an, dass IBM Spectrum Protect die Datei nur sichert, wenn sie sich seit der letzten Sicherung geändert hat. IBM Spectrum Protect betrachtet eine Datei als geändert, wenn folgende Bedingungen zutreffen:

- Das Datum der letzten Änderung hat sich geändert.
- Die Dateigröße hat sich geändert.
- Der Dateieigner hat sich geändert.
- Die Dateiberechtigungen haben sich geändert.

#### ABSolute

Gibt an, dass IBM Spectrum Protect die Datei sichert, unabhängig davon, ob sie sich geändert hat.

Der Wert für MODE wird nur für vollständige Teilsicherungen verwendet. Dieser Wert wird bei einer partiellen Teilsicherung oder einer selektiven Sicherung ignoriert.

#### SERialization

Gibt an, wie IBM Spectrum Protect Dateien oder Verzeichnisse verarbeitet, wenn sie während der Sicherungsverarbeitung geändert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist SHRSTATIC. Gültige Werte:

#### SHRStatic

Gibt an, dass IBM Spectrum Protect eine Datei oder ein Verzeichnis nur sichert, wenn die Datei oder das Verzeichnis während der Sicherung nicht geändert wird. IBM Spectrum Protect versucht bis zu viermal, eine Sicherung durchzuführen,

abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wurde. Wird die Datei oder das Verzeichnis während jedes Sicherungsversuchs geändert, wird sie bzw. es von IBM Spectrum Protect nicht gesichert.

#### Static

Gibt an, dass IBM Spectrum Protect eine Datei oder ein Verzeichnis nur sichert, wenn die Datei oder das Verzeichnis während der Sicherung nicht geändert wird. IBM Spectrum Protect versucht nur einmal, die Sicherung durchzuführen.

Plattformen, die die Option STATIC nicht unterstützen, nehmen den Standardwert SHRSTATIC an.

#### SHRDynamic

Gibt an, dass IBM Spectrum Protect die Datei oder das Verzeichnis während des letzten Sicherungsversuchs sichert, auch wenn die Datei oder das Verzeichnis während der Sicherung geändert wird. IBM Spectrum Protect versucht bis zu viermal, eine Sicherung durchzuführen, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wurde.

#### Dynamic

Gibt an, dass IBM Spectrum Protect eine Datei oder ein Verzeichnis beim ersten Versuch sichert, auch wenn die Datei oder das Verzeichnis während der Sicherungsverarbeitung geändert wird.

Achtung: Die Werte SHRDYNAMIC und DYNAMIC sind mit Vorsicht zu verwenden. IBM Spectrum Protect bestimmt anhand dieser Werte, ob eine Datei oder ein Verzeichnis gesichert wird, während Änderungen vorgenommen werden. Aus diesem Grund ist die Sicherungsversion möglicherweise nur eine Sicherung mit grober Übereinstimmung. Eine Sicherung mit grober Übereinstimmung gibt den aktuellen Inhalt der Datei oder des Verzeichnisses nicht korrekt wieder, da sie einige, aber nicht alle Änderungen enthält. Wird eine Datei, die eine Sicherung mit grober Übereinstimmung enthält, zurückgeschrieben, ist die Datei möglicherweise nicht brauchbar. Dies ist von der Anwendung abhängig, die die Datei verwendet. Ist eine Sicherung mit grober Übereinstimmung nicht akzeptabel, definieren Sie für SERIALIZATION den Wert SHRSTATIC oder STATIC, damit IBM Spectrum Protect nur dann eine Sicherungsversion erstellt, wenn die Datei oder das Verzeichnis nicht geändert wird.

#### TOCDestination

Gibt den primären Speicherpool an, in dem ein Inhaltsverzeichnis für jede NDMP-Sicherungs- oder -Sicherungsgruppenoperation anfänglich gespeichert wird, für die ein Inhaltsverzeichnis generiert wird (NDMP - Network Data Management Protocol). Dieser Parameter ist wahlfrei. Ein Kopierspeicherpool kann nicht als Zielort angegeben werden. Der als Zielort angegebene Speicherpool muss das Datenformat NATIVE oder NONBLOCK haben. Um Ladeverzögerungen zu vermeiden, wird empfohlen, dass der Speicherpool die Einheitenklasse DISK oder DEVTYPE=FILE hat. Die Generierung eines Inhaltsverzeichnisses ist eine Option für NDMP-Sicherungsoperationen, wird aber nicht für andere Imagesicherungsoperationen unterstützt.

Wird die Erstellung eines Inhaltsverzeichnisses (TOC) für eine Sicherungsoperation angefordert, die NDMP verwendet, und ist das Image an eine Verwaltungsklasse gebunden, deren Sicherungskopiengruppe keinen Zielort für das Inhaltsverzeichnis angibt, hängt das Ergebnis von dem TOC-Parameter für die Sicherungsoperation ab.

- Bei TOC=PREFERRED (Standardwert) wird die Sicherung ohne Erstellung eines Inhaltsverzeichnisses fortgesetzt.
- Bei TOC=YES schlägt die gesamte Sicherung fehl, da kein Inhaltsverzeichnis erstellt werden kann.

## Beispiel: Eine Sicherungskopiengruppe erstellen

---

Eine Sicherungskopiengruppe STANDARD für Verwaltungsklasse ACTIVEFILES in Maßnahmengruppe VACATION in der Maßnahmendomäne EMPLOYEE\_RECORDS erstellen. Den Zielort der Sicherung auf BACKUPPOOL setzen. Für das Mindestintervall zwischen Sicherungen drei Tage angeben, unabhängig davon, ob die Dateien geändert wurden. Bis zu fünf Sicherungsversionen einer Datei aufbewahren, während die Datei im Client-Dateisystem vorhanden ist.

```
define copygroup employee_records
vacation activefiles standard type=backup
destination=backuppools frequency=3
verexists=5 mode=absolute
```

## DEFINE COPYGROUP (Archivierungskopiengruppe definieren)

---

Mit diesem Befehl kann eine neue Archivierungskopiengruppe innerhalb einer bestimmten Verwaltungsklasse, Maßnahmengruppe und Maßnahmendomäne definiert werden.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Kopiengruppe gehört.

## Syntax

---

```
>>-DEFine COpygroup--Domänename--Name_der_Maßnahmengruppe--Klassename-->>
```

```

.-STANDARD-.
>-----Type-----Archive--DESTination-----Poolname----->
'-STANDARD-'

.-FREQuency---Cmd-. .-RETVer---365-----.
>-----+-----+-----+-----+-----+-----+----->
'-FREQuency---Cmd-' '-RETVer---+Tage---+'
                               '-NOLimit-'

.-RETInit---CREAtion--. .-RETMin---365-----.
>-----+-----+-----+-----+-----+-----+----->
'-RETInit---Event---' '-RETMin---Tage---'

.-MODE---ABSolute-.
>-----+-----+-----+-----+-----+-----+----->
'-MODE---ABSolute-'

.-SERialization---SHRStatic-----.
>-----+-----+-----+-----+-----+-----+-----><
'-SERialization---+SHRStatic---+'
                               +-Static-----+
                               +-SHRDYnamic-+
                               '-DYnamic---'

```

## Parameter

Domänenname (Erforderlich)

Gibt den Namen der Maßnahmendomäne an, für die die Kopiengruppe definiert wird.

Name\_der\_Maßnahmengruppe (Erforderlich)

Gibt den Namen der Maßnahmengruppe an, für die die Kopiengruppe definiert wird.

Für eine Verwaltungsklasse, die zu der aktiven Maßnahmengruppe (ACTIVE) gehört, kann keine Kopiengruppe definiert werden.

Klassenname (Erforderlich)

Gibt den Namen der Verwaltungsklasse an, für die die Kopiengruppe definiert wird.

STANDARD

Gibt den Namen der Kopiengruppe an, der STANDARD lauten muss. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD.

Type=Archive (Erforderlich)

Gibt an, dass eine Archivierungskopiengruppe definiert werden soll.

DESTination (Erforderlich)

Gibt den primären Speicherpool an, in dem der Server anfänglich die Archivierungskopie speichert. Ein Kopiespeicherpool kann nicht als Zielort angegeben werden.

FREQuency=Cmd

Gibt die Kopienhäufigkeit an, die CMD lauten muss. Dieser Parameter ist wahlfrei. Der Standardwert ist CMD.

RETVer

Gibt die Anzahl Tage an, die eine Archivierungskopie aufbewahrt werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist 365. Gültige Werte:

Tage

Gibt den Zeitraum an, den eine Archivierungskopie aufbewahrt werden soll. Sie können eine ganze Zahl im Bereich von 0 bis 30000 angeben.

Tipp: Um sicherzustellen, dass Ihre Daten nach einem Malwarevorfall, wie z. B. einer Ransomware-Attacke, wiederhergestellt werden können, geben Sie einen Wert von mindestens 30 Tagen an.

Die Serveroption RETENTIONEXTENSION kann sich auf die Datenträgeraufbewahrungsdauer auswirken, wenn die folgenden Bedingungen erfüllt sind:

- Sie geben Null als Anzahl der Tage an
- Der Zielspeicherpool für die Archivierungskopiengruppe ist ein SnapLock-Speicherpool (RECLAMATIONTYPE=SNAPLOCK)

Wenn beide Bedingungen erfüllt sind, wird die Aufbewahrungsdauer der Datenträger durch den Wert der Serveroption RETENTIONEXTENSION definiert. Der Wert der Serveroption RETENTIONEXTENSION wird auch angewendet, wenn Daten durch einen Serverprozess, wie z. B. die Umlagerung, oder mithilfe des Befehls MOVE DATA oder MOVE NODEDATA in den Snaplock-Speicherpool kopiert oder versetzt werden.

NOLimit

Gibt an, dass eine Archivierungskopie unbegrenzt aufbewahrt werden soll.

Wird NOLIMIT angegeben, werden Archivierungskopien von dem Server unbegrenzt aufbewahrt, es sei denn, ein Benutzer oder Administrator löscht die Datei aus dem Server-Speicher. Wird NOLIMIT angegeben, können Sie nicht auch EVENT für den Parameter RETINIT angeben.

Der Wert des Parameters RETVER kann Auswirkungen auf die Verwaltungsklasse haben, mit der der Server ein archiviertes Verzeichnis verbindet. Wenn der Client die Option ARCHMC nicht verwendet, verbindet der Server Verzeichnisse, die archiviert werden, mit der Standardverwaltungsklasse. Verfügt die Standardverwaltungsklasse über keine Archivierungskopiengruppe, verbindet der Server Verzeichnisse, die archiviert werden, mit der Verwaltungsklasse mit dem kürzesten Aufbewahrungszeitraum.

Der Parameter RETVER der Archivierungskopiengruppe der Verwaltungsklasse, an die ein Objekt gebunden wird, bestimmt das Aufbewahrungskriterium für jedes Objekt. Eine Beschreibung des Datenschutzes befindet sich unter dem Befehl SET ARCHIVERETENTIONPROTECTION.

Wenn der im Parameter DESTINATION angegebene primäre Speicherpool zu einer Centera-Einheitenklasse gehört und der Datenschutz aktiviert ist, wird der Wert für RETVER zu Zwecken der Aufbewahrungsverwaltung an Centera gesendet. Eine Beschreibung des Datenschutzes befindet sich unter dem Befehl SET ARCHIVERETENTIONPROTECTION.

#### RETIInit

Gibt an, wann der durch das RETVER-Attribut angegebene Aufbewahrungszeitraum beginnt. Dieser Parameter ist wahlfrei. Wenn Sie den Wert für RETINIT während der Erstellung der Kopiengruppe definieren, können Sie ihn später nicht ändern. Der Standardwert ist CREATION. Gültige Werte:

##### CREATION

Gibt an, dass der durch das RETVER-Attribut angegebene Aufbewahrungszeitraum zu dem Zeitpunkt beginnt, zu dem eine Archivierungskopie auf dem IBM Spectrum Protect-Server gespeichert wird.

##### Event

Gibt an, dass der im Parameter RETVER angegebene Aufbewahrungszeitraum zu dem Zeitpunkt beginnt, zu dem eine Clientanwendung den Server über ein Ereignis bezüglich des Aufbewahrungsstarts für die Archivierungskopie informiert. Wird RETINIT=EVENT angegeben, können Sie nicht gleichzeitig RETVER=NOLIMIT angeben.

Tipp: Sie können "Löschen unzulässig" für ein Objekt angeben, das mit RETINIT=EVENT gespeichert wurde und für das noch kein Ereignis gesendet wurde. Wird das Ereignis gesendet, während die Angabe "Löschen unzulässig" wirksam ist, beginnt der Aufbewahrungszeitraum, aber das Objekt wird nicht gelöscht, während "Löschen unzulässig" wirksam ist.

#### RETMIn

Gibt die Mindestanzahl von Tagen an, die eine Archivierungskopie aufbewahrt werden soll, nachdem sie archiviert wurde. Dieser Parameter ist wahlfrei. Der Standardwert ist 365. Wird RETINIT=CREATION angegeben, wird dieser Parameter ignoriert.

#### MODE=ABSolute

Gibt an, dass eine Datei immer archiviert wird, wenn der Client dies anfordert. Der Parameter MODE muss den Wert ABSOLUTE haben. Dieser Parameter ist wahlfrei. Der Standardwert ist ABSOLUTE.

#### SERialization

Gibt an, wie IBM Spectrum Protect Dateien verarbeitet, die während der Archivierung geändert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist SHRSTATIC. Gültige Werte:

##### SHRStatic

Gibt an, dass IBM Spectrum Protect eine Datei nur archiviert, wenn sie nicht geändert wird. IBM Spectrum Protect versucht bis zu viermal, eine Archivierungsoperation durchzuführen, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wird. Wenn die Datei während des Archivierungsversuchs geändert wird, archiviert IBM Spectrum Protect die Datei nicht.

##### Static

Gibt an, dass IBM Spectrum Protect eine Datei nur archiviert, wenn sie nicht geändert wird. IBM Spectrum Protect versucht nur einmal, die Archivierungsoperation durchzuführen.

Plattformen, die die Option STATIC nicht unterstützen, nehmen den Standardwert SHRSTATIC an.

##### SHRDynamic

Gibt an, dass IBM Spectrum Protect die Datei während des letzten Archivierungsversuchs archiviert, auch wenn die Datei während der Archivierung geändert wird. IBM Spectrum Protect versucht bis zu viermal, die Datei zu archivieren, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wird.

##### Dynamic

Gibt an, dass IBM Spectrum Protect eine Datei beim ersten Versuch archiviert, auch wenn sie während der Archivierungsverarbeitung geändert wird.

Achtung: Die Werte SHRDYNAMIC und DYNAMIC sind mit Vorsicht zu verwenden. IBM Spectrum Protect bestimmt anhand dieser Werte, ob eine Datei archiviert wird, während Änderungen vorgenommen werden. Aus diesem Grund ist die Archivierungskopie möglicherweise nur eine Sicherung mit grober Übereinstimmung. Eine Sicherung mit grober Übereinstimmung gibt den Inhalt der Datei nicht korrekt wieder, da sie einige, aber nicht alle Änderungen enthält. Wird eine Datei, die eine Sicherung mit grober Übereinstimmung enthält, abgerufen, ist die Datei möglicherweise nicht brauchbar. Dies ist von der Anwendung abhängig, die die Datei verwendet. Ist eine Sicherung mit grober Übereinstimmung nicht



Gibt an, dass die Einheit zum Versetzen von Daten ein NAS-Dateiserver in einem Cluster ist.  
Einschränkung: Sie können den Wert NASCLUSTER nur bei DATAFORMAT=NETAPPDUMP angeben.

#### NASVSERVER

Gibt an, dass die Einheit zum Versetzen von Daten eine virtuelle Speichereinheit innerhalb eines Clusters ist.  
Einschränkung: Sie können den Wert NASVSERVER nur bei DATAFORMAT=NETAPPDUMP angeben.

#### HLAddress (Erforderlich)

Gibt entweder die numerische IP-Adresse oder den Domännennamen an, die bzw. der für den Zugriff auf den NAS-Dateiserver verwendet wird.

Tipp: Um die numerische IP-Adresse zu bestimmen, greifen Sie auf den NAS-Dateiserver zu. Führen Sie dann die Anweisungen in der Dokumentation für den Dateiserver aus, um die Adresse abzurufen.

#### LLAddress

Gibt die TCP-Anschlussnummer für den Zugriff auf die NAS-Einheit für NDMP-Sitzungen (NDMP = Network Data Management Protocol) an. Dieser Parameter ist wahlfrei. Der Standardwert ist 10000.

#### USERid (Erforderlich)

Gibt die Benutzer-ID eines Benutzers an, der berechtigt ist, eine NDMP-Sitzung mit dem NAS-Dateiserver einzuleiten. Geben Sie beispielsweise die Benutzer-ID ein, die auf dem NetApp-Dateiserver für NDMP-Verbindungen konfiguriert ist.

Tipp: Um die Benutzer-ID zu bestimmen, greifen Sie auf den NAS-Dateiserver zu. Führen Sie dann die Anweisungen in der Dokumentation für den Dateiserver aus, um die Benutzer-ID abzurufen.

#### PASSword (Erforderlich)

Gibt das Kennwort der Benutzer-ID für die Anmeldung beim NAS-Dateiserver an.

Tipp: Um das Kennwort zu bestimmen, greifen Sie auf den NAS-Dateiserver zu. Führen Sie dann die Anweisungen in der Dokumentation für den Dateiserver aus, um das Kennwort abzurufen.

#### ONLine

Gibt an, ob die Einheit zum Versetzen von Daten für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

#### Yes

Der Standardwert. Gibt an, dass die Einheit zum Versetzen von Daten für die Verwendung verfügbar ist.

#### No

Gibt an, dass die Einheit zum Versetzen von Daten nicht für die Verwendung verfügbar ist. Wird die Hardware gewartet, können Sie mit dem Befehl UPDATE DATAMOVER die Einheit zum Versetzen von Daten in den Offline-Status setzen.

Wird ein Speicherarchiv durch die Verwendung eines Pfads von einer NAS-Einheit zum Versetzen von Daten zu dem Speicherarchiv gesteuert, und ist die NAS-Einheit zum Versetzen von Daten offline, kann der Server nicht auf das Speicherarchiv zugreifen. Wird der Server angehalten und erneut gestartet, während die NAS-Einheit zum Versetzen von Daten offline ist, wird das Speicherarchiv nicht initialisiert.

#### DATAFormat (Erforderlich)

Gibt das Datenformat an, das von dieser Einheit zum Versetzen von Daten verwendet wird.

#### NETAPPDump

Muss für NetApp-NAS-Dateiserver und IBM® System Storage N Series verwendet werden.

#### CELERRADump

Muss für EMC Celerra NAS-Dateiserver verwendet werden.

#### NDMPDump

Muss für NAS-Dateiserver verwendet werden, die keine NetApp- oder EMC-Dateiserver sind.

## Beispiel: Eine Einheit zum Versetzen von Daten nach Domänenname definieren

---

Eine Einheit zum Versetzen von Daten für den Knoten NAS1 definieren. Der Domänenname für die Einheit zum Versetzen von Daten lautet NETAPP2.EXAMPLE.COM, die Anschlussnummer ist 10000.

```
define datamover nas1 type=nas hladdress=netapp2.example.com lladdress=10000  
userid=root password=admin dataformat=netappdump
```

## Beispiel: Eine Einheit zum Versetzen von Daten nach IP-Adresse definieren

---

Eine Einheit zum Versetzen von Daten für den Knoten NAS2 definieren. Die numerische IP-Adresse der Einheit zum Versetzen von Daten ist 203.0.113.0, die Anschlussnummer lautet 10000. Der NAS-Dateiserver ist kein NetApp- oder EMC-Dateiserver.

```
define datamover nas2 type=nas hladdress=203.0.113.0 lladdress=10000  
userid=root password=admin dataformat=ndmpdump
```

## Beispiel: Eine Einheit zum Versetzen von Daten für einen Clusterdateiserver nach IP-Adresse definieren

---

Eine Einheit zum Versetzen von Daten für den Clusterdateiserver NAS3 definieren. Der NAS-Dateiserver ist eine NetApp-Einheit. Die numerische IP-Adresse der Einheit zum Versetzen von Daten ist 198.51.100.0, die Anschlussnummer lautet 10000.

```
define datamover nas3 type=nascluster hladdress=198.51.100.0
  lladdress=10000 userid=root password=admin dataformat=netappdump
```



## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE DATAMOVER

| Befehl           | Beschreibung  |
|------------------|---|
| DEFINE PATH      | Definiert einen Pfad von einer Quelle zu einem Ziel.                                    |
| DELETE DATAMOVER | Löscht eine Einheit zum Versetzen von Daten.  |
| QUERY DATAMOVER  | Zeigt Definitionen der Einheit zum Versetzen von Daten an.                              |
| REGISTER NODE    | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest. |
| UPDATE DATAMOVER | Ändert die Definition einer Einheit zum Versetzen von Daten.                            |

## DEFINE DEVCLASS (Einheitenklasse definieren)

Verwenden Sie diesen Befehl, um eine Einheitenklasse für einen Speichereinheitentyp zu definieren. Für den Server muss eine Einheitenklasse definiert werden, damit eine Einheit verwendet werden kann.



Die neueste Liste der unterstützten Einheiten und gültigen Einheitenklassenformate befindet sich auf der Website für die unterstützten IBM Spectrum Protect-Einheiten:  AIX-Betriebssysteme  Windows-Betriebssysteme

- Supported devices for AIX and Windows

 Linux-Betriebssysteme

- Supported devices for Linux

Anmerkung: Die Einheitenklasse DISK wird von IBM Spectrum Protect definiert und kann mit dem Befehl DEFINE DEVCLASS nicht geändert werden.

 AIX-Betriebssysteme  Linux-Betriebssysteme Wenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in DEFINE DEVCLASS - z/OS Media-Server (Einheitenklasse für z/OS Media-Server definieren).

Die folgenden IBM Spectrum Protect-Einheitenklassen sind nach Einheitentyp sortiert.



- DEFINE DEVCLASS (Einheitenklasse 3590 definieren)
- DEFINE DEVCLASS (Einheitenklasse 3592 definieren)
- DEFINE DEVCLASS (Einheitenklasse 4MM definieren)
- DEFINE DEVCLASS (Einheitenklasse 8MM definieren)
- DEFINE DEVCLASS (Einheitenklasse CENTERA definieren)
- DEFINE DEVCLASS (Einheitenklasse DLT definieren)
- DEFINE DEVCLASS (Einheitenklasse ECARTRIDGE definieren)
- DEFINE DEVCLASS (Einheitenklasse FILE definieren)
-  AIX-Betriebssysteme  Windows-Betriebssysteme DEFINE DEVCLASS (Einheitenklasse GENERICTAPE definieren)
- DEFINE DEVCLASS (Einheitenklasse LTO definieren)
- DEFINE DEVCLASS (Einheitenklasse NAS definieren)
- DEFINE DEVCLASS (Einheitenklasse REMOVABLEFILE definieren)
- DEFINE DEVCLASS (Einheitenklasse SERVER definieren)
- DEFINE DEVCLASS (Einheitenklasse VOLSAFE definieren)

Tabelle 1. Zugehörige Befehle für DEFINE DEVCLASS


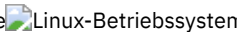
| Befehl           | Beschreibung  |
|------------------|---|
| BACKUP DEVCONFIG | Sichert IBM Spectrum Protect-Einheitendaten in einer Datei.   |
| DEFINE LIBRARY   | Definiert ein automatisiertes oder manuelles Kassettenarchiv. |
| DELETE DEVCLASS  | Löscht eine Einheitenklasse.                                  |



| Befehl          | Beschreibung                                   |
|-----------------|--|
| QUERY DEVCLASS  | Zeigt Informationen zu Einheitenklassen an.    |
| QUERY DIRSPACE  | Zeigt Informationen zu Verzeichnissen FILE an. |
| UPDATE DEVCLASS | Ändert die Attribute einer Einheitenklasse.    |

## DEFINE DEVCLASS (Einheitenklasse 3590 definieren)

Verwenden Sie die Einheitenklasse 3590, wenn Sie 3590-Bandeinheiten verwenden.

  Wenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in DEFINE DEVCLASS (Einheitenklasse 3590 für z/OS Media-Server definieren).

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-DEFine DEVclass--Einheitenklassenname----->
>--LIBRary----Kassettenarchivname--DEVType-----3590----->
. -FORMAT-----DRIVE----- .
>+-----+-----+-----+----->
' -FORMAT-----+DRIVE---+ ' ' -ESTCAPacity-----Größe- '
      +-3590B---+
      +-3590C---+
      +-3590E-B-+
      +-3590E-C-+
      +-3590H-B-+
      '-3590H-C-'

. -PREFIX-----ADSM----- .
>+-----+-----+-----+----->
' -PREFIX-----+ADSM-----+-'
      '-Banddatenträgerpräfix-'

. -MOUNTRetention-----60----- . -MOUNTWait-----60----- .
>+-----+-----+-----+----->
' -MOUNTRetention-----Minuten- ' ' -MOUNTWait-----Minuten- '

. -MOUNTLimit-----DRIVES----- .
>+-----+-----+-----+-----><
' -MOUNTLimit-----+DRIVES+-+ '
      +-Anzahl+
      '-0-----'

```

### Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRARY (Erforderlich)

Gibt den Namen des definierten Kassettenarchivobjekts an, das die Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können.

Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

DEVType=3590 (Erforderlich)

Gibt an, dass der Einheitentyp 3590 der Einheitenklasse zugeordnet wird. 3590 gibt an, dass dieser Einheitenklasse Magnetbandkassetteneinheiten IBM® 3590 zugeordnet werden.

FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Geben Sie stattdessen das Format an, das die Laufwerke verwenden.

In den folgenden Tabellen sind die Aufzeichnungsformate, die geschätzten Kapazitäten und die Optionen der Aufzeichnungsformate für 3590-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für 3590

| Format   | Geschätzte Kapazität  | Beschreibung   |
|--|---|--|
| DRIVE  | –   | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| 3590B  | 10,0 GB   | Dekomprimiertes (Basis-)Format   |
| 3590C  | Siehe Anmerkung<br>20,0 GB  | Komprimiertes Format   |
| 3590E-B  | 10,0 GB   | Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format   |
| 3590E-C  | Siehe Anmerkung<br>20,0 GB  | Komprimiertes Format, ähnlich dem 3590C-Format   |
| 3590H-B  | 30,0 GB (J-Kassette – Standardlänge)<br>60,0 GB (K-Kassette - erweiterte Länge)                     | Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format   |
| 3590H-C  | Siehe Anmerkung<br>60,0 GB (J-Kassette - Standardlänge)<br>120,0 GB (K-Kassette - erweiterte Länge) | Komprimiertes Format, ähnlich dem 3590C-Format   |
| Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann die tatsächliche Kapazität abhängig von der Effektivität der Komprimierung größer als der aufgelistete Wert sein. |   |  |

Tabelle 2. Auswahl des Aufzeichnungsformats für 3590-Einheiten

| Einheit        | Format          |                 |                 |                 |                 |                 |
|----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
|                | 3590B           | 3590C           | 3590E-B         | 3590E-C         | 3590H-B         | 3590H-C         |
| 3590Ultra SCSI | Lesen/Schreiben | Lesen/Schreiben | ---             | ---             | ---             | ---             |
| 3590E          | Lesen/Schreiben | Lesen/Schreiben | Lesen/Schreiben | Lesen/Schreiben | Lesen/Schreiben | Lesen/Schreiben |
| 3590H          | Lesen           | Lesen           | Lesen           | Lesen           |                 |                 |
|                | Lesen           | Lesen           |                 |                 |                 |                 |

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist AD5M. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl


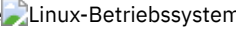
Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

## DEFINE DEVCLASS (Einheitenklasse 3592 definieren)

Verwenden Sie die Einheitenklasse 3592, wenn Sie 3592-Bandeinheiten verwenden.

  Wenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in DEFINE DEVCLASS (Einheitenklasse 3592 für z/OS Media-Server definieren).

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>--DEFine DEVclass--Einheitenklassenname----->
>--LIBRARY----Kassettenarchivname--DEVType----3592----->
                                     (1)
  .-LBProtect----No----- .-WORM----No-----
>+-----+-----+-----+-----+-----+-----+-----+----->
  '-LBProtect----+READWrite+-' '-WORM----+Yes+-'
      +-WRITEOnly-+           '-No--'
      '-No-----'

  .-SCALECAPacity----100----- .-FORMAT----DRIVE-----
>+-----+-----+-----+-----+-----+-----+-----+----->
  '-SCALECAPacity----+100+-' '-FORMAT----+DRIVE----+'
      +-90--+                +-3592-----+
      '-20--'                +-3592C----+
                          +-3592-2----+
                          +-3592-2C--+
                          +-3592-3----+
                          +-3592-3C--+
                          +-3592-4----+
                          +-3592-4C--+
                          +-3592-5----+
                          +-3592-5C--+
                          +-3592-5A--+
                          '-3592-5AC-'

>+-----+-----+-----+-----+-----+-----+-----+----->
  '-ESTCAPacity----Größe-'

  .-PREFIX----ADSM-----
>+-----+-----+-----+-----+-----+-----+-----+----->
  '-PREFIX----+ADSM-----+'
      '-Banddatenträgerpräfix-'

  .-MOUNTRetention----60----- .-MOUNTWait----60-----
>+-----+-----+-----+-----+-----+-----+-----+----->
  '-MOUNTRetention----Minuten-' '-MOUNTWait----Minuten-'

  .-MOUNTLimit----DRIVES-----
>+-----+-----+-----+-----+-----+-----+-----+----->
  '-MOUNTLimit----+DRIVES+-'
      +-Anzahl+
      '-0-----'

                                     (1) (2)
  .-DRIVEEncryption----ALLOW-----
>+-----+-----+-----+-----+-----+-----+-----+----->
  '-DRIVEEncryption----+ON-----+'
      +-ALLOW----+
      +-EXTERNAL-+
      '-OFF-----'
```

Anmerkungen:

1. Sie können nicht WORM=Yes in Verbindung mit DRIVEENCRYPTION=ON angeben.
2. Laufwerkverschlüsselung wird nur für 3592-Laufwerke der Generation 2 oder höher unterstützt.

## Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

## LIBRARY (Erforderlich)

Gibt den Namen des definierten Kassettenarchivobjekts an, das die Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können.

Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

## DEVType=3592 (Erforderlich)

Gibt an, dass der Einheitentyp 3592 der Einheitenklasse zugeordnet wird.

## LBProtect

Gibt an, ob der Schutz logischer Blöcke verwendet wird, um die Integrität von Daten sicherzustellen, die auf Band gespeichert sind. Wenn LBPROTECT auf READWRITE oder WRITEONLY gesetzt ist, verwendet der Server dieses Feature des Bandlaufwerks für den Schutz logischer Blöcke und generiert CRC-Zugriffsschutzinformationen für jeden Datenblock, der auf Band geschrieben wird. Der Server überprüft auch die CRC-Zugriffsschutzinformationen, wenn Daten von dem Band gelesen werden.

Der Standardwert ist NO.

Die folgenden Werte sind gültig:

### READWrite

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect und dem Bandlaufwerk erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen. Der Wert READWRITE hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

Wird der Parameter LBPROTECT auf READWRITE gesetzt, müssen Sie nicht den Parameter CRCDATA in einer Speicherpooldefinition angeben, da der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust bereitstellt.

### WRITEOnly

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk nur für Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Für Leseoperationen überprüfen der Server und das Bandlaufwerk nicht die CRC-Informationen. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect zum Generieren der CRC-Informationen und für das Bandlaufwerk zum Berechnen und Vergleichen der CRC-Werte für Schreiboperationen erforderlich ist. Der Wert WRITEONLY hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

### No

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen nicht aktiviert ist. Der Server aktiviert jedoch den Schutz logischer Blöcke bei Schreiboperationen für einen sich füllenden Datenträger, der bereits über Daten mit dem Schutz logischer Blöcke verfügt.

Einschränkung: Der Schutz logischer Blöcke wird nur für IBM® 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher unterstützt.

In Technote 1634851, Additional information on the IBM Spectrum Protect LBProtect option, wird erläutert, wann der Parameter LBProtect zu verwenden ist.

## WORM

Gibt an, ob die Laufwerke WORM-Datenträger (Write Once, Read Many) verwenden. Dieser Parameter ist wahlfrei. Der Standardwert ist No. Das Feld kann einen der folgenden Werte enthalten:

### Yes

Gibt an, dass die Laufwerke WORM-Datenträger verwenden.

### No

Gibt an, dass die Laufwerke keine WORM-Datenträger verwenden.

### Hinweis:

1. Um die 3592-WORM-Unterstützung in 3584-Kassettenarchiven zu verwenden, müssen Sie den WORM-Parameter angeben. Der Server unterscheidet zwischen WORM- und Nicht-WORM-Arbeitsdatenträgern. Soll jedoch die 3592-WORM-Unterstützung in 349X-Kassettenarchiven verwendet werden, müssen Sie auch WORMSCRATCHCATEGORY im Befehl DEFINE LIBRARY definieren. Ausführliche Informationen siehe DEFINE LIBRARY (Kassettenarchiv definieren).
2. Bei WORM=Yes ist der einzige gültige Wert für den Parameter SCALECAPACITY der Wert 100.
3. Stellen Sie zusammen mit Ihren Hardwarelieferanten sicher, dass sich Ihre Hardware auf der entsprechenden Unterstützungsstufe befindet.

## SCALECAPacity

Gibt den Prozentsatz der Datenträgerkapazität an, der zum Speichern von Daten verwendet werden kann. Dieser Parameter ist wahlfrei. Der Standardwert ist 100. Gültige Werte sind 20, 90 oder 100.

Wird für SCALECAPacity der Wert 100 angegeben, wird die maximale Speicherkapazität zur Verfügung gestellt. Wird der Wert 20 angegeben, wird die schnellste Zugriffszeit zur Verfügung gestellt.

Anmerkung: Der Wert für SCALECAPacity wird nur wirksam, wenn Daten zum ersten Mal auf einen Datenträger geschrieben werden. Alle Aktualisierungen an der Einheitenklasse für SCALECAPacity haben erst dann Auswirkungen auf Datenträger, auf die bereits Daten geschrieben wurden, wenn die Datenträger wieder in den Arbeitsdatenträgerstatus versetzt werden.

#### FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Geben Sie stattdessen das Format an, das die Laufwerke verwenden.

In der folgenden Tabelle sind die Aufzeichnungsformate, die geschätzten Kapazitäten und die Optionen der Aufzeichnungsformate für 3592-Einheiten aufgelistet.

Tipp: Der Formatname wird beispielsweise als 3592-X, 3592-XC, 3592-XA oder 3592-XAC angegeben. Dabei gibt X die Laufwerkgeneration, C ein komprimiertes Format und A ein Archivierungslaufwerk an.

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für 3592

| Format  | Geschätzte Kapazität | Beschreibung   |
|---|----------------------|--|
| DRIVE   | –                    | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| 3592  | 300 GB               | Dekomprimiertes (Basis-)Format   |
| 3592C   | Siehe Anmerkung.     | Komprimiertes Format   |
| 3592-2  | 500 GB               | JA-Bänder mit dekomprimiertem (Basis-)Format   |
|   | 700 GB               | JB-Bänder mit dekomprimiertem (Basis-)Format   |
| 3592-2C   | 1,5 TB               | JA-Bänder mit komprimiertem Format   |
|   | 2,1 TB               | JB-Bänder mit komprimiertem Format   |
| 3592-3  | 640 GB               | JA-Bänder mit dekomprimiertem (Basis-)Format   |
|   | 1 TB                 | JB-Bänder mit dekomprimiertem (Basis-)Format   |
| 3592-3C   | 1,9 TB               | JA-Bänder mit komprimiertem Format   |
|   | 3 TB                 | JB-Bänder mit komprimiertem Format   |
| 3592-4  | 400 GB               | JK-Bänder mit dekomprimiertem (Basis-)Format   |
|   | 1,5 TB               | JB-Bänder mit dekomprimiertem (Basis-)Format   |
|   | 3,1 TB               | JC-Bänder mit dekomprimiertem (Basis-)Format   |
| 3592-4C   | 1,2 TB               | JK-Bänder mit komprimiertem Format   |
|   | 4,4 TB               | JB-Bänder mit komprimiertem Format   |
|   | 9,4 TB               | JC-Bänder mit komprimiertem Format   |
| 3592-5<br>(Für IBM TS1150 Modell<br>3592 E08-Laufwerke<br>mit Produkt-ID<br>03592E08) | 900 GB               | JK-Bänder mit dekomprimiertem (Basis-)Format   |
|   | 7000 GB              | JC/JY-Bänder mit dekomprimiertem (Basis-)Format  |
|   | 2000 GB              | JL-Bänder mit dekomprimiertem (Basis-)Format   |
|   | 10.000 GB            | JD/JZ-Bänder mit dekomprimiertem (Basis-)Format  |

| Format   | Geschätzte Kapazität                               | Beschreibung   |
|--|--|--|
| 3592-5C<br><br>(Für IBM TS1150 Modell<br>3592 E08-Laufwerke<br>mit Produkt-ID<br>03592E08)   | Hängt von der<br>Komprimierbarkeit der<br>Daten ab | JK-Bänder mit komprimiertem Format<br><br>JC/JY-Bänder mit komprimiertem Format<br><br>JL-Bänder mit komprimiertem Format<br><br>JD/JZ-Bänder mit komprimiertem Format |
| 3592-5A<br><br>(Für IBM TS1155 Modell<br>3592 55F-Laufwerke<br>mit Produkt-ID<br>0359255F)   | 3000 GB<br><br>15.000 GB                           | JL-Bänder mit dekomprimiertem (Basis-)Format<br><br>JD/JZ-Bänder mit dekomprimiertem (Basis-)Format  |
| 3592-5AC<br><br>(Für IBM TS1155 Modell<br>3592 55F-Laufwerke<br>mit Produkt-ID<br>0359255F)  | Hängt von der<br>Komprimierbarkeit der<br>Daten ab | JL-Bänder mit komprimiertem Format<br><br>JD/JZ-Bänder mit komprimiertem Format  |
| Anmerkung: Verwendet dieses Format die Komprimierungsfunktion für Bandlaufwerke, kann je nach Effektivität der Komprimierung die tatsächliche Kapazität von der geschätzten Kapazität abweichen. |  |  |

Wichtig: Um eine optimale Leistung zu erzielen, sollte das Mischen von Laufwerken verschiedener Generationen in einem einzelnen SCSI-Kassettenarchiv vermieden werden. Müssen Sie Laufwerkgenerationen in einem SCSI-Kassettenarchiv mischen, verwenden Sie eine der speziellen Konfigurationen, die in dem Abschnitt zum Mischen von Generationen von 3592-Datenträgern beschrieben sind.

Spezielle Konfigurationen sind auch erforderlich, wenn verschiedene Generationen von 3592-Laufwerken in 349x- und ACSLS-Kassettenarchiven gemischt werden.

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

#### DRIVEEncryption

Gibt an, ob die Laufwerkverschlüsselung zulässig ist. Dieser Parameter ist wahlfrei. Der Standardwert ist ALLOW.

#### ON

Gibt an, dass IBM Spectrum Protect der Schlüsselmanager für die Laufwerkverschlüsselung ist und die Laufwerkverschlüsselung für leere Speicherpooledatenträger nur erlaubt, wenn das Anwendungsverfahren aktiviert ist. (Andere Typen von Datenträgern, wie beispielsweise Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger, werden nicht verschlüsselt.) Wird ON angegeben und entweder das Kassettenarchivverfahren oder das Systemverfahren der Verschlüsselung aktiviert, ist die Laufwerkverschlüsselung nicht zulässig, und Sicherungsoperationen schlagen fehl.

#### ALLOW

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Die Laufwerkverschlüsselung für leere Datenträger ist jedoch erlaubt, wenn entweder das Kassettenarchivverfahren oder das Systemverfahren der Verschlüsselung aktiviert ist.

#### EXTERNAL

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Verwenden Sie diese Einstellung mit einer Verschlüsselungsmethodik, die von einem anderen Anbieter zur Verfügung gestellt wird und die mit dem Anwendungsverfahren der Verschlüsselung verwendet wird, das für das Laufwerk aktiviert ist.

Geben Sie EXTERNAL an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect nicht inaktiviert.



Geben Sie dagegen ALLOW an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect inaktiviert.

OFF

Gibt an, dass die Laufwerkverschlüsselung nicht zulässig ist. Wird entweder das Kassettenarchivverfahren oder das Systemverfahren der Verschlüsselung aktiviert, schlagen Sicherungen fehl. Wird das Anwendungsverfahren aktiviert, inaktiviert IBM Spectrum Protect die Verschlüsselung, und die Ausführung von Sicherungen wird versucht.

## DEFINE DEVCLASS (Einheitenklasse 4MM definieren)

Verwenden Sie die Einheitenklasse 4MM, wenn Sie 4-mm-Bandeinheiten verwenden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-DEFine DEVclass--Einheitenklassenname----->
>--LIBRARY----Kassettenarchivname--DEVType----4MM----->
. -FORMAT-----DRIVE----- .
>+-----+-----+-----+-----+----->
' -FORMAT-----+DRIVE--+' ' -ESTCAPacity---Größe-'
      +-DDS1--+
      +-DDS1C+
      +-DDS2--+
      +-DDS2C+
      +-DDS3--+
      +-DDS3C+
      +-DDS4--+
      +-DDS4C+
      +-DDS5--+
      +-DDS5C+
      +-DDS6--+
      '-DDS6C-'

. -PREFIX-----ADSM----- .
>+-----+-----+-----+-----+----->
' -PREFIX-----+ADSM-----+'
      '-Banddatenträgerpräfix-'

. -MOUNTWait----60----- . -MOUNTRetention----60----- .
>+-----+-----+-----+-----+----->
' -MOUNTWait----Minuten-' ' -MOUNTRetention----Minuten-'

. -MOUNTLimit----DRIVES----- .
>+-----+-----+-----+-----+-----><
' -MOUNTLimit----+DRIVES--+'
      +-Anzahl+
      '-0-----'
```

### Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRARY (Erforderlich)

Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten 4-mm-Bandlaufwerke enthält. Informationen über die Definition eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

DEVType=4MM (Erforderlich)

Gibt an, dass der Einheitentyp 4MM der Einheitenklasse zugeordnet wird. 4MM bedeutet, dass dieser Einheitenklasse 4-mm-Bandeinheiten zugeordnet werden.

FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Geben Sie stattdessen das Format an, das die Laufwerke verwenden.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für 4-mm-Einheiten aufgelistet:

**Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für 4-mm-Bänder**

| Format   | Geschätzte Kapazität                                      | Beschreibung   |
|--|---|--|
| DRIVE  | –   | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| DDS1   | 2,6 GB (60 Meter)<br>4,0 GB (90 Meter)                    | Dekomprimiertes Format, gilt nur für 60-Meter-Bänder und 90-Meter-Bänder   |
| DDS1C  | Siehe Anmerkung<br>1,3 GB (60 Meter)<br>2,0 GB (90 Meter) | Komprimiertes Format, gilt nur für 60-Meter-Bänder und 90-Meter-Bänder   |
| DDS2   | 4,0 GB  | Dekomprimiertes Format, gilt nur für 120-Meter-Bänder  |
| DDS2C  | Siehe Anmerkung<br>8,0 GB                                 | Komprimiertes Format, gilt nur für 120-Meter-Bänder  |
| DDS3   | 12,0 GB   | Dekomprimiertes Format, gilt nur für 125-Meter-Bänder  |
| DDS3C  | Siehe Anmerkung<br>24,0 GB                                | Komprimiertes Format, gilt nur für 125-Meter-Bänder  |
| DDS4   | 20,0 GB   | Dekomprimiertes Format, gilt nur für 150-Meter-Bänder  |
| DDS4C  | Siehe Anmerkung<br>40,0 GB                                | Komprimiertes Format, gilt nur für 150-Meter-Bänder  |
| DDS5   | 36 GB   | Dekomprimiertes Format bei Verwendung von DAT 72-Datenträgern  |
| DDS5C  | Siehe Anmerkung<br>72 GB                                  | Komprimiertes Format bei Verwendung von DAT 72-Datenträgern  |
| DDS6   | 80 GB   | Dekomprimiertes Format bei Verwendung von DAT 160-Datenträgern   |
| DDS6C  | Siehe Anmerkung<br>160 GB                                 | Komprimiertes Format bei Verwendung von DAT 160-Datenträgern   |
| Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann die tatsächliche Kapazität abhängig von der Effektivität der Komprimierung größer als der aufgelistete Wert sein. |   |  |

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Für weitere Informationen zur geschätzten Standardkapazität für 4-mm-Bänder siehe Tabelle 1.

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist AD5M. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

## DEFINE DEVCLASS (Einheitenklasse 8MM definieren)

Verwenden Sie die Einheitenklasse 8MM, wenn Sie 8-mm-Bandseinheiten verwenden.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-DEFine DEVclass--Einheitenklassenname----->
--LIBRARY----Kassettenarchivname--DEVType----8MM----->
. -WORM----No----- . -FORMAT----DRIVE-----
>+-----+-----+-----+-----+-----+----->
' -WORM----+No--+ ' ' -FORMAT----+DRIVE--+ '
      '-Yes- '                +-8200--+
                                +-8200C--+
                                +-8500--+
                                +-8500C--+
                                +-8900--+
                                +-AIT--+
                                +-AITC--+
                                +-M2----+
                                +-M2C---+
                                +-SAIT--+
                                +-SAITC--+
                                +-VXA2--+
                                +-VXA2C--+
                                +-VXA3--+
                                '-VXA3C-'

>+-----+-----+-----+-----+-----+----->
' -ESTCAPacity----Größe- '

. -PREFIX----ADSM-----
>+-----+-----+-----+-----+-----+----->
' -PREFIX----+ADSM-----+-'
      '-Banddatenträgerpräfix- '

. -MOUNTRetention----60----- . -MOUNTWait----60-----
>+-----+-----+-----+-----+-----+----->
' -MOUNTRetention----Minuten- ' ' -MOUNTWait----Minuten- '

. -MOUNTLimit----DRIVES-----
>+-----+-----+-----+-----+-----+----->
' -MOUNTLimit----+DRIVES--+ '
      +-Anzahl+
      '-0-----'


```

## Parameter

### Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

### LIBRARY (Erforderlich)

Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten 8-mm-Bandlaufwerke enthält. Informationen über die Definition eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

### DEVType=8MM (Erforderlich)

Gibt an, dass der Einheitentyp 8MM der Einheitenklasse zugeordnet wird. 8MM bedeutet, dass dieser Einheitenklasse 8-mm-Bandeinheiten zugeordnet werden.

### WORM

Gibt an, ob die Laufwerke WORM-Datenträger (Write Once, Read Many) verwenden. Dieser Parameter ist wahlfrei. Der Standardwert ist No. Das Feld kann einen der folgenden Werte enthalten:

#### Yes

Gibt an, dass die Laufwerke WORM-Datenträger verwenden.

#### No

Gibt an, dass die Laufwerke keine WORM-Datenträger verwenden.

Anmerkung: Wird Yes ausgewählt, sind nur die folgenden Optionen für den Parameter FORMAT verfügbar:

- DRIVE

- AIT
- AITC

## FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Geben Sie stattdessen das Format an, das die Laufwerke verwenden.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für 8-mm-Einheiten aufgelistet:

**Tabelle 1. Aufzeichnungsformat und geschätzte Standardkapazität für 8-mm-Band**

| <b>Format</b>         |                                     | <b>Beschreibung</b>   |
|-----------------------|-------------------------------------|---|
| <b>Datenträgertyp</b> | <b>Geschätzte Kapazität</b>         |   |
| DRIVE                 | –                                   | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| 8200                  | 2,3 GB                              | Dekomprimiertes (Standard) Format, verwendet 112-Meter-Standardbandkassetten  |
| 8200C                 | Siehe Anmerkung<br>3,5 GB<br>4,6 GB | Komprimiertes Format, verwendet 112-Meter-Standardbandkassetten   |
| 8500                  | Siehe Anmerkung                     | Laufwerke (Lesen/Schreiben)   |
| 15 m                  | 600 MB                              | Eliant 820 (LS)   |
| 15 m                  | 600 MB                              | Exabyte 8500/8500C (LS)   |
| 15 m                  | 600 MB                              | Exabyte 8505 (LS)   |
| 54 m                  | 2,35 GB                             | Eliant 820 (LS)   |
| 54 m                  | 2,35 GB                             | Exabyte 8500/8500C (LS)   |
| 54 m                  | 2,35 GB                             | Exabyte 8505 (LS)   |
| 112 m                 | 5 GB oder 10,0 GB                   | Eliant 820 (LS)   |
| 112 m                 | 5 GB oder 10,0 GB                   | Exabyte 8500/8500C (LS)   |
| 112 m                 | 5 GB oder 10,0 GB                   | Exabyte 8505 (LS)   |
| 160 m XL              | 7 GB                                | Eliant 820 (LS)   |
| 8500C                 | Siehe Anmerkung                     | Laufwerke (Lesen/Schreiben)   |
| 15 m                  | 1,2 GB                              | Eliant 820 (LS)   |
| 15 m                  | 1,2 GB                              | Exabyte 8500/8500C (LS)   |
| 15 m                  | 1,2 GB                              | Exabyte 8505 (LS)   |
| 54 m                  | 4,7 GB                              | Eliant 820 (LS)   |
| 54 m                  | 4,7 GB                              | Exabyte 8500/8500C (LS)   |
| 54 m                  | 4,7 GB                              | Exabyte 8505 (LS)   |
| 112 m                 | 5 GB oder 10,0 GB                   | Eliant 820 (LS)   |
| 112 m                 | 5 GB oder 10,0 GB                   | Exabyte 8500/8500C (LS)   |
| 112 m                 | 5 GB oder 10,0 GB                   | Exabyte 8505 (LS)   |
| 160 m XL              | 7 GB                                | Eliant 820 (LS)   |
| 8900                  | Siehe Anmerkung                     | Laufwerk (Lesen/Schreiben)  |
| 15 m                  | ----2,5 GB                          | Mammoth 8900 (L)  |
| 54 m                  | –40 GB                              | Mammoth 8900 (L)  |
| 112 m                 |                                     | Mammoth 8900 (L)  |
| 160 m XL              |                                     | Mammoth 8900 (L)  |
| 22 m                  |                                     | Mammoth 8900 (LS)   |
| 125 m                 |                                     | Mammoth 8900 (LS mit Upgrade)   |
| 170 m                 |                                     | Mammoth 8900 (LS)   |

| <b>Format</b>         |                             | <b>Beschreibung</b>                |
|-----------------------|-----------------------------|------------------------------------|
| <b>Datenträgertyp</b> | <b>Geschätzte Kapazität</b> |                                    |
| AIT                   | Siehe Anmerkung             | Laufwerk                           |
| SDX1–25C              | 25 GB                       | AIT-, AIT2- und AIT3-Laufwerke     |
| SDX1–35C              | 35 GB                       | AIT-, AIT2- und AIT3-Laufwerke     |
| SDX2–36C              | 36 GB50 GB                  | AIT2- und AIT3-Laufwerke           |
| SDX2–50C              | 100 GB150 GB200 GB400       | AIT2- und AIT3-Laufwerke           |
| SDX3–100C             | GB                          | AIT3-, AIT4- und AIT5-Laufwerke    |
| SDX3X-150C            |                             | AIT3-Ex-, AIT4- und AIT5-Laufwerke |
| SDX4–200C             |                             | AIT4- und AIT5-Laufwerke           |
| SDX5-400C             |                             | AIT5-Laufwerk                      |
| AITC                  | Siehe Anmerkung             | Laufwerk                           |
| SDX1–25C              | 50 GB                       | AIT-, AIT2- und AIT3-Laufwerke     |
| SDX1–35C              | 91 GB                       | AIT-, AIT2- und AIT3-Laufwerke     |
| SDX2–36C              | 72 GB130 GB                 | AIT2- und AIT3-Laufwerke           |
| SDX2–50C              | 260 GB                      | AIT2- und AIT3-Laufwerke           |
| SDX3–100C             | 390 GB                      | AIT3-, AIT4- und AIT5-Laufwerke    |
| SDX3X-150C            | 520 GB                      | AIT3-Ex-, AIT4- und AIT5-Laufwerke |
| SDX4–200C             | 1040 GB                     | AIT4- und AIT5-Laufwerke           |
| SDX5-400C             |                             | AIT5-Laufwerk                      |
| M2                    | Siehe Anmerkung             | Laufwerk (Lesen/Schreiben)         |
| 75 m                  | 20,0 GB40,0 GB60,0 GB       | Mammoth II (LS)                    |
| 150 m                 |                             | Mammoth II (LS)                    |
| 225 m                 |                             | Mammoth II (LS)                    |
| M2C                   | Siehe Anmerkung             | Laufwerk (Lesen/Schreiben)         |
| 75 m                  | 50,0 GB                     | Mammoth II (LS)                    |
| 150 m                 | 100,0 GB                    | Mammoth II (LS)                    |
| 225 m                 | 150,0 GB                    | Mammoth II (LS)                    |
| SAIT                  | Siehe Anmerkung             | Laufwerk (Lesen/Schreiben)         |
|                       | 500 GB                      | Sony SAIT1–500 (LS)                |
| SAITC                 | Siehe Anmerkung             | Laufwerk (Lesen/Schreiben)         |
|                       | 1300 GB (1,3 TB)            | Sony SAIT1–500 (LS)                |
| VXA2                  | Siehe Anmerkung             | Laufwerk (Lesen/Schreiben)         |
| V6 (62 m)             | 20 GB40 GB60 GB             | VXA–2                              |
| V10 (124 m)           |                             |                                    |
| V17 (170 m)           |                             |                                    |
| VXA2C                 | Siehe Anmerkung             | Laufwerk (Lesen/Schreiben)         |
| V6 (62 m)             | 40 GB80 GB120 GB            | VXA–2                              |
| V10 (124 m)           |                             |                                    |
| V17 (170 m)           |                             |                                    |
| VXA3                  | Siehe Anmerkung             | Laufwerk (Lesen/Schreiben)         |
| X6 (62 m)             | 40 GB86 GB                  | VXA–3                              |
| X10 (124 m)           | 160 GB                      |                                    |
| X23 (230 m)           |                             |                                    |
| VXA3C                 | Siehe Anmerkung             | Laufwerk (Lesen/Schreiben)         |
| X6 (62 m)             | 80 GB172 GB                 | VXA–3                              |
| X10 (124 m)           | 320 GB                      |                                    |
| X23 (230 m)           |                             |                                    |

| Format   |                      | Beschreibung |
|--|----------------------|--------------|
| Datenträgertyp   | Geschätzte Kapazität |              |
| Anmerkung: Die tatsächlichen Kapazitäten können abhängig von den verwendeten Kassetten und Laufwerken variieren.   |                      |              |
| <ul style="list-style-type: none"> <li>• Für das M2C-Format ist das normale Komprimierungsverhältnis 2,5:1.</li> <li>• Für das AITC- und SAITC-Format ist das normale Komprimierungsverhältnis 2,6:1.</li> </ul> |                      |              |

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Für weitere Informationen zur geschätzten Standardkapazität für 8-mm-Bänder siehe Tabelle 1.

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

## MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

## Beispiel: Eine 8-mm-Einheitenklasse definieren

---

Die Einheitenklasse 8MMTAPE für eine 8-mm-Einheit in dem Kassettenarchiv AUTO definieren. Das Format ist DRIVE, Grenzwert für Ladeanforderungen 2, Ladedauer ist 10, Banddatenträgerpräfix lautet ADSMVOL und die geschätzte Kapazität beträgt 6 GB.

```
define devclass 8mmtape devtype=8mm library=auto
format=drive mountlimit=2 mountretention=10
prefix=adsmvol estcapacity=6G
```

## DEFINE DEVCLASS (Einheitenklasse CENTERA definieren)

---

Verwenden Sie die Einheitenklasse CENTERA, wenn Sie EMC Centera-Speichereinheiten verwenden. Der Einheitentyp CENTERA verwendet Dateien als Datenträger zum sequenziellen Speichern von Daten. Er ähnelt der Einheitenklasse FILE.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
>>-DEFine DEVclass--Einheitenklassenname--DEVType-----CENTERA--->
      .-,-----
      (1)  v      |
>--HLAddress-----ID-Adresse-+-?PEA-Datei----->
      .-MINCapacity-----100M--.  .-MOUNTLimit-----1-----
>+-----+-----+-----+-----<
  '-MINCapacity-----Größe-'  '-MOUNTLimit-----Anzahl-'
```

Anmerkungen:

1. Für jede Centera-Einheitenklasse müssen Sie mindestens eine IP-Adresse angeben. Ein PEA-Dateiname und -Pfad (PEA = Pool Entry Authorization) sind jedoch optional, und maximal eine PEA-Dateispezifikation kann auf die IP-Adressen folgen. Verwenden Sie das Zeichen "?", um den PEA-Dateinamen und -Pfad von den IP-Adressen zu trennen.

## Parameter

---

Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.


DEVType=CENTERA (Erforderlich)




Gibt an, dass der Einheitentyp Centera dieser Einheitenklasse zugeordnet wird. Alle Datenträger, die zu einem Speicherpool gehören, der für diese Einheitenklasse definiert ist, sind logische Datenträger, die eine Art von Datenträger mit sequenziellem Zugriff sind.

#### HLAddress

Gibt mindestens eine IP-Adresse für die Centera-Speichereinheit und optional den Namen und Pfad einer PEA-Datei (PEA = Pool Entry Authorization) an. Geben Sie die IP-Adressen in Schreibweise mit Trennzeichen an (beispielsweise 9.10.111.222). Eine Centera-Einheit kann mehrere IP-Adressen haben. Werden mehrere IP-Adressen angegeben, wird bei der Speicher- oder Abrufoperation versucht, eine Verbindung mit jeder angegebenen IP-Adresse herzustellen, bis eine gültige Adresse gefunden wird.

 Bei dem PEA-Dateinamen und -Pfadnamen muss die Groß-/Kleinschreibung beachtet werden.

Werden Name und Pfad einer PEA-Datei angehängt, stellen Sie sicher, dass die Datei in einem Verzeichnis auf dem System gespeichert wird, auf dem der Server ausgeführt wird. Verwenden Sie das Zeichen "?", um den PEA-Dateinamen und -Pfad von der IP-Adresse zu trennen. Beispiel:  Windows-Betriebssysteme

```
HLADDRESS=9.10.111.222,9.10.111.223?c:\controlFiles\TSM.PEA
```

 AIX-Betriebssysteme

```
HLADDRESS=9.10.111.222,9.10.111.223?/user/ControlFiles/TSM.PEA
```

Geben Sie nur einen PEA-Dateinamen und Pfad für jede Einheitenklassendefinition an. Geben Sie zwei verschiedene Centera-Einheitenklassen an, die auf dieselbe Centera-Speichereinheit zeigen, und enthalten die Einheitenklassendefinitionen verschiedene PEA-Dateinamen und -Pfade, verwendet der Server die PEA-Datei, die im Einheitenklassenparameter HLADDRESS angegeben ist, der zuerst zum Öffnen der Centera-Speichereinheit verwendet wurde.

Tipps:

1. Der Server schließt während der Installation keine PEA-Datei ein. Wenn Sie keine PEA-Datei erstellen, verwendet der Server das Centera-Standardprofil, mit dem es Anwendungen erlaubt werden kann, Daten auf einer Centera-Speichereinheit zu lesen, zu schreiben, zu löschen und abzufragen. Um eine genauere Steuerung zu ermöglichen, erstellen Sie eine PEA-Datei mit der Befehlszeilenschnittstelle, die von EMC Centera zur Verfügung gestellt wird. Ausführliche Informationen zur Centera-Authentifizierung und -Berechtigung befinden sich im EMC Centera *Programmer's Guide*.
2. Sie können den PEA-Dateinamen und -Pfad auch in einer Umgebungsvariablen mit der Syntax `CENTERA_PEA_LOCATION=Dateipfad_Dateiname` angeben. Der mit dieser Umgebungsvariablen angegebene PEA-Dateiname und -Pfad gilt für alle Centera-Cluster. Wird diese Variable verwendet, müssen Sie keinen PEA-Dateinamen und -Pfad mit dem Parameter HLADDRESS angeben.

#### MINCAPacity

Gibt die Mindestgröße für Centera-Datenträger an, die einem Speicherpool in dieser Einheitenklasse zugeordnet sind. Dieser Wert stellt das Mindestdatenvolumen dar, das auf einem Centera-Datenträger gespeichert wird, bevor der Server den Datenträger als voll kennzeichnet. Centera-Datenträger akzeptieren weiterhin Daten, bis das Mindestdatenvolumen gespeichert wurde. Dieser Parameter ist wahlfrei.

Dieser Wert muss als ganze Zahl gefolgt von einem **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte) angegeben werden. Der Standardwert ist 100 MB (MINCAPACITY=100M). Der zulässige Mindestwert ist 1 MB (MINCAPACITY=1M). Der zulässige Maximalwert ist 128 GB (MINCAPACITY=128G).

#### MOUNTLimit

Gibt die maximale Anzahl von Dateien an, die gleichzeitig für die Ein- und Ausgabe geöffnet sein kann. Der Standardwert ist 1. Dieser Parameter ist optional. Sie können eine beliebige Zahl von 0 aufwärts angeben; die Summe aller Grenzwerte für Ladeanforderungen für alle Einheitenklassen, die derselben Centera-Einheit zugeordnet sind, darf jedoch die maximale Anzahl der von Centera erlaubten Sitzungen nicht überschreiten.

## DEFINE DEVCLASS (Einheitenklasse DLT definieren)

---

Verwenden Sie die Einheitenklasse DLT, wenn Sie DLT-Bandeinheiten verwenden.

### Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

---

```
>>-DEFine DEVclass--Einheitenklassenname----->
```



Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Geben Sie stattdessen das Format an, das die Laufwerke verwenden.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für DLT-Einheiten aufgelistet:

**Tabelle 1. Aufzeichnungsformat und geschätzte Standardkapazität für DLT**

| <b>Format</b> | <b>Geschätzte Kapazität</b> | <b>Beschreibung</b>  |
|---------------|-----------------------------|--|
| DRIVE         | –                           | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| DLT1          | 40,0 GB                     | Dekomprimiertes Format, verwendet nur CompacTape III-Kassetten<br>Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke  |
| DLT1C         | Siehe 1.<br>80,0 GB         | Komprimiertes Format, verwendet nur CompacTape III-Kassetten<br>Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke  |
| DLT10         | 10,0 GB                     | Dekomprimiertes Format, verwendet nur CompacTape III-Kassetten<br>Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke  |
| DLT10C        | Siehe 1.<br>20,0 GB         | Komprimiertes Format, verwendet nur CompacTape III-Kassetten<br>Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke  |
| DLT15         | 15,0 GB                     | Dekomprimiertes Format, verwendet nur CompacTape IIIxt-Kassetten<br>Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke  |
| DLT15C        | Siehe 1.<br>30,0 GB         | Komprimiertes Format, verwendet nur CompacTape IIIxt-Kassetten<br>Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke  |
| DLT20         | 20,0 GB                     | Dekomprimiertes Format, verwendet nur CompacTape IV-Kassetten<br>Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke   |
| DLT20C        | Siehe 1.<br>40,0 GB         | Komprimiertes Format, verwendet nur CompacTape IV-Kassetten<br>Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke   |
| DLT35         | 35,0 GB                     | Dekomprimiertes Format, verwendet nur CompacTape IV-Kassetten<br>Gültig für DLT7000- und DLT8000-Laufwerke   |
| DLT35C        | Siehe 1.<br>70,0 GB         | Komprimiertes Format, verwendet nur CompacTape IV-Kassetten<br>Gültig für DLT7000- und DLT8000-Laufwerke   |
| DLT40         | 40,0 GB                     | Dekomprimiertes Format, verwendet CompacTape IV-Kassetten<br>Gültig für DLT8000-Laufwerk   |
| DLT40C        | Siehe 1.<br>80,0 GB         | Komprimiertes Format, verwendet CompacTape IV-Kassetten<br>Gültig für DLT8000-Laufwerk   |
| DLT2          | 80,0 GB                     | Dekomprimiertes Format, verwendet Quantum DLT VS1-Banddatenträger  |
| DLT2C         | Siehe 1.<br>160,0 GB        | Komprimiertes Format, verwendet Quantum DLT VS1-Banddatenträger  |
| DLT4          | 160,0 GB                    | Dekomprimiertes Format, verwendet Quantum DLTtape VS1-Kassetten.<br>Gültig für Quantum DLT-V4-Laufwerk   |
| DLT4C         | Siehe 1.<br>320,0 GB        | Komprimiertes Format, verwendet Quantum DLTtape VS1-Kassetten.<br>Gültig für Quantum DLT-V4-Laufwerk   |

| Format  | Geschätzte Kapazität | Beschreibung  |
|---|----------------------|---|
| SDLT<br>Siehe 2.  | 100,0 GB             | Dekomprimiertes Format, verwendet Super DLT Tape 1-Kassetten<br><br>Gültig für Super DLT-Laufwerk   |
| SDLTC<br>Siehe 2.   | Siehe 1.<br>200,0 GB | Komprimiertes Format, verwendet Super DLT Tape 1-Kassetten<br><br>Gültig für Super DLT-Laufwerk     |
| SDLT320<br>Siehe 2.   | 160,0 GB             | Dekomprimiertes Format, verwendet Quantum SDLT I-Datenträger<br><br>Gültig für Super DLT-Laufwerk   |
| SDLT320C<br>Siehe 2.  | Siehe 1.<br>320,0 GB | Komprimiertes Format, verwendet Quantum SDLT I-Datenträger<br><br>Gültig für Super DLT-Laufwerk     |
| SDLT600   | 300,0 GB             | Dekomprimiertes Format, verwendet SuperDLTtape-II-Datenträger<br><br>Gültig für Super DLT-Laufwerk  |
| SDLT600C  | Siehe 1.<br>600,0 GB | Komprimiertes Format, verwendet SuperDLTtape-II-Datenträger<br><br>Gültig für Super DLT-Laufwerk    |
| DLTS4   | 800 GB               | Dekomprimiertes Format, verwendet Quantum DLT S4-Datenträger.<br><br>Gültig für ein DLT-S4-Laufwerk |
| DLTS4C  | Siehe 1.<br>1,6 TB   | Komprimiertes Format, verwendet Quantum DLT S4-Datenträger.<br><br>Gültig für ein DLT-S4-Laufwerk   |
| Anmerkung:<br><br><ol style="list-style-type: none"> <li>1. Je nach Effektivität der Komprimierung kann die tatsächliche Kapazität größer als der aufgeführte Wert sein.</li> <li>2. IBM Spectrum Protect unterstützt kein Kassettenarchiv, das sowohl Backward Read Compatible (BRC) SDLT- als auch Non-Backward Read Compatible (NBRC) SDLT-Laufwerke enthält.</li> </ol> |                      |   |

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Für weitere Informationen zu geschätzten Kapazitäten siehe Tabelle 1.

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

## MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

## MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

## MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.



### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

## DEFINE DEVCLASS (Einheitenklasse ECARTRIDGE definieren)

---

Verwenden Sie die Einheitenklasse ECARTRIDGE, wenn Sie StorageTek-Laufwerke wie beispielsweise StorageTek T9840 oder T10000 verwenden.

  Wenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in DEFINE DEVCLASS (Einheitenklasse ECARTRIDGE für z/OS Media-Server definieren).

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
>>-DEFine DEVclass--Einheitenklassenname----->
```

```

>--LIBRARY-----Kassettenarchivname--DEVType-----ECARTridge----->

                                (1)
.-LBProtect-----No-----, .-WORM-----No-----.
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-LBProtect-----+READWrite+-' '-WORM-----+No--+-'
      +-WRITEOnly+-          '-Yes-'
      '-No-----'

.-FORMAT-----DRIVE-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-FORMAT-----+DRIVE-----+' '-ESTCAPacity-----Größe-'
      +-T9840C-----+
      +-T9840C-C--+
      +-T9840D-----+
      +-T9840D-C--+
      +-T10000A-----+
      +-T10000A-C+
      +-T10000B-----+
      +-T10000B-C+
      +-T10000C-----+
      +-T10000C-C+
      +-T10000D-----+
      '-T10000D-C-'

.-PREFIX-----ADSM-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-PREFIX-----+ADSM-----+'
      '-Banddatenträgerpräfix-'

.-MOUNTRetention-----60-----, .-MOUNTWait-----60-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-MOUNTRetention-----+Minuten-' '-MOUNTWait-----+Minuten-'

.-MOUNTLimit-----DRIVES-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-MOUNTLimit-----+DRIVES+-'
      +-Anzahl+
      '-0-----'

                                (1) (2)
.-DRIVEEncryption-----ALLOW-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-DRIVEEncryption-----+ON-----+'
      +-ALLOW-----+
      +-EXTernal+
      '-OFF-----'

```

#### Anmerkungen:

1. Sie können nicht WORM=Yes in Verbindung mit DRIVEENCRYPTION=ON angeben.
2. Sie können die Laufwerkverschlüsselung nur für Oracle StorageTek T10000B-Laufwerke mit dem Formatwert DRIVE, T10000B oder T10000B-C, für Oracle StorageTek T10000C-Laufwerke mit dem Formatwert DRIVE, T10000C oder T10000C-C und für Oracle StorageTek T10000D-Laufwerke mit dem Formatwert DRIVE, T10000D und T10000D-C verwenden.

## Parameter

#### Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

#### LIBRARY (Erforderlich)

Gibt den Namen des definierten Kassettenarchivobjekts an, das die Kassettenbandlaufwerke (ECARTRIDGE) enthält, die von dieser Einheitenklasse verwendet werden können. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

#### DEVType=ECARTridge (Erforderlich)

Gibt an, dass der Einheitentyp ECARTRIDGE der Einheitenklasse zugeordnet wird. ECARTRIDGE gibt an, dass ein bestimmter Typ von Magnetbandkassette (StorageTek) dieser Einheitenklasse zugeordnet ist.

#### LBProtect

Gibt an, ob der Schutz logischer Blöcke verwendet wird, um die Integrität von Daten sicherzustellen, die auf Band gespeichert sind. Wenn LBPROTECT auf READWRITE oder WRITEONLY gesetzt ist, verwendet der Server dieses Feature des Bandlaufwerks für den Schutz logischer Blöcke und generiert CRC-Zugriffsschutzinformationen für jeden Datenblock, der auf Band geschrieben wird. Der Server überprüft auch die CRC-Zugriffsschutzinformationen, wenn Daten von dem Band gelesen werden.

Der Standardwert ist NO.

Die folgenden Werte sind gültig:

#### READWrite

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect und dem Bandlaufwerk erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen. Der Wert READWRITE hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

Wird der Parameter LBPROTECT auf READWRITE gesetzt, müssen Sie nicht den Parameter CRCDATA in einer Speicherpooldefinition angeben, da der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust bereitstellt.

#### WRITEOnly

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk nur für Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Für Leseoperationen überprüfen der Server und das Bandlaufwerk nicht die CRC-Informationen. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect zum Generieren der CRC-Informationen und für das Bandlaufwerk zum Berechnen und Vergleichen der CRC-Werte für Schreiboperationen erforderlich ist. Der Wert WRITEONLY hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

#### No

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen nicht aktiviert ist. Der Server aktiviert jedoch den Schutz logischer Blöcke bei Schreiboperationen für einen sich füllenden Datenträger, der bereits über Daten mit dem Schutz logischer Blöcke verfügt.

Einschränkung: Der Schutz logischer Blöcke wird nur auf Oracle StorageTek T10000C- und Oracle StorageTek T10000D-Laufwerken unterstützt.

#### WORM

Gibt an, ob die Laufwerke WORM-Datenträger (Write Once, Read Many) verwenden. Dieser Parameter ist wahlfrei. Der Standardwert ist No. Das Feld kann einen der folgenden Werte enthalten:

#### Yes

Gibt an, dass die Laufwerke WORM-Datenträger verwenden.

#### No

Gibt an, dass die Laufwerke keine WORM-Datenträger verwenden.

Einschränkung: Wird Yes ausgewählt, sind nur die folgenden Optionen für den Parameter FORMAT verfügbar:

- DRIVE
- T9840C
- T9840C-C
- T9840D
- T9840D-C
- T10000A
- T10000A-C
- T10000B
- T10000B-C
- T10000C
- T10000C-C
- T10000D
- T10000D-C

#### FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Geben Sie stattdessen das Format an, das die Laufwerke verwenden.

Wichtig: Wird DRIVE für eine Einheitenklasse angegeben, die über inkompatible Einheiten mit sequenziellem Zugriff verfügt, müssen Datenträger in Einheiten geladen werden, die in dem Format lesen oder schreiben können, das beim ersten Laden des Datenträgers eingerichtet wurde. Dies kann zu Verzögerungen führen, wenn die einzige Einheit mit sequenziellem Zugriff, die auf den Datenträger zugreifen kann, bereits im Gebrauch ist.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für ECARTRIDGE-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für ECARTRIDGE-Bänder

| Format | Geschätzte Kapazität | Beschreibung |
|--------|----------------------|--------------|
|--------|----------------------|--------------|

| Format   | Geschätzte Kapazität | Beschreibung   |
|--|----------------------|--|
| DRIVE  | –                    | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| T9840C   | 40 GB                | Dekomprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840C-C   | 80 GB                | Komprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840D   | 75 GB                | Dekomprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840D-C   | 150 GB               | Komprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette   |
| T10000A  | 500 GB               | Dekomprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette  |
| T10000A-C  | 1 TB                 | Komprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette  |
| T10000B  | 1 TB                 | Dekomprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette   |
| T10000B-C  | 2 TB                 | Komprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette   |
| T10000C  | 5 TB                 | Dekomprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000C-C  | 10 TB                | Komprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000D  | 8 TB                 | Dekomprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000D-C  | 15 TB                | Komprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| Anmerkungen:   |                      |  |
| <ul style="list-style-type: none"> <li>Einige Formate verwenden die Datenkomprimierung über Hardware mittels Bandlaufwerk. Je nach Effektivität der Komprimierung kann die tatsächliche Kapazität doppelt so groß (oder größer) sein wie der aufgeführte Wert.</li> <li>T10000A-Laufwerke können nur das T10000A-Format lesen und schreiben. T10000B-Laufwerke können das T10000A-Format lesen, aber nicht schreiben. T10000C-Laufwerke können die T10000A- und T10000B-Formate lesen, aber nicht schreiben. T10000D-Laufwerke können die T10000A-, T10000B- und T10000C-Formate lesen, aber nicht schreiben.</li> </ul> |                      |  |

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:



- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

#### DRIVEEncryption

Gibt an, ob die Laufwerkverschlüsselung zulässig ist. Dieser Parameter ist wahlfrei. Der Standardwert ist ALLOW.

Einschränkungen:

1. Sie können die Laufwerkverschlüsselung nur für die folgenden Laufwerke verwenden:
  - Oracle StorageTek T10000B-Laufwerke, die den Formatwert DRIVE, T10000B oder T10000B-C haben
  - Oracle StorageTek T10000C-Laufwerke, die den Formatwert DRIVE, T10000C oder T10000C-C haben
  - Oracle StorageTek T10000D-Laufwerke, die den Formatwert DRIVE, T10000D oder T10000D-C haben

2. Sie können nicht IBM Spectrum Protect als Schlüsselmanager für die Laufwerkverschlüsselung von WORM-Datenträgern angeben (WORM - Write Once Read Many). Sie können nicht WORM=Yes in Verbindung mit DRIVEENCRYPTION=ON angeben.
3. Ist die Verschlüsselung für eine Einheitenklasse aktiviert und ist die Einheitenklasse einem Speicherpool zugeordnet, sollte der Speicherpool nicht einen Arbeitsdatenträgerpool mit anderen Einheitenklassen gemeinsam nutzen, die nicht verschlüsselt werden können. Ist ein Band verschlüsselt und soll das Band in einem Laufwerk verwendet werden, das nicht verschlüsselt werden kann, müssen Sie das Band manuell mit einem neuen Kennsatz versehen, bevor es in diesem Laufwerk verwendet werden kann.

#### ON

Gibt an, dass IBM Spectrum Protect der Schlüsselmanager für die Laufwerkverschlüsselung ist und die Laufwerkverschlüsselung für leere Speicherpooldatenträger nur erlaubt, wenn das Anwendungsverfahren aktiviert ist. (Andere Typen von Datenträgern werden nicht verschlüsselt. Beispielsweise werden Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger nicht verschlüsselt.) Wird ON angegeben und ein anderes Verschlüsselungsverfahren aktiviert, ist die Laufwerkverschlüsselung nicht zulässig, und Sicherungsoperationen schlagen fehl.

#### ALLOW

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Die Laufwerkverschlüsselung für leere Datenträger ist jedoch zulässig, wenn ein anderes Verschlüsselungsverfahren aktiviert ist.

#### EXtErnal


Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Verwenden Sie diese Einstellung mit einer Verschlüsselungsmethodik, die von einem anderen Anbieter zur Verfügung gestellt wird und die mit dem Anwendungsverfahren der Verschlüsselung verwendet wird, das für das Laufwerk aktiviert ist. Geben Sie EXTERNAL an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect nicht inaktiviert. Geben Sie dagegen ALLOW an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect inaktiviert.

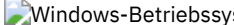
#### OFF



Gibt an, dass die Laufwerkverschlüsselung nicht zulässig ist. Wird ein anderes Verschlüsselungsverfahren aktiviert, schlagen Sicherungen fehl. Wird das Anwendungsverfahren aktiviert, inaktiviert IBM Spectrum Protect die Verschlüsselung, und die Ausführung von Sicherungen wird versucht.

## DEFINE DEVCLASS (Einheitenklasse FILE definieren)

Verwenden Sie die Einheitenklasse FILE, wenn Dateien im Magnetplattenspeicher als Datenträger verwendet werden, die Daten sequenziell speichern (wie auf Band).

  Die Einheitenklasse FILE unterstützt keine Kassettenarchive EXTERNAL.

 Die Einheitenklasse FILE unterstützt keine EXTERNAL- oder Remote Storage Manager-Kassettenarchive.

  Wenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in DEFINE DEVCLASS (Einheitenklasse FILE für z/OS Media-Server definieren).

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-DEFine DEVclass--Einheitenklassenname--DEVType-----FILE----->
. -MOUNTLimit-----20----- . -MAXCAPacity-----10G---
>>+-----+-----+-----+-----+-----+----->
' -MOUNTLimit-----Anzahl- ' ' -MAXCAPacity-----Größe- '
. -DIRectory-----Name_des_aktuellen_Verzeichnisses-.
>>+-----+-----+-----+-----+-----+----->
|           |           |           |           |           |
|           v           |           |           |           |
' -DIRectory-----Verzeichnisname+-----+-----'
. -SHAREd-----No-----
>>+-----+-----+-----+-----+-----+-----<
```

'-SHARED-----+--No--+-'  
'-Yes-'

## Parameter

---

### Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.



### DEVType=FILE (Erforderlich)

Gibt an, dass der Einheitentyp FILE der Einheitenklasse zugeordnet wird. FILE bedeutet, dass dieser Einheitenklasse eine Datei zugeordnet ist. Wenn der Server auf einen Datenträger zugreifen muss, der zu dieser Einheitenklasse gehört, öffnet er eine Datei und liest oder schreibt Dateidaten.

Eine Datei ist eine Form eines Datenträgers mit sequenziellem Zugriff.

### MOUNTLimit

Gibt die maximale Anzahl von Dateien an, die gleichzeitig für die Ein- und Ausgabe geöffnet sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist 20. Sie können eine Zahl von 0 bis 4096 angeben.

  Wird die Einheitenklasse mit einem Speicheragenten gemeinsam genutzt (durch Angabe des Parameters SHARED=YES), werden Laufwerke definiert oder gelöscht, um eine Übereinstimmung mit dem Grenzwert für Ladeanforderung zu erreichen.



Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

### MAXCAPacity

Gibt die maximale Größe einer Datenspeicherdatei an, die für einen Speicherpool in dieser Einheitenklasse definiert ist.

Der Wert des Parameters MAXCAPACITY wird auch als Zuordnungseinheit verwendet, wenn Speicherbereichsauslöser für den Speicherpool Datenträger erstellen. Der Standardwert ist 10 GB (MAXCAPACITY=10G). Der angegebene Wert muss kleiner-gleich der maximal unterstützten Größe einer Datei im Zieldateisystem sein.



Dieser Wert muss als ganze Zahl gefolgt von einem K (Kilobyte), M (Megabyte), G (Gigabyte) oder T (Terabyte) angegeben werden. Die Mindestgröße ist 1 MB (MAXCAPACITY=1M). Wenn Sie eine Einheitenklasse FILE für Datenbanksicherungsdatenträger definieren, geben Sie einen Wert für MAXCAPACITY an, der für die Größe der Datenbank angemessen ist und der die Anzahl der Datenbankdatenträger minimiert.


  Definieren Sie keinen Wert für MAXCAPACITY, der größer als 640 MB ist, wenn diese Datei für die REMOVABLEFILE CD-Unterstützung bestimmt ist. Ein Wert, der kleiner als der verwendbare Speicherbereich (650 MB) einer CD ist, ermöglicht eine Eins-zu-Eins-Übereinstimmung zwischen Dateien aus der Einheitenklasse FILE und Kopien, die sich auf CD befinden.

### DIRECTory

Gibt die Verzeichnisposition(en) der in dieser Einheitenklasse verwendeten Dateien an. Schließen Sie die gesamte Liste der Verzeichnisse in Anführungszeichen ein und verwenden Sie Kommas, um einzelne Verzeichnisnamen voneinander zu trennen. Sonderzeichen (z. B. Leerzeichen) sind in Verzeichnisnamen zulässig. Die Verzeichnisliste "abc def,xyz" enthält beispielsweise zwei Verzeichnisse: abc def und xyz.



Dieser Parameter ist wahlfrei.

  Der Standardwert ist das aktuelle Arbeitsverzeichnis des Servers zum Zeitpunkt der Befehlsausgabe.



 Der Standardwert ist das aktuelle Arbeitsverzeichnis des Servers zum Zeitpunkt der Befehlsausgabe. Windows-Registry-Informationen werden verwendet, um das Standardverzeichnis zu bestimmen.

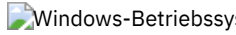
Durch die Angabe eines oder mehrerer Verzeichnisnamen wird die Position angegeben, an der der Server die Dateien speichert, die Speicherdatenträger für diese Einheitenklasse darstellen.

Für die NetApp-SnapLock-Unterstützung (Speicherpools mit RECLAMATIONTYPE=SNAPLOCK, die diese Einheitenklasse verwenden) müssen die mit dem Parameter DIRECTORY angegebenen Verzeichnisse auf die Verzeichnisse auf den NetApp-SnapLock-Datenträgern zeigen.

  Bei der Verarbeitung des Befehls erweitert der Server den oder die angegebenen Verzeichnisnamen in die vollständig qualifizierte Form (beginnend beim Stammverzeichnis).

Wenn der Server einen Arbeitsdatenträger zuordnen muss, erstellt er eine neue Datei in einem dieser Verzeichnisse. (Der Server kann ein beliebiges der Verzeichnisse auswählen, in dem neue Arbeitsdatenträger erstellt werden sollen.) Bei Arbeitsdatenträgern, die zum Speichern von Clientdaten verwendet werden, hat die durch den Server erstellte Datei die Dateinamenerweiterung .bfs. Bei Arbeitsdatenträgern, auf denen Exportdaten gespeichert werden, wird die Dateinamenerweiterung .exp verwendet.

  Wenn Sie beispielsweise eine Einheitenklasse mit dem Verzeichnis tsmstor definieren und der Server einen Arbeitsdatenträger in dieser Einheitenklasse benötigt, um Exportdaten zu speichern, könnte der Name der Datei, die der Server erstellt, tsmstor\00566497.exp lauten.

 Wenn Sie beispielsweise eine Einheitenklasse mit dem Verzeichnis c:\server definieren und der Server einen Arbeitsdatenträger in dieser Einheitenklasse benötigt, um Exportdaten zu speichern, könnte der Name der Datei, die der Server erstellt, c:\server\00566497.exp lauten.

Wichtig: Sie müssen sicherstellen, dass Speicheragenten auf neu erstellte FILE-Datenträger zugreifen können. Kann der Speicheragent nicht auf einen FILE-Datenträger zugreifen, werden Operationen möglicherweise nur auf einem LAN-Pfad wiederholt, oder die Operationen können fehlschlagen. Weitere Informationen enthält die Beschreibung des Parameters DIRECTORY in DEFINE PATH (Pfad definieren).

Tipp: Geben Sie mehrere Verzeichnisse für eine Einheitenklasse an, stellen Sie sicher, dass die Verzeichnisse separaten Dateisystemen zugeordnet sind. Bei Speicherbereichsauslöserfunktionen und Berechnungen des Speicherbereichs im Speicherpool wird der Speicherbereich berücksichtigt, der in jedem Verzeichnis verbleibt. Wenn Sie mehrere Verzeichnisse für eine Einheitenklasse angeben und sich die Verzeichnisse in demselben Dateisystem befinden, berechnet der Server den Speicherbereich durch Hinzufügen von Werten, die den Speicherbereich darstellen, der in jedem Verzeichnis verbleibt. Diese Speicherbereichsberechnungen sind ungenau. Anstatt einen Speicherpool mit ausreichend Speicherbereich für eine Operation auszuwählen, kann der Server den falschen Speicherpool auswählen und frühzeitig über keinen Speicherbereich mehr verfügen. Bei Speicherbereichsauslösern kann eine ungenaue Berechnung zu einem Fehler bei der Erweiterung des Speicherbereichs führen, der in einem Speicherpool verfügbar ist. Ein Fehler bei der Erweiterung des Speicherbereichs in einem Speicherpool ist eine der Bedingungen, die zur Inaktivierung eines Auslösers führen kann. Wird ein Auslöser inaktiviert, da der Speicherbereich in einem Speicherpool nicht erweitert werden konnte, können Sie den Auslöser erneut aktivieren, indem Sie den folgenden Befehl ausgeben: `update spacetrigger stg`. Es sind keine weiteren Änderungen an dem Speicherbereichsauslöser erforderlich.

#### SHAREd

Gibt an, dass diese Einheitenklasse FILE von dem Server und von einem oder mehreren Speicheragenten gemeinsam genutzt wird. Zur Vorbereitung der gemeinsamen Nutzung wird automatisch ein Kassettenarchiv zusammen mit einer Anzahl von Laufwerken definiert, die dem Wert des Parameters MOUNTLIMIT entspricht. Die Laufwerknamen bestehen aus dem Namen des Kassettenarchivs plus einer Zahl von 1 bis zum Grenzwert für Ladeanforderung (Mount-Limit). Lautet der Kassettenarchivname beispielsweise FILE und ist der Grenzwert für Ladeanforderung auf 4 gesetzt, haben die Laufwerke die Namen FILE11, FILE12, FILE13, FILE14.

Informationen zu Voraussetzungen, wenn Speicher vom Server und Speicheragenten gemeinsam genutzt wird, befinden sich unter [IBM® Support Portal for IBM Spectrum Protect](#).

## Beispiel: Eine Einheitenklasse FILE mit mehreren Verzeichnissen definieren

---

Eine Einheitenklasse definieren, die mehrere Verzeichnisse angibt.



```
define devclass multidir devtype=file
    directory=/usr/xyz,/usr/abc,/usr/uvw
```



```
define devclass multidir devtype=file
    directory=/opt/xyz,/opt/abc,/opt/uvw
```



```
define devclass multidir devtype=file
    directory=e:\xyz,f:\abc,g:\uvw
```

## Beispiel: Eine Einheitenklasse FILE mit einer Kapazität von 50 MB definieren

---

Die Einheitenklasse PLAINFILES mit dem Einheitentyp FILE und einer maximalen Kapazität von 50 MB definieren.

```
define devclass plainfiles devtype=file
    maxcapacity=50m
```

## DEFINE DEVCLASS (Einheitenklasse GENERICTAPE definieren)

Verwenden Sie die Einheitenklasse GENERICTAPE für Bandlaufwerke, die von Einheitentreibern des Betriebssystems unterstützt werden.

Bei Verwendung dieses Einheitentyps erkennt der Server weder den Einheitentyp noch das Kassettenaufzeichnungsformat. Wenn ein E/A-Fehler auftritt, sind die Fehlerinformationen weniger ausführlich im Vergleich zu den Fehlerinformationen für einen bestimmten Einheitentyp (z. B. 8MM), da der Server den Einheitentyp nicht erkennt. Bei der Definition von Einheiten für den Server dürfen keine verschiedenen Einheitentypen in demselben Einheitentyp gemischt werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-DEFine DEVclass--Einheitenklassenname----->
>--LIBRary----Kassettenarchivname--DEVType----GENERICTape---->
                                     .-MOUNTRetention----60-----.
>--+-----+-----+-----+-----+-----+-----+----->
  '-ESTCAPacity----Größe- '  '-MOUNTRetention----Minuten- '
                                     .-MOUNTWait----60-----.
                                     .-MOUNTLimit----DRIVES-----.
>--+-----+-----+-----+-----+-----+-----+-----<
  '-MOUNTWait----Minuten- '  '-MOUNTLimit----+DRIVES-+- '
                                     +-Anzahl+
                                     '-0-----'
```

### Parameter

#### Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

#### LIBRARY (Erforderlich)

Gibt den Namen des definierten Kassettenarchivobjekts an, das die Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können.

Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

#### DEVType=GENERICTape (Erforderlich)

Gibt an, dass der Einheitentyp GENERICTAPE der Einheitenklasse zugeordnet wird. GENERICTAPE bedeutet, dass die Datenträger für diese Einheitenklasse in Bandlaufwerken verwendet werden, die vom Bandeinheitentreiber des Betriebssystems unterstützt werden.

Der Server erkennt, dass die Datenträger entfernt und weitere Datenträger eingelegt werden können, innerhalb der mit dem Parameter MOUNTLIMIT für die Einheitenklasse und dem Parameter MAXSCRATCH für den Speicherpool gesetzten Grenzwerte.

Datenträger in einer Einheitenklasse mit dem Einheitentyp GENERICTAPE sind Datenträger mit sequenziellem Zugriff.

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Geben Sie eine dem verwendeten Bandlaufwerk entsprechende Kapazität an.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

## DEFINE DEVCLASS (Einheitenklasse LTO definieren)

Verwenden Sie die Einheitenklasse LTO, wenn Sie LTO-Bandeinheiten verwenden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-DEFine DEVclass--Einheitenklassenname----->
>--LIBRary----Kassettenarchivname--DEVType----LTO----->
                                     (1)
. -LBProtect----No----- . -WORM----No-----
>--+-----+-----+-----+-----+----->
' -LBProtect----+READWrite+-' -WORM----+No--+-'
      +-WRITEOnly-+          '-Yes-'
      '-No-----'

. -FORMAT----DRIVE-----
>--+-----+-----+-----+-----+----->
' -FORMAT----+DRIVE-----+' -ESTCAPacity----Größe-'
```

```

+-ULTRIUM---+
+-ULTRIUMC--+
+-ULTRIUM2---+
+-ULTRIUM2C--+
+-ULTRIUM3---+
+-ULTRIUM3C--+
+-ULTRIUM4---+
+-ULTRIUM4C--+
+-ULTRIUM5---+
+-ULTRIUM5C--+
+-ULTRIUM6---+
'-ULTRIUM6C-'

.-PREFIX-----ADSM-----
>-----+----->
'-PREFIX-----+ADSM-----+'
      '-Banddatenträgerpräfix-'

.-MOUNTRetention----60-----.-MOUNTWait----60-----
>-----+-----+----->
'-MOUNTRetention----Minuten-' '-MOUNTWait----Minuten-'

.-MOUNTLimit----DRIVES-----
>-----+----->
'-MOUNTLimit----+DRIVES--+'
      +-Anzahl+
      '-0-----'

(1) (2)
.-DRIVEEncryption----ALLOW-----
>-----+-----><
'-DRIVEEncryption----+ON-----+'
      +-ALLOW----+
      +-EXTERNAL-+
      '-OFF-----'

```

Anmerkungen:

1. Sie können nicht WORM=Yes in Verbindung mit DRIVEENCRYPTION=ON angeben.
2. Laufwerkverschlüsselung wird nur für Ultrium 4-, Ultrium 5- und Ultrium 6-Laufwerke und -Datenträger unterstützt.

## Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRARY (Erforderlich)

Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten LTO-Bandlaufwerke enthält. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

DEVType=LTO (Erforderlich)

Gibt an, dass der Einheitentyp LTO (Linear Tape Open) der Einheitenklasse zugeordnet wird.

LBProtect

Gibt an, ob der Schutz logischer Blöcke verwendet wird, um die Integrität von Daten sicherzustellen, die auf Band gespeichert sind. Wenn LBPROTECT auf READWRITE oder WRITEONLY gesetzt ist, verwendet der Server dieses Feature des Bandlaufwerks für den Schutz logischer Blöcke und generiert CRC-Zugriffsschutzinformationen für jeden Datenblock, der auf Band geschrieben wird. Der Server überprüft auch die CRC-Zugriffsschutzinformationen, wenn Daten von dem Band gelesen werden.

Der Standardwert ist NO.

Die folgenden Werte sind gültig:

READWrite

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect und dem Bandlaufwerk erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen. Der Wert READWRITE hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

Wird der Parameter LBPROTECT auf READWRITE gesetzt, müssen Sie nicht den Parameter CRCDATA in einer Speicherpooldefinition angeben, da der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust bereitstellt.

WRITEOnly

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk nur für Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Für Leseoperationen überprüfen der Server und das Bandlaufwerk nicht die CRC-Informationen. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect zum Generieren der CRC-Informationen und für das Bandlaufwerk zum Berechnen und Vergleichen der CRC-Werte für Schreiboperationen erforderlich ist. Der Wert WRITEONLY hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

No

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen nicht aktiviert ist. Der Server aktiviert jedoch den Schutz logischer Blöcke bei Schreiboperationen für einen sich füllenden Datenträger, der bereits über Daten mit dem Schutz logischer Blöcke verfügt.

Einschränkung: Der Schutz logischer Blöcke wird nur auf IBM® LTO5-Laufwerken und unterstützten LTO6-Laufwerken unterstützt.

#### WORM

Gibt an, ob die Laufwerke WORM-Datenträger (Write Once, Read Many) verwenden. Dieser Parameter ist wahlfrei. Der Standardwert ist No. Das Feld kann einen der folgenden Werte enthalten:

Yes

Gibt an, dass die Laufwerke WORM-Datenträger verwenden.

No

Gibt an, dass die Laufwerke keine WORM-Datenträger verwenden.

Anmerkung:

1. Sollen WORM-Datenträger in einem Kassettenarchiv verwendet werden, müssen alle Laufwerke in dem Kassettenarchiv WORM-fähig sein.
2. Sie können nicht IBM Spectrum Protect als Schlüsselmanager für die Laufwerkverschlüsselung von WORM-Datenträgern angeben (WORM - Write Once Read Many). (Die Angabe von WORM=Yes in Verbindung mit DRIVEENCRYPTION=ON wird nicht unterstützt.)

#### FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Geben Sie stattdessen das Format an, das die Laufwerke verwenden.

Gehen Sie wie folgt vor, wenn alle Laufwerke von Ultrium-Einheiten auf Ultrium 2-Einheiten migriert werden:

- Löschen Sie alle vorhandenen Ultrium-Laufwerkdefinitionen und die Pfade, die ihnen zugeordnet sind.
- Definieren Sie die neuen Ultrium 2-Laufwerke und Pfade.

Sollen verschiedene Generationen von LTO-Datenträgern und -laufwerken gemischt werden, sind die folgenden Einschränkungen zu beachten.

Tabelle 1. Lese-/Schreibfunktionalität verschiedener Generationen von LTO-Laufwerken

| Laufwerke                 | Datenträger der Generation 1 | Datenträger der Generation 2 | Datenträger der Generation 3 | Datenträger der Generation 4 | Datenträger der Generation 5 | Datenträger der Generation 6 |
|---------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|
| Generation 1              | Lesen und schreiben          | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             |
| Generation 2              | Lesen und schreiben          | Lesen und schreiben          | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             |
| Generation 3 <sup>1</sup> | Nur lesen                    | Lesen und schreiben          | Lesen und schreiben          | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             |
| Generation 4 <sup>2</sup> | nicht zutreffend             | Nur lesen                    | Lesen und schreiben          | Lesen und schreiben          | nicht zutreffend             | nicht zutreffend             |
| Generation 5 <sup>3</sup> | nicht zutreffend             | nicht zutreffend             | Nur lesen                    | Lesen und schreiben          | Lesen und schreiben          | nicht zutreffend             |
| Generation 6 <sup>4</sup> | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | Nur lesen                    | Lesen und schreiben          | Lesen und schreiben          |



| Laufwerke  | Datenträger der Generation 1 | Datenträger der Generation 2 | Datenträger der Generation 3 | Datenträger der Generation 4 | Datenträger der Generation 5 | Datenträger der Generation 6 |
|--|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|
| <sup>1</sup> In einem Kassettenarchiv mit einem Laufwerk der Generation 3 müssen alle Arbeitsdatenträger der Generation 1 entnommen werden und alle Speicherpooldatenträger der Generation 1 müssen in "schreibgeschützt" aktualisiert werden. |                              |                              |                              |                              |                              |                              |
| <sup>2</sup> In einem Kassettenarchiv mit einem Laufwerk der Generation 4 müssen alle Arbeitsdatenträger der Generation 2 entnommen werden und alle Speicherpooldatenträger der Generation 2 müssen in "schreibgeschützt" aktualisiert werden. |                              |                              |                              |                              |                              |                              |
| <sup>3</sup> In einem Kassettenarchiv mit einem Laufwerk der Generation 5 müssen alle Arbeitsdatenträger der Generation 3 entnommen werden und alle Speicherpooldatenträger der Generation 3 müssen in "schreibgeschützt" aktualisiert werden. |                              |                              |                              |                              |                              |                              |
| <sup>4</sup> In einem Kassettenarchiv mit einem Laufwerk der Generation 6 müssen alle Arbeitsdatenträger der Generation 4 entnommen werden und alle Speicherpooldatenträger der Generation 4 müssen in "schreibgeschützt" aktualisiert werden. |                              |                              |                              |                              |                              |                              |

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für LTO-Einheiten aufgelistet:

Tabelle 2. Aufzeichnungsformat und geschätzte Standardkapazität für LTO

| Format   | Geschätzte Kapazität       | Beschreibung   |
|--|----------------------------|--|
| DRIVE  | –                          | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| ULTRIUM  | 100 GB                     | Dekomprimiertes Format, verwendet Ultrium-Kassetten  |
| ULTRIUMC   | Siehe Anmerkung<br>200 GB  | Komprimiertes Format, verwendet Ultrium-Kassetten  |
| ULTRIUM2   | 200 GB                     | Dekomprimiertes (Standard) Format, verwendet Ultrium 2-Kassetten   |
| ULTRIUM2C  | Siehe Anmerkung<br>400 GB  | Komprimiertes Format, verwendet Ultrium 2-Kassetten  |
| ULTRIUM3   | 400 GB                     | Dekomprimiertes (Standard) Format, verwendet Ultrium 3-Kassetten   |
| ULTRIUM3C  | Siehe Anmerkung<br>800 GB  | Komprimiertes Format, verwendet Ultrium 3-Kassetten  |
| ULTRIUM4   | 800 GB                     | Dekomprimiertes (Standard) Format, verwendet Ultrium 4-Kassetten   |
| ULTRIUM4C  | Siehe Anmerkung<br>1,6 TB  | Komprimiertes Format, verwendet Ultrium 4-Kassetten  |
| ULTRIUM5   | 1,5 TB                     | Dekomprimiertes (Standard-)Format, verwendet Ultrium 5-Kassetten   |
| ULTRIUM5C  | Siehe Anmerkung<br>3,0 TB  | Komprimiertes Format, verwendet Ultrium 5-Kassetten  |
| ULTRIUM6   | 2,5 TB                     | Dekomprimiertes (Standard) Format, verwendet Ultrium 6-Kassetten   |
| ULTRIUM6C  | Siehe Anmerkung<br>6,25 TB | Komprimiertes Format, verwendet Ultrium 6-Kassetten  |
| Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann die tatsächliche Kapazität abhängig von der Effektivität der Komprimierung größer als der aufgelistete Wert sein. |                            |  |

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Für weitere Informationen zu geschätzten Kapazitäten siehe Tabelle 2.

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

#### DRIVEEncryption

Gibt an, ob die Laufwerkverschlüsselung zulässig ist. Dieser Parameter ist wahlfrei. Der Standardwert ist ALLOW. Laufwerkverschlüsselung wird nur für Ultrium 4-, Ultrium 5- und Ultrium 6-Laufwerke und -Datenträger unterstützt. Einschränkung: Ist die Verschlüsselung für eine Einheitenklasse aktiviert und ist die Einheitenklasse einem Speicherpool zugeordnet, sollte der Speicherpool nicht einen Arbeitsdatenträgerpool mit anderen Einheitenklassen gemeinsam nutzen, die nicht verschlüsselt werden können. Ist ein Band verschlüsselt und soll das Band in einem Laufwerk verwendet werden, das nicht verschlüsselt werden kann, müssen Sie das Band manuell mit einem neuen Kennsatz versehen, bevor es in diesem Laufwerk verwendet werden kann.

#### ON

Gibt an, dass IBM Spectrum Protect der Schlüsselmanager für die Laufwerkverschlüsselung ist und die Laufwerkverschlüsselung für leere Speicherpooldatenträger nur erlaubt, wenn das Anwendungsverfahren aktiviert ist. (Andere Typen von Datenträgern werden nicht verschlüsselt. Beispielsweise werden Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger nicht verschlüsselt.) Wird ON angegeben und ein anderes Verschlüsselungsverfahren aktiviert, ist die Laufwerkverschlüsselung nicht zulässig, und Sicherungsoperationen schlagen fehl.

Anmerkung: Sie können nicht IBM Spectrum Protect als Schlüsselmanager für die Laufwerkverschlüsselung von WORM-Datenträgern angeben (WORM - Write Once Read Many). (Die Angabe von WORM=Yes in Verbindung mit DRIVEENCRYPTION=ON wird nicht unterstützt.)

#### ALLOW

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Die Laufwerkverschlüsselung für leere Datenträger ist jedoch zulässig, wenn ein anderes Verschlüsselungsverfahren aktiviert ist.

#### EXTERNAL

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Verwenden Sie diese Einstellung mit einer Verschlüsselungsmethodik, die von einem anderen Anbieter zur Verfügung gestellt wird und die mit dem Anwendungsverfahren der Verschlüsselung verwendet wird, das für das Laufwerk aktiviert ist. Geben Sie EXTERNAL an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect nicht inaktiviert. Geben Sie dagegen ALLOW an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect inaktiviert.

#### OFF

Gibt an, dass die Laufwerkverschlüsselung nicht zulässig ist. Wird ein anderes Verschlüsselungsverfahren aktiviert, schlagen Sicherungen fehl. Wird das Anwendungsverfahren aktiviert, inaktiviert IBM Spectrum Protect die Verschlüsselung, und die Ausführung von Sicherungen wird versucht.

## Beispiel: Eine Einheitenklasse LTO definieren

---

Die Einheitenklasse LTOTAPE für ein LTO-Laufwerk in dem Kassettenarchiv LTOLIB definieren. Das Format ist ULTRIUM, der Grenzwert für Ladeanforderung ist 12, die Ladedauer ist 5, das Banddatenträgerpräfix lautet SMVOL und die geschätzte Kapazität beträgt 100 GB.

```
define devclass ltotape devtype=lto library=ltolib
format=ultrium mountlimit=12 mountretention=5
prefix=smvol estcapacity=100G
```

## DEFINE DEVCLASS (Einheitenklasse NAS definieren)

---

Verwenden Sie die Einheitenklasse NAS (Network Attached Storage), wenn Sie NDMP-Operationen zum Sichern von NAS-Dateiservern verwenden (NDMP - Network Data Management Protocol). Die Einheitenklasse ist für Laufwerke bestimmt, die der NAS-Dateiserver für Sicherungen unterstützt.

  Die Einheitenklasse NAS unterstützt keine Kassettenarchive EXTERNAL.

 Die Einheitenklasse NAS unterstützt keine EXTERNAL- oder Remote Storage Manager-Kassettenarchive.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
>>-DEFine DEVclass--Einheitenklassenname--DEVType-----NAS----->
```

```

>--LIBRARY---Kassettenarchivname--MOUNTRetention---0----->
. -MOUNTWait---60----- . -MOUNTLimit---DRIVES-----
>+-----+-----+-----+-----+-----+----->
' -MOUNTWait---Minuten- ' -MOUNTLimit---DRIVES-+-'
                                     +-Anzahl-+
                                     '-0-----'

>--ESTCAPacity---Größe----->
. -PREFIX---ADSM-----
>+-----+-----+-----+----->
' -PREFIX---+ADSM-----+-'
      '-Banddatenträgerpräfix-'

```

## Parameter

### Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

### DEVType=NAS (Erforderlich)

Gibt an, dass der Einheitentyp NAS (Network-Attached Storage) der Einheitenklasse zugeordnet wird. Der NAS-Einheitentyp ist für Laufwerke bestimmt, die mit einem NAS-Dateiserver verbunden sind und von einem NAS-Dateiserver zum Sichern von NAS-Dateisystemen verwendet werden.

### LIBRARY (Erforderlich)

Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten SCSI-Bandlaufwerke enthält. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

### MOUNTRetention=0 (Erforderlich)

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Null (0) ist der einzige unterstützte Wert für Einheitenklassen mit DEVType=NAS.

### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

### Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

### ESTCAPacity (Erforderlich)

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

## PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

```
AB.CD2.E
```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

## Beispiel: Eine Einheitenklasse NAS definieren

---

Die Einheitenklasse NASTAPE für ein NAS-Laufwerk in dem Kassettenarchiv NASLIB definieren. Der Grenzwert für Ladeanforderung ist DRIVES, die Ladedauer ist 0, das Banddatenträgerpräfix lautet SMVOL und die geschätzte Kapazität beträgt 200 GB.

```
define devclass nastape devtype=nas library=naslib
mountretention=0 mountlimit=drives
prefix=smvol estcapacity=200G
```

## DEFINE DEVCLASS (Einheitenklasse REMOVABLEFILE definieren)

---

Verwenden Sie die Einheitenklasse REMOVABLEFILE für Einheiten für austauschbare Datenträger, die als lokale, entfernbare Dateisysteme angeschlossen sind.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
>>-DEFine DEVclass--Einheitenklassenname----->
>--LIBRARY----Kassettenarchivname--DEVType----REMOVABLEfile--->
  .-MAXCAPacity----verbleibender_Speicherbereich-.
>--+-----+-----+-----+-----+----->
  '-MAXCAPacity----Größe-----'
  .-MOUNTRetention----60----- .-MOUNTWait----60-----
>--+-----+-----+-----+-----+----->
  '-MOUNTRetention--Minuten-' '-MOUNTWait----Minuten-'
  .-MOUNTLimit----DRIVES----- .
>--+-----+-----+-----+-----+-----><
  '-MOUNTLimit----++DRIVES++'
    +-Anzahl+
    '-0-----'
```

## Parameter

---

Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRARY (Erforderlich)

Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten Laufwerke für austauschbare Datenträger enthält. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl

DEFINE LIBRARY.

DEVType=REMOVABLEfile (Erforderlich)

Gibt an, dass der Einheitentyp REMOVABLEFILE der Einheitenklasse zugeordnet wird. REMOVABLEFILE bedeutet, dass die Datenträger für diese Einheitenklasse Dateien auf lokalen, austauschbaren Datenträgern sind.

Datenträger in einer Einheitenklasse mit dem Einheitentyp REMOVABLEFILE sind Datenträger mit sequenziellem Zugriff.

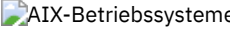
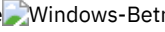
Verwenden Sie die Dienstprogramme des Einheitsherstellers, um die Datenträger zu formatieren (falls erforderlich) und zu kennzeichnen. Der Kennsatz auf den Datenträgern muss folgende Bedingungen erfüllen:

- Der Kennsatz darf maximal 11 Zeichen haben.
- Der Datenträgerkennsatz und der Name der Datei auf dem Datenträger müssen exakt übereinstimmen.
-   Der Parameter MAXCAPACITY muss auf einen Wert gesetzt werden, der niedriger als die Kapazität des Datenträgers ist.

MAXCAPacity

Gibt die maximale Größe der Datenträger an, die für einen Speicherpool definiert sind, der durch diese Einheitenklasse kategorisiert wird. Dieser Parameter ist wahlfrei.

Der Parameter MAXCAPACITY muss auf einen Wert gesetzt werden, der niedriger als die Kapazität des Datenträgers ist. Bei CD-Datenträgern kann die maximale Kapazität nicht größer als 650 MB sein.

  Da der Server nur eine Datei pro physischen austauschbaren Datenträger öffnet, ist die Kapazität so zu wählen, dass diese eine Datei die Datenträgerkapazität vollständig nutzt.

Verbleibender\_Speicherbereich

Der Standardwert für die maximale Kapazität ist der auf dem Datenträger verbleibende Speicherbereich nach seiner ersten Verwendung.

Größe

Dieser Wert muss als ganze Zahl gefolgt von einem K (Kilobyte), M (Megabyte), G (Gigabyte) oder T (Terabyte) angegeben werden.

MAXCAPACITY=5M gibt beispielsweise an, dass die maximale Kapazität eines Datenträgers in dieser Einheitenklasse 5 MB beträgt. Der zulässige Mindestwert ist 1 MB (d. h. MAXCAPACITY=1M).

MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

## DEFINE DEVCLASS (Einheitenklasse SERVER definieren)

---

Verwenden Sie die Einheitenklasse SERVER, um Speicherdatenträger oder Dateien zu verwenden, die auf einem anderen IBM Spectrum Protect-Server archiviert sind.

Wird der Aufbewahrungsschutz für Daten mit dem Befehl SET ARCHIVERETENTIONPROTECTION aktiviert, können Sie keine Servereinheitenklasse definieren.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
>>-DEFine DEVclass--Einheitenklassenname--DEVType---SERVER---->
                                     .-MAXCAPacity---500M--.
>--SERVERName---Servername--+-----+-----+----->
                                     '-MAXCAPacity---Größe-'
                                     .-MOUNTLimit---1----- .-MOUNTRetention---60-----
>+-----+-----+-----+-----+-----+----->
                                     '-MOUNTLimit---Anzahl-' '-MOUNTRetention---Minuten-'
                                     .-PREFIX---ADSM----- .
>+-----+-----+-----+-----+-----+----->
                                     '-PREFIX---ADSM-----+-'
                                     '-Datenträgerpräfix-'
                                     .-RETRYPeriod---10----- .
>+-----+-----+-----+-----+-----+----->
                                     '-RETRYPeriod---Wiederholungszeitraum (Minuten)-'
                                     .-RETRYInterval---30----- .
>+-----+-----+-----+-----+-----+-----><
                                     '-RETRYInterval---Wiederholungsintervall (Sekunden)-'
```

## Parameter

---

#### Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

#### DEVType=SERVER (Erforderlich)

Gibt eine Fernverbindung an, die virtuelle Bereiche unterstützt.

#### SERVERName (Erforderlich)

Gibt den Namen des Servers an. Der Parameter SERVERNAME muss einem definierten Server entsprechen.

#### MAXCAPacity

Gibt die maximale Größe für Objekte an, die auf dem Zielserver erstellt werden; der Standardwert ist 500M. Dieser Parameter ist wahlfrei.

#### 500M

Gibt an, dass die maximale Kapazität 500M (500 MB) beträgt.

#### Größe

Dieser Wert muss als ganze Zahl gefolgt von einem K (Kilobyte), M (Megabyte), G (Gigabyte) oder T (Terabyte) angegeben werden. Der zulässige Mindestwert ist 1 MB (MAXCAPACITY=1M).

#### MOUNTLimit

Gibt die maximal zulässige Anzahl gleichzeitig stattfindender Sitzungen zwischen dem Quellenserver und dem Zielserv an. Alle Versuche, auf mehr Sitzungen zuzugreifen als mit dem Grenzwert für Ladeanforderung angegeben sind, haben das Warten des Anforderers zur Folge. Dieser Parameter ist wahlfrei. Der Standardwert ist 1. Sie können eine Zahl von 1 bis 4096 angeben.  
Gültige Werte:

1

Gibt an, dass nur eine Sitzung zwischen dem Quellenserver und dem Zielserv zulässig ist.

Anzahl

Gibt die Anzahl der gleichzeitig stattfindenden Sitzungen zwischen dem Quellenserver und dem Zielserv an.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die eine inaktive Verbindung mit dem Zielserv aufrechterhalten werden soll, bevor die Verbindung geschlossen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60. Sie können eine Zahl von 0 bis 9999 angeben.  
Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### PREFIX

Gibt den Anfangsabschnitt des Archivierungsdateinamens der höheren Ebene auf dem Zielserv an. Dieser Parameter ist wahlfrei. Der Standardwert ist AD\$M. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Archivierungsdateinamens der höheren Ebene, der das Standardpräfix verwendet, ist AD\$M.volume1.

#### RETRYPeriod

Gibt den Wiederholungszeitraum in Minuten an. Der Wiederholungszeitraum ist das Intervall, während dem der Server versucht, eine Verbindung zu einem Zielserv herzustellen, falls ein Übertragungsfehler vermutet wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben. Der Standardwert ist 10 Minuten.

#### RETRYInterval

Gibt das Wiederholungsintervall in Sekunden an. Das Wiederholungsintervall gibt an, wie oft Wiederholungen in einer bestimmten Zeitperiode erfolgen. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 1 bis 9999 angeben. Der Standardwert ist 30 Sekunden.

## DEFINE DEVCLASS (Einheitenklasse VOLSAFE definieren)

---

Verwenden Sie den Einheitentyp VOLSAFE, um mit StorageTek VolSafe-Datenträgern und -Laufwerken zu arbeiten. Diese Technologie verwendet Datenträger, die nicht überschrieben werden können. Verwenden Sie diese Datenträger daher nicht für kurzfristige Sicherungen von Clientdateien, der Serverdatenbank oder von Exportbändern.

Einschränkungen:

1. NAS-angeschlossene Kassettenarchive werden nicht unterstützt.
2. VolSafe-Datenträger und Datenträger mit Lese-/Schreibzugriff müssen sich in separaten Speicherpools befinden.
3. Stellen Sie Kassetten mit CHECKLABEL=YES im Befehl CHECKIN LIBVOLUME zurück.
4. Kennzeichnen Sie Kassetten mit OVERWRITE=NO im Befehl LABEL LIBVOLUME. Werden VolSafe-Kassetten mehrmals gekennzeichnet, können keine weiteren Daten auf sie geschrieben werden.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.



## Syntax

```
>>-DEFine DEVclass--Einheitenklassenname----->
>--LIBRARY----Kassettenarchivname--DEVType----VOLSAFE----->
      .-FORMAT----DRIVE-----.
>--WORM----Yes--+-----+----->
      '-FORMAT----+DRIVE----+'
              +-9840-----+
              +-9840-C----+
              +-T9840C----+
              +-T9840C-C--+
              +-T9840D----+
              +-T9840D-C--+
              +-T10000A----+
              +-T10000A-C--+
              +-T10000B----+
              +-T10000B-C--+
              +-T10000C----+
              +-T10000C-C--+
              +-T10000D----+
              '-T10000D-C-'

      .-MOUNTRetention----60-----.
>+-----+-----+----->
      '-ESTCAPacity----Größe-' '-MOUNTRetention----Minuten-'

      .-PREFIX----ADSM-----.
>+-----+-----+----->
      '-PREFIX----+ADSM----+'
              '-Datenträgerpräfix-'

      .-MOUNTWait----60-----.  .-MOUNTLimit----DRIVES-----.
>+-----+-----+-----<
      '-MOUNTWait----Minuten-' '-MOUNTLimit----+DRIVES--+-'
                                  +-Anzahl-+
                                  '-0-----'
```

## Parameter

### Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

### LIBRARY (Erforderlich)

Gibt den Namen des definierten Kassettenarchivobjekts an, das die VolSafe-Laufwerke enthält, die von dieser Einheitenklasse verwendet werden können. Sind Laufwerke in einem Kassettenarchiv VolSafe-aktiviert, müssen alle Laufwerke in dem Kassettenarchiv VolSafe-aktiviert sein. Lesen Sie die Informationen in der Hardwareokumentation zur Aktivierung von VolSafe auf den 9840- und T10000-Laufwerken.

Informationen über das Definieren eines Kassettenarchivobjekts befinden sich in DEFINE LIBRARY (Kassettenarchiv definieren).

### DEVType=VOLSAFE (Erforderlich)

Gibt an, dass der Einheitentyp VOLSAFE der Einheitenklasse zugeordnet wird. Der Kennsatz bei diesem Kassettentyp kann einmal überschrieben werden. IBM Spectrum Protect führt diese Überschreibung aus, wenn der erste Datenblock geschrieben wird. Daher ist es wichtig, dass die Verwendung des Befehls LABEL LIBVOLUME auf ein Mal pro Datenträger begrenzt wird. Verwenden Sie hierfür den Parameter OVERWRITE=NO.

### WORM

Gibt an, ob die Laufwerke WORM-Datenträger (Write Once, Read Many) verwenden. Der Parameter ist erforderlich. Der Wert muss Yes lauten.

Yes

Gibt an, dass die Laufwerke WORM-Datenträger verwenden.

### FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

Wichtig: Wird DRIVE für eine Einheitenklasse angegeben, die über inkompatible Einheiten mit sequenziellem Zugriff verfügt, müssen Datenträger in Einheiten geladen werden, die in dem Format lesen oder schreiben können, das beim ersten Laden des Datenträgers eingerichtet wurde. Dies kann zu Verzögerungen führen, wenn die einzige Einheit mit sequenziellem Zugriff, die auf den Datenträger zugreifen kann, bereits im Gebrauch ist.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für VolSafe-Einheiten aufgelistet:  
**Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für VOLSAFE-Datenträger**

| Format    | Geschätzte Kapazität     | Beschreibung   |
|-----------|--------------------------|--|
| DRIVE     | –                        | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| 9840      | 20 GB                    | Dekomprimiertes (Standard) Format, verwendet eine 20-GB-Kassette mit 270 Meter Band  |
| 9840-C    | Siehe Anmerkung<br>80 GB | Komprimiertes LZ-1 Enhanced-Format (4:1), verwendet eine 80-GB-Kassette mit 270 Meter Band   |
| T9840C    | 40 GB                    | Dekomprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840C-C  | 80 GB                    | Komprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840D    | 75 GB                    | Dekomprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840D-C  | 150 GB                   | Komprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette   |
| T10000A   | 500 GB                   | Dekomprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette  |
| T10000A-C | 1 TB                     | Komprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette  |
| T10000B   | 1 TB                     | Dekomprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette   |
| T10000B-C | 2 TB                     | Komprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette   |
| T10000C   | 5 TB                     | Dekomprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000C-C | 10 TB                    | Komprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000D   | 8 TB                     | Dekomprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000D-C | 15 TB                    | Komprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Für weitere Informationen zur geschätzten Standardkapazität von Magnetbandkassetten siehe Tabelle 1.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von

Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### PREFIX

Gibt den Anfangsabschnitt des Archivierungsdateinamens der höheren Ebene auf dem Zielsystem an. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Archivierungsdateinamens der höheren Ebene, der das Standardpräfix verwendet, ist ADSM.volume1.

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

## DEFINE DEVCLASS - z/OS Media-Server (Einheitenklasse für z/OS Media-Server definieren)

Verwenden Sie den Befehl DEFINE DEVCLASS, um eine Einheitenklasse für einen Speichereinheitentyp zu definieren. Für den Server muss eine Einheitenklasse definiert werden, damit eine Einheit verwendet werden kann. Eine begrenzte Gruppe von

Einheitenklassentypen ist für Einheiten verfügbar, auf die über einen z/OS Media-Server zugegriffen wird.

- DEFINE DEVCLASS (Einheitenklasse 3590 für z/OS Media-Server definieren)
- DEFINE DEVCLASS (Einheitenklasse 3592 für z/OS Media-Server definieren)
- DEFINE DEVCLASS (Einheitenklasse ECARTRIDGE für z/OS Media-Server definieren)
- DEFINE DEVCLASS (Einheitenklasse FILE für z/OS Media-Server definieren)

Tabelle 1. Zugehörige Befehle für DEFINE DEVCLASS

| Befehl                              | Beschreibung   |
|-------------------------------------|--|
| BACKUP DEVCONFIG                    | Sichert IBM Spectrum Protect-Einheitendaten in einer Datei.  |
| DEFINE LIBRARY                      | Definiert ein automatisiertes oder manuelles Kassettenarchiv.  |
| DELETE DEVCLASS                     | Löscht eine Einheitenklasse.   |
| QUERY DEVCLASS                      | Zeigt Informationen zu Einheitenklassen an.  |
| UPDATE DEVCLASS (z/OS Media-Server) | Ändert die Attribute einer Einheitenklasse für Speicher, der von einem z/OS Media-Server verwaltet wird. |

## DEFINE DEVCLASS (Einheitenklasse 3590 für z/OS Media-Server definieren)

Um einen z/OS Media-Server für den Zugriff auf 3590-Einheiten zu verwenden, müssen Sie eine Einheitenklasse 3590 definieren. Geben Sie in der Einheitenklassendefinition ein Kassettenarchiv an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-DEFine DEVclass--Einheitenklassenname----->
>--LIBRary----ZOSMEDIA-Kassettenarchiv--DEVType-----3590----->
                                     .-ESTCAPacity--9G-----.
>--+-----+-----+-----+-----+-----+-----+----->
  '-FORMAT-----+DRIVE---+'  '-ESTCAPacity-----Größe---'
                                     +-3590B---+
                                     +-3590C---+
                                     +-3590E-B-+
                                     +-3590E-C-+
                                     +-3590H-B-+
                                     '-3590H-C-'

                                     .-PREFIX----ADSM-----
>--+-----+-----+-----+-----+-----+-----+----->
  '-PREFIX-----+ADSM-----+'
                                     '-Banddatenträgerpräfix-'

                                     .-MOUNTRetention---60-----
                                     .-MOUNTWait-----60-----
>--+-----+-----+-----+-----+-----+-----+----->
  '-MOUNTRetention---Minuten-'  '-MOUNTWait-----Minuten-'

                                     .-MOUNTLimit---2-----
                                     .-COMpression---Yes-----
>--+-----+-----+-----+-----+-----+-----+----->
  '-MOUNTLimit-----+DRIVES-+'  '-COMpression---+Yes-+'
                                     +-Anzahl-+
                                     '-0-----'

>--+-----+-----+-----+-----+-----+-----+----->
  +-EXPIration---jjjttt-+
  '-RETention---Tage-----'

                                     .-PROtection---No-----
>--+-----+-----+-----+-----+-----+-----+----->
  '-PROtection---+No-----+'
                                     +-Yes-----+
                                     '-Automatic-'
```

```

.-UNIT---3590-----
>-----><
'-UNIT---Einheitenname-'

```

## Parameter

### Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

### LIBRARY (Erforderlich)

Gibt den Namen eines Kassettenarchivs an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde. Das Kassettenarchiv und die Bandlaufwerke, die von dieser Einheitenklasse verwendet werden können, werden von dem z/OS Media-Server gesteuert.

Informationen zum Definieren eines Kassettenarchivs befinden sich unter dem Befehl DEFINE LIBRARY.

### DEVtype=3590 (Erforderlich)

Gibt an, dass der Einheitentyp 3590 der Einheitenklasse zugeordnet wird. 3590 bedeutet, dass der Einheitenklasse Magnetbandkassetteneinheiten IBM 3590 zugeordnet werden.

Einschränkung: Der z/OS Media-Server unterstützt beim Schreiben auf 3590-Bandlaufwerke 256-KB-Datenblöcke. Überprüfen Sie, ob Ihre Hardware dies unterstützt.

### FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Die folgende Tabelle enthält die Aufzeichnungsformate.

Tabelle 1. Aufzeichnungsformate für 3590

| Format   | Beschreibung   |
|--|--|
| 3590B  | Dekomprimiertes (Basis-)Format                           |
| 3590C  | Komprimiertes Format                                     |
| 3590E-B  | Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format |
| 3590E-C  | Komprimiertes Format, ähnlich dem 3590C-Format           |
| 3590H-B  | Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format |
| 3590H-C  | Komprimiertes Format, ähnlich dem 3590C-Format           |
| Anmerkung: Wenn das Format die Datenkomprimierung über Hardware mittels Bandlaufwerk verwendet, kann die tatsächliche Kapazität je nach Effektivität der Komprimierung zunehmen. |  |

### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei. Der Standardwert für die geschätzte Kapazität von 3590-Bändern beträgt 9 GB.

Dieser Parameter kann angegeben werden, wenn die geschätzte Standardkapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist. Der Wert bestimmt nicht das auf dem Datenträger gespeicherte Datenvolumen. Der Server verwendet den Wert, um die Belegung zu schätzen, bevor ein Datenträger gefüllt ist. Wenn ein Datenträger voll ist, wird für die Berechnung der Belegung das tatsächlich auf dem Band gespeicherte Datenvolumen verwendet.

Geben Sie den Wert als ganze Zahl mit einem der folgenden Einheitenanzeiger an: **K** (KB), **M** (MB), **G** (GB) oder **T** (TB). Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt. Der zulässige Mindestwert ist 100 KB (ESTCAPACITY=100K).

### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADMS. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Banddatenträger beibehalten wird, bevor er entladen wird. Die Zeitspanne für die Ladedauer beginnt nach Ablauf des Inaktivitätszeitlimits. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Geben Sie eine Zahl von 0 bis 9999 an.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

#### MOUNTWait

Gibt die maximale Anzahl Minuten an, die der z/OS Media-Server auf das Laden eines Datenträgers wartet. Wird auf die Ladeanforderung nicht innerhalb der angegebenen Zeit geantwortet, schlägt die Ladeanforderung fehl. Ist eine Einheit erfolgreich zugeordnet und wird die Anforderung zum Öffnen der Einheit nicht innerhalb der angegebenen Zeit ausgeführt, wird die Anforderung zum Öffnen der Einheit beendet und die Ladeanforderung schlägt fehl.

Dieser Parameter ist wahlfrei. Der Standardwert ist 60. Geben Sie eine Zahl von 1 bis 9999 an.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Standardwert ist 2.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Sie können einen der folgenden Werte angeben:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt. Sie können eine Zahl von 0 bis 4096 angeben.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können.

#### COMPression

Gibt an, ob die Dateikomprimierung für diese Einheitenklasse verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Sie können einen der folgenden Werte angeben:

#### Yes

Gibt an, dass die Daten der Banddatenträger komprimiert werden.

#### No

Gibt an, dass die Daten der Banddatenträger nicht komprimiert werden.

#### EXPIration

Gibt das Verfallsdatum an, das in den Bandkennsätzen für diese Einheitenklasse angegeben wird. Dieser Parameter ist wahlfrei. Es gibt keinen Standardwert.

Geben Sie das Datum an, an dem der Server das Band nicht mehr benötigt. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Geben Sie das Verfallsdatum im Format *jjjjtt* an (vier Stellen für das Jahr und drei Stellen für den Tag). Beispielsweise wird der 7. Januar 2014 als 2014007 angegeben (der siebte Tag des Jahres 2014).

Wenn Sie den Parameter EXPIRATION angeben, können Sie nicht den Parameter RETENTION angeben.

#### RETention

Gibt die Anzahl Tage an, die das Band aufbewahrt werden soll. Dieser Parameter ist wahlfrei.

Geben Sie die Anzahl der Tage (1 - 9999) an, die der Server das Band voraussichtlich verwenden wird. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Wenn Sie den Parameter RETENTION angeben, können Sie nicht den Parameter EXPIRATION angeben.

#### PROtection

Gibt an, ob das RACF-Programm (falls installiert) Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Wenn Schutz zur Verfügung gestellt wird, werden RACF-Profile bei der ersten Verwendung der Datenträger erstellt. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

##### No

Gibt an, dass das RACF-Programm keine Datenträger schützt, die dieser Einheitenklasse zugeordnet sind.

##### Yes

Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Für die Datenträger werden RACF-Profile erstellt, wenn der Server die Datenträger zum ersten Mal verwendet; die Profile werden jedoch nicht gelöscht, wenn Datenträger auf dem Server gelöscht werden. Die Profile müssen manuell gelöscht werden.

Tipp: Sind sensible Daten auf den Datenträgern gespeichert, die dieser Einheitenklasse zugeordnet sind, verwenden Sie PROTECTION=YES und löschen Sie RACF-Profile manuell nur nach dem Entfernen der Banddatenträger.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

#### Automatic

Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. RACF-Profile werden für Datenträger erstellt, wenn der Server zum ersten Mal die Datenträger verwendet. RACF-Profile werden gelöscht, wenn Datenträger auf dem Server gelöscht werden.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

Wichtig: Wird PROTECTION=AUTOMATIC angegeben, wird beim Löschen eines Datenträgers sein RACF-Profil gelöscht. Der Datenträger ist daher nicht mehr durch das RACF-Programm geschützt. Andere Benutzer können auf die Daten auf diesen Datenträgern zugreifen.

Wenn Sie PROTECTION=AUTOMATIC angeben, gibt der z/OS Media-Server RACROUTE-Befehle aus, um Profile zu löschen, wenn ein Datenträger auf dem Server gelöscht wird. Die ausgegebenen Löschbefehle sind von den aktuellen Systemwerten für TAPEVOL und TAPEDSN abhängig. Wenn die Systemeinstellungen geändert werden, löscht der z/OS Media-Server vorhandene Profile möglicherweise nicht.

Ändern Sie nicht die Einstellung in PROTECTION=AUTOMATIC für eine Einheitenklasse, für die PROTECTION=NO definiert wurde. Es können Datenträger ohne Profile vorhanden sein, und es werden Fehlernachrichten generiert, wenn diese Datenträger gelöscht werden. Wenn ein anderer Wert für PROTECTION erforderlich ist, definieren Sie eine neue Einheitenklasse.

Die Erstellung und das Löschen von Profilen erfolgen aufgrund der Schutzeinstellungen, wenn der Datenträger zum ersten Mal verwendet und wenn er gelöscht wird. Der Server erstellt keine Profile für Datenträger, die er bereits verwendet hat. Wenn für den Schutz AUTOMATIC angegeben ist, versucht der Server, Profile zu löschen, wenn Datenträger gelöscht werden.

Die Dokumentation zu dem RACF-Programm enthält ausführliche Informationen zu den Einstellungen für TAPEVOL und TAPEDSN und zu den Profilen, die erstellt werden, wenn diese Einstellungen aktiv sind.

#### UNIT

Gibt einen privaten Einheitennamen für eine Gruppe von Bandeinheiten an, die 3590-Band unterstützen. Dieser Parameter ist wahlfrei. Der Standardeinheitenname ist 3590. Der Einheitenname kann bis zu 8 Zeichen umfassen.

## DEFINE DEVCLASS (Einheitenklasse 3592 für z/OS Media-Server definieren)

Um einen z/OS Media-Server für den Zugriff auf 3592-Einheiten zu verwenden, müssen Sie eine Einheitenklasse 3592 definieren. Geben Sie in der Einheitenklassendefinition ein Kassettenarchiv an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-DEFine DEVclass--Einheitenklassenname----->
>--LIBRARY----ZOSMEDIA-Kassettenarchiv--DEVType-----3592----->
. -FORMAT----Drive----- . -WORM----No-----
>-----+-----+-----+-----+-----+-----+----->
' -FORMAT----+DRIVE---+ ' ' -WORM----+Yes--+ '
      +-3592----+          ' -No-- '
      +-3592C---+
      +-3592-2---+
      +-3592-2C--+
      +-3592-3---+
      +-3592-3C--+
      +-3592-4---+
      '-3592-4C-'

. -ESTCAPacity----300G--.
>-----+-----+-----+-----+-----+-----+----->
' -ESTCAPacity----Größe- '

. -PREFIX----ADSM----- .
>-----+-----+-----+-----+-----+-----+----->
' -PREFIX----+ADSM-----+ '
      '-Banddatenträgerpräfix- '

. -MOUNTRetention---60----- . -MOUNTWait---60----- .
>-----+-----+-----+-----+-----+-----+----->
' -MOUNTRetention---Minuten- ' ' -MOUNTWait---Minuten- '

. -MOUNTLimit---2----- . -COMPRESSION---Yes----- .
>-----+-----+-----+-----+-----+-----+----->
' -MOUNTLimit---+DRIVES--+ ' ' -COMPRESSION---+Yes--+ '
      +-Anzahl+          ' -No-- '
      '-0-----'

>-----+-----+-----+-----+-----+-----+----->
+ -EXPIration---jjjjttt+
' -RETention---Tage----- '

. -PROtection---No----- .
>-----+-----+-----+-----+-----+-----+----->
' -PROtection---+No-----+ '
      +-Yes-----+
      '-Automatic-'

. -UNIT---3592----- .
>-----+-----+-----+-----+-----+-----+----->
' -UNIT---Einheitenname- '
```

## Parameter

### Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

### LIBRARY (Erforderlich)

Gibt den Namen eines Kassettenarchivs an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde. Das Kassettenarchiv und die Bandlaufwerke, die von dieser Einheitenklasse verwendet werden können, werden von dem z/OS Media-Server gesteuert.

Informationen zum Definieren eines Kassettenarchivs befinden sich unter dem Befehl DEFINE LIBRARY.

### DEVType=3592 (Erforderlich)

Gibt an, dass der Einheitentyp 3592 der Einheitenklasse zugeordnet wird.

### FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

Die folgende Tabelle enthält die Aufzeichnungsformate.

Tabelle 1. Aufzeichnungsformate für 3592



| <b>Format</b>  | <b>Beschreibung</b>  |
|--|--|
| 3592   | Dekomprimiertes (Basis-)Format   |
| 3592C  | Komprimiertes Format   |
| 3592-2   | Dekomprimiertes (Basis) Format, ähnlich dem 3592-Format  |
| 3592-C   | Komprimiertes Format, ähnlich dem 3592C-Format   |
| 3592-3   | Dekomprimiertes (Basis) Format, ähnlich dem 3592-Format  |
| 3592-3C  | Komprimiertes Format, ähnlich dem 3592C-Format   |
| 3592-4   | Dekomprimiertes (Basis) Format, ähnlich dem 3592-Format  |
| 3592-4C  | Komprimiertes Format, ähnlich dem 3592C-Format   |
| DRIVE  | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann je nach Effektivität der Komprimierung die tatsächliche Kapazität von dem aufgelisteten Wert abweichen. |  |

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet. Um optimale Ergebnisse zu erzielen, mischen Sie nicht Generationen von Laufwerken in demselben Kassettenarchiv. Enthält ein Kassettenarchiv gemischte Generationen, können Datenträgerfehler auftreten. Beispielsweise können Laufwerke der Generation 1 und Generation 2 keine Datenträger der Generation 3 lesen. Falls möglich, führen Sie für alle Laufwerke ein Upgrade auf 3592 Generation 3 durch. Kann nicht für alle Laufwerke ein Upgrade auf 3592 Generation 3 durchgeführt werden, müssen Sie eine spezielle Konfiguration verwenden.

#### WORM

Gibt an, ob die Laufwerke WORM-Datenträger (Write Once, Read Many) verwenden. Dieser Parameter ist wahlfrei. Der Standardwert ist No. Sie können einen der folgenden Werte angeben:

Yes

Gibt an, dass die Laufwerke WORM-Datenträger verwenden.

No

Gibt an, dass die Laufwerke keine WORM-Datenträger verwenden.

Tipp: Der IBM Spectrum Protect-Server löscht nicht automatisch Arbeitsdatenträger in WORM-Speicherpools, nachdem die Datenträger durch den Verfallsprozess oder durch andere Prozesse geleert wurden. Um diese Datenträger zu löschen und die Datenträger aus WORM-Speicherpools zu entfernen, müssen Sie den Befehl DELETE VOLUME verwenden. IBM Spectrum Protect kann keine WORM-Datenträger wiederverwenden, die vom Server beschrieben und dann aus einem Speicherpool gelöscht wurden.

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn die geschätzte Standardkapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist. Der Wert bestimmt nicht das auf dem Datenträger gespeicherte Datenvolumen. Der Server verwendet den Wert, um die Belegung zu schätzen, bevor ein Datenträger gefüllt ist. Wenn ein Datenträger voll ist, wird für die Berechnung der Belegung das tatsächlich auf dem Band gespeicherte Datenvolumen verwendet.

Geben Sie den Wert als ganze Zahl mit einem der folgenden Einheitenanzeiger an: **K** (KB), **M** (MB), **G** (GB) oder **T** (TB). Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt. Der zulässige Mindestwert ist 100 KB (ESTCAPACITY=100K).

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist AD5M. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist AD\$M.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Banddatenträger beibehalten wird, bevor er entladen wird. Die Zeitspanne für die Ladedauer beginnt nach Ablauf des Inaktivitätszeitlimits. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Geben Sie eine Zahl von 0 bis 9999 an.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

#### MOUNTWait

Gibt die maximale Anzahl Minuten an, die der z/OS Media-Server auf das Laden eines Datenträgers wartet. Wird auf die Ladeanforderung nicht innerhalb der angegebenen Zeit geantwortet, schlägt die Ladeanforderung fehl. Ist eine Einheit erfolgreich zugeordnet und wird die Anforderung zum Öffnen der Einheit nicht innerhalb der angegebenen Zeit ausgeführt, wird die Anforderung zum Öffnen der Einheit beendet und die Ladeanforderung schlägt fehl.

Dieser Parameter ist wahlfrei. Der Standardwert ist 60. Geben Sie eine Zahl von 1 bis 9999 an.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Standardwert ist 2.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Sie können einen der folgenden Werte angeben:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt. Sie können eine Zahl von 0 bis 4096 angeben.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können.

#### COMPression

Gibt an, ob die Dateikomprimierung für diese Einheitenklasse verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Sie können einen der folgenden Werte angeben:

#### Yes

Gibt an, dass die Daten der Banddatenträger komprimiert werden.

#### No

Gibt an, dass die Daten der Banddatenträger nicht komprimiert werden.

#### EXPIration

Gibt das Verfallsdatum an, das in den Bandkennsätzen für diese Einheitenklasse angegeben wird. Dieser Parameter ist wahlfrei. Es gibt keinen Standardwert.

Geben Sie das Datum an, an dem der Server das Band nicht mehr benötigt. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Geben Sie das Verfallsdatum im Format *jjjjtt* an (vier Stellen für das Jahr und drei Stellen für den Tag). Beispielsweise wird der 7. Januar 2014 als 2014007 angegeben (der siebte Tag des Jahres 2014).

Wenn Sie den Parameter EXPIRATION angeben, können Sie nicht den Parameter RETENTION angeben.

#### RETention

Gibt die Anzahl Tage an, die das Band aufbewahrt werden soll. Dieser Parameter ist wahlfrei.

Geben Sie die Anzahl der Tage (1 - 9999) an, die der Server das Band voraussichtlich verwenden wird. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Wenn Sie den Parameter RETENTION angeben, können Sie nicht den Parameter EXPIRATION angeben.

#### PROtection

Gibt an, ob das RACF-Programm (falls installiert) Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Wenn Schutz zur Verfügung gestellt wird, werden RACF-Profile bei der ersten Verwendung der Datenträger erstellt. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

##### No

Gibt an, dass das RACF-Programm keine Datenträger schützt, die dieser Einheitenklasse zugeordnet sind.

##### Yes

Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Für die Datenträger werden RACF-Profile erstellt, wenn der Server die Datenträger zum ersten Mal verwendet; die Profile werden jedoch nicht gelöscht, wenn Datenträger auf dem Server gelöscht werden. Die Profile müssen manuell gelöscht werden.

Tipp: Sind sensible Daten auf den Datenträgern gespeichert, die dieser Einheitenklasse zugeordnet sind, verwenden Sie PROTECTION=YES und löschen Sie RACF-Profile manuell nur nach dem Entfernen der Banddatenträger.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

##### Automatic

Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. RACF-Profile werden für Datenträger erstellt, wenn der Server zum ersten Mal die Datenträger verwendet. RACF-Profile werden gelöscht, wenn Datenträger auf dem Server gelöscht werden.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

Wichtig: Wird PROTECTION=AUTOMATIC angegeben, wird beim Löschen eines Datenträgers sein RACF-Profil gelöscht. Der Datenträger ist daher nicht mehr durch das RACF-Programm geschützt. Andere Benutzer können auf die Daten auf diesen Datenträgern zugreifen.

Wenn Sie PROTECTION=AUTOMATIC angeben, gibt der z/OS Media-Server RACROUTE-Befehle aus, um Profile zu löschen, wenn ein Datenträger auf dem Server gelöscht wird. Die ausgegebenen Löschbefehle sind von den aktuellen Systemwerten für TAPEVOL und TAPEDSN abhängig. Wenn die Systemeinstellungen geändert werden, löscht der z/OS Media-Server vorhandene Profile möglicherweise nicht.

Ändern Sie nicht die Einstellung in PROTECTION=AUTOMATIC für eine Einheitenklasse, für die PROTECTION=NO definiert wurde. Es können Datenträger ohne Profile vorhanden sein, und es werden Fehlermeldungen generiert, wenn diese Datenträger gelöscht werden. Wenn ein anderer Wert für PROTECTION erforderlich ist, definieren Sie eine neue Einheitenklasse.

Die Erstellung und das Löschen von Profilen erfolgen aufgrund der Schutzeinstellungen, wenn der Datenträger zum ersten Mal verwendet und wenn er gelöscht wird. Der Server erstellt keine Profile für Datenträger, die er bereits verwendet hat. Wenn für den Schutz AUTOMATIC angegeben ist, versucht der Server, Profile zu löschen, wenn Datenträger gelöscht werden.

Die Dokumentation zu dem RACF-Programm enthält ausführliche Informationen zu den Einstellungen für TAPEVOL und TAPEDSN und zu den Profilen, die erstellt werden, wenn diese Einstellungen aktiv sind.

#### UNIT

Gibt einen privaten Einheitennamen für eine Gruppe von Bandeneinheiten an, die 3592-Band unterstützen. Dieser Parameter ist wahlfrei. Der Standardwert ist 3592. Der Einheitenname kann bis zu 8 Zeichen umfassen.

# DEFINE DEVCLASS (Einheitenklasse ECARTRIDGE für z/OS Media-Server definieren)

Um einen z/OS Media-Server für den Zugriff auf StorageTek-Laufwerke, wie z. B. StorageTek T9840 oder T10000, zu verwenden, müssen Sie eine Einheitenklasse ECARTRIDGE definieren. Geben Sie in der Einheitenklassendefinition ein Kassettenarchiv an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-DEFine DEVclass--Einheitenklassenname----->
>--LIBRary---ZOSMEDIA-Kassettenarchiv----->
>--DEVType---ECARTridge----->
      .-FORMAT---DRIVE-----.
      +-----+-----+-----+
      '-FORMAT---+DRIVE---+'
              +-T9840C-----+
              +-T9840C-C---+
              +-T9840D-----+
              +-T9840D-C---+
              +-T10000A---+
              +-T10000A-C+
              +-T10000B---+
              +-T10000B-C+
              +-T10000C---+
              +-T10000C-C+
              +-T10000D---+
              '-T10000D-C-'

      .-ESTCAPacity---9G---.
>+-----+-----+-----+----->
      '-ESTCAPacity---Größe-'

      .-PREFIX---ADSM-----.
>+-----+-----+-----+----->
      '-PREFIX---+ADSM---+'
              '-Banddatenträgerpräfix-'

      .-MOUNTRetention---60-----.  .-MOUNTWait---60-----.
>+-----+-----+-----+----->
      '-MOUNTRetention---Minuten-'  '-MOUNTWait---Minuten-'

      .-MOUNTLimit---2-----.  .-COMPRESSION---Yes-----.
>+-----+-----+-----+----->
      '-MOUNTLimit---+DRIVES+-'  '-COMPRESSION---+Yes+-'
              +-Anzahl+
              '-0-----'
              '-No--'

>+-----+-----+-----+----->
      +-EXPIration---jjjjttt+
      '-RETention---Tage-----'

      .-PROtection---No-----.
>+-----+-----+-----+----->
      '-PROtection---+No-----+'
              +-Yes-----+
              '-Automatic-'

      .-UNIT---9840-----.
>+-----+-----+-----+-----><
      '-UNIT---Einheitenname-'
```

## Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

## LIBRARY (Erforderlich)

Gibt den Namen eines Kassettenarchivs an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde. Das Kassettenarchiv und die Bandlaufwerke, die von dieser Einheitenklasse verwendet werden können, werden von dem z/OS Media-Server gesteuert.

Informationen zum Definieren eines Kassettenarchivs befinden sich unter dem Befehl DEFINE LIBRARY.

## DEVType=ECARTridge (Erforderlich)

Gibt an, dass der Einheitentyp ECARTRIDGE der Einheitenklasse zugeordnet wird. Der Einheitentyp ECARTRIDGE ist für StorageTek-Laufwerke, wie z. B. StorageTek T9840 oder T10000, bestimmt.

## FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Die folgende Tabelle enthält die Aufzeichnungsformate.

Tabelle 1. Aufzeichnungsformate für ECARTRIDGE-Bänder

| Format   | Geschätzte Kapazität | Beschreibung   |
|--|----------------------|--|
| DRIVE  | -                    | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. DRIVE ist der Standardwert.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| T9840C   | 40 GB                | Dekomprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840C-C   | 80 GB                | Komprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840D   | 75 GB                | Dekomprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840D-C   | 150 GB               | Komprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette   |
| T10000A  | 500 GB               | Dekomprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette  |
| T10000A-C  | 1 TB                 | Komprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette  |
| T10000B  | 1 TB                 | Dekomprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette   |
| T10000B-C  | 2 TB                 | Komprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette   |
| T10000C  | 5 TB                 | Dekomprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000C-C  | 10 TB                | Komprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000D  | 8 TB                 | Dekomprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000D-C  | 15 TB                | Komprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| Anmerkung:   |                      |  |
| <ul style="list-style-type: none"><li>Einige Formate verwenden eine Komprimierungsfunktion der Bandlaufwerkhardware. Je nach Effektivität der Komprimierung kann die tatsächliche Kapazität doppelt so groß (oder größer) sein wie der aufgeführte Wert.</li><li>T10000A-Laufwerke können nur das T10000A-Format lesen und schreiben. T10000B-Laufwerke können das T10000A-Format lesen, aber nicht schreiben. T10000C-Laufwerke können die T10000A- und T10000B-Formate lesen, aber nicht schreiben. T10000D-Laufwerke können die T10000A-, T10000B- und T10000C-Formate lesen, aber nicht schreiben.</li></ul> |                      |  |

## ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei. Die standardmäßige geschätzte Kapazität ist 9 GB.

Dieser Parameter kann angegeben werden, wenn die geschätzte Standardkapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist. Der Wert bestimmt nicht das auf dem Datenträger gespeicherte Datenvolumen. Der Server verwendet den Wert, um die Belegung zu schätzen, bevor ein Datenträger gefüllt ist. Wenn ein Datenträger voll ist, wird für die Berechnung der Belegung das tatsächlich auf dem Band gespeicherte Datenvolumen verwendet.

Geben Sie den Wert als ganze Zahl mit einem der folgenden Einheitenanzeiger an: K (KB), M (MB), G (GB) oder T (TB). Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt. Der zulässige Mindestwert ist

100 KB (ESTCAPACITY=100K).

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Banddatenträger beibehalten wird, bevor er entladen wird. Die Zeitspanne für die Ladedauer beginnt nach Ablauf des Inaktivitätszeitlimits. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Geben Sie eine Zahl von 0 bis 9999 an.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

#### MOUNTWait

Gibt die maximale Anzahl Minuten an, die der z/OS Media-Server auf das Laden eines Datenträgers wartet. Wird auf die Ladeanforderung nicht innerhalb der angegebenen Zeit geantwortet, schlägt die Ladeanforderung fehl. Ist eine Einheit erfolgreich zugeordnet und wird die Anforderung zum Öffnen der Einheit nicht innerhalb der angegebenen Zeit ausgeführt, wird die Anforderung zum Öffnen der Einheit beendet und die Ladeanforderung schlägt fehl.

Dieser Parameter ist wahlfrei. Der Standardwert ist 60. Geben Sie eine Zahl von 1 bis 9999 an.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Standardwert ist 2.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Sie können einen der folgenden Werte angeben:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt. Sie können eine Zahl von 0 bis 4096 angeben.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können.

#### COMPRESSION

Gibt an, ob die Dateikomprimierung für diese Einheitenklasse verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Sie können einen der folgenden Werte angeben:

#### Yes

Gibt an, dass die Daten der Banddatenträger komprimiert werden.

No

Gibt an, dass die Daten der Banddatenträger nicht komprimiert werden.

#### EXPIration

Gibt das Verfallsdatum an, das in den Bandkennsätzen für diese Einheitenklasse angegeben wird. Dieser Parameter ist wahlfrei. Es gibt keinen Standardwert.

Geben Sie das Datum an, an dem der Server das Band nicht mehr benötigt. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Geben Sie das Verfallsdatum im Format *jjjjtt* an (vier Stellen für das Jahr und drei Stellen für den Tag). Beispielsweise wird der 7. Januar 2014 als *2014007* angegeben (der siebte Tag des Jahres 2014).

Wenn Sie den Parameter EXPIRATION angeben, können Sie nicht den Parameter RETENTION angeben.

#### RETention

Gibt die Anzahl Tage an, die das Band aufbewahrt werden soll. Dieser Parameter ist wahlfrei.

Geben Sie die Anzahl der Tage (1 - 9999) an, die der Server das Band voraussichtlich verwenden wird. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Wenn Sie den Parameter RETENTION angeben, können Sie nicht den Parameter EXPIRATION angeben.

#### PROtection

Gibt an, ob das RACF-Programm (falls installiert) Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Wenn Schutz zur Verfügung gestellt wird, werden RACF-Profile bei der ersten Verwendung der Datenträger erstellt. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass das RACF-Programm keine Datenträger schützt, die dieser Einheitenklasse zugeordnet sind.

Yes

Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Für die Datenträger werden RACF-Profile erstellt, wenn der Server die Datenträger zum ersten Mal verwendet; die Profile werden jedoch nicht gelöscht, wenn Datenträger auf dem Server gelöscht werden. Die Profile müssen manuell gelöscht werden. Tipp: Sind sensible Daten auf den Datenträgern gespeichert, die dieser Einheitenklasse zugeordnet sind, verwenden Sie PROTECTION=YES und löschen Sie RACF-Profile manuell nur nach dem Entfernen der Banddatenträger.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

Automatic

Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. RACF-Profile werden für Datenträger erstellt, wenn der Server zum ersten Mal die Datenträger verwendet. RACF-Profile werden gelöscht, wenn Datenträger auf dem Server gelöscht werden.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

Wichtig: Wird PROTECTION=AUTOMATIC angegeben, wird beim Löschen eines Datenträgers sein RACF-Profil gelöscht. Der Datenträger ist daher nicht mehr durch das RACF-Programm geschützt. Andere Benutzer können auf die Daten auf diesen Datenträgern zugreifen.

Wenn Sie PROTECTION=AUTOMATIC angeben, gibt der z/OS Media-Server RACROUTE-Befehle aus, um Profile zu löschen, wenn ein Datenträger auf dem Server gelöscht wird. Die ausgegebenen Löschbefehle sind von den aktuellen Systemwerten für TAPEVOL und TAPEDSN abhängig. Wenn die Systemeinstellungen geändert werden, löscht der z/OS Media-Server vorhandene Profile möglicherweise nicht.

Ändern Sie nicht die Einstellung in PROTECTION=AUTOMATIC für eine Einheitenklasse, für die PROTECTION=NO definiert wurde. Es können Datenträger ohne Profile vorhanden sein, und es werden Fehlermeldungen generiert, wenn diese Datenträger gelöscht werden. Wenn ein anderer Wert für PROTECTION erforderlich ist, definieren Sie eine neue Einheitenklasse.

Die Erstellung und das Löschen von Profilen erfolgen aufgrund der Schutzeinstellungen, wenn der Datenträger zum ersten Mal verwendet und wenn er gelöscht wird. Der Server erstellt keine Profile für Datenträger, die er bereits verwendet hat. Wenn für den Schutz AUTOMATIC angegeben ist, versucht der Server, Profile zu löschen, wenn Datenträger gelöscht werden.

Die Dokumentation zu dem RACF-Programm enthält ausführliche Informationen zu den Einstellungen für TAPEVOL und TAPEDSN und zu den Profilen, die erstellt werden, wenn diese Einstellungen aktiv sind.

#### UNIT

Gibt einen privaten Einheitennamen für eine Gruppe von Bandeinheiten an, die ECARTRIDGE-Bänder unterstützen. Verwenden Sie den Einheitennamen, der die Untergruppe der Laufwerke im Kassettenarchiv darstellt, die mit dem z/OS-System verbunden sind. Dieser Parameter ist wahlfrei. Der Standardwert ist 9840. Der Einheitenname kann bis zu 8 Zeichen umfassen.

## Beispiel: Eine Einheitenklasse mit dem Einheitentyp ECARTRIDGE definieren

Die Einheitenklasse E1 mit dem Einheitentyp ECARTRIDGE sowie aktiviertem RACF-Schutz für alle Banddatenträger, die dieser Einheitenklasse zugeordnet sind, definieren. Alle Daten werden für diese Einheitenklasse komprimiert. Die Einheitenklasse gilt für das Kassettenarchiv mit dem Namen ZOSELIB eines z/OS Media-Servers.

```
define devclass e1 devtype=ecartridge library=zoselib compression=yes
    protection=yes
```

## DEFINE DEVCLASS (Einheitenklasse FILE für z/OS Media-Server definieren)

Um einen z/OS Media-Server für den Zugriff auf Speicherdatenträger auf Magnetplatteneinheiten zu verwenden, müssen Sie eine Einheitenklasse FILE definieren. Geben Sie in der Einheitenklassendefinition ein Kassettenarchiv an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde.

Ein Datenträger in dieser Einheitenklasse ist eine lineare VSAM-Datei (VSAM - Virtual Storage Access Method), auf die vom z/OS Media-Server zugegriffen wird. Arbeitsdatenträger können mit der Einheitenklasse verwendet werden und der z/OS Media-Server kann die lineare VSAM-Datei dynamisch zuordnen. Es ist nicht erforderlich, Datenträger für den Server zu definieren, um die Einheitenklasse zu verwenden. Wenn Sie Datenträger definieren, definieren Sie das Qualifikationsmerkmal der höheren Ebene so, dass SMS die Zuordnungsanforderung durch den z/OS Media-Server erkennt. Bei Verwendung von definierten Datenträgern wird die Funktion zum Formatieren von Datenträgern für den Server nicht unterstützt, wenn diese Einheitenklasse verwendet wird. Der z/OS Media-Server verwendet beim Füllen von FILE-Datenträgern ein FormatWrite-Feature des DFSMS Media Manager.

Sie können Datenträger für die Einheitenklasse FILE definieren, indem Sie den Befehl DEFINE VOLUME verwenden. Der z/OS Media-Server ordnet jedoch erst dann Speicherbereich für einen definierten Datenträger zu, wenn der Datenträger für seine erste Verwendung geöffnet wird.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-DEFine DEVclass--Einheitenklassenname--DEVType----FILE----->
                                     .-MAXCAPacity----10G---.
>--LIBRary----Kassettenarchivname--+-----+----->
                                     '-MAXCAPacity----Größe-'

    .-PRIMARYalloc----2600M-.    .-SECONDARYalloc----2600M-.
>--+-----+-----+-----+----->
    '-PRIMARYalloc----Größe-'    '-SECONDARYalloc----Größe-'

    .-PREFIX----ADSM-----.
>--+-----+-----+-----+----->
    '-PREFIX----Dateidatenträgerpräfix-'

    .-MOUNTLimit----20-----.
>--+-----+-----+-----+-----<
    '-MOUNTLimit----Anzahl-'
```

## Parameter

DEVType=FILE (Erforderlich)

Gibt an, dass der Einheitentyp FILE der Einheitenklasse zugeordnet wird.

LIBRARY (Erforderlich)



Gibt den Namen eines Kassettenarchivs an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde. Auf den Plattenspeicher, der von dieser Einheitenklasse verwendet wird, wird von dem z/OS Media-Server zugegriffen, und der Plattenspeicher wird von SMS verwaltet.

Informationen zum Definieren eines Kassettenarchivs befinden sich unter dem Befehl DEFINE LIBRARY.

#### MAXCAPacity

Gibt die maximale Größe der Dateidatenträger an, die für einen Speicherpool in dieser Einheitenklasse definiert sind. Dieser Parameter ist wahlfrei. Der Standardwert ist 10 GB (MAXCAPACITY=10G).

Dieser Wert muss als ganze Zahl gefolgt von einem K (KB), M (MB), G (GB) oder T (TB) angegeben werden. Die Mindestgröße ist 1 MB (MAXCAPACITY=1M). Die maximale Größe ist 16384 GB (MAXCAPACITY=16384G).

#### PRIMARYalloc

Gibt den anfänglichen Speicherbereich an, der dynamisch zugeordnet wird, wenn ein neuer Datenträger geöffnet wird. Es muss genügend Speicherbereich verfügbar sein, um den Wert für die primäre Bereichszuordnung zu erfüllen. Die SMS-Richtlinie (SMS = Storage Management Subsystem) bestimmt, ob mehrere physische Datenträger verwendet werden können, um die Anforderung zur primären Bereichszuordnung zu erfüllen.

Dieser Parameter ist wahlfrei. Dieser Wert muss als ganze Zahl gefolgt von einem K (KB), M (MB), G (GB) oder T (TB) angegeben werden. Die Mindestgröße ist 100 KB (PRIMARYALLOC=100K). Die maximale Größe ist 16384 GB (MAXCAPACITY=16384G). Die Standardgröße ist 2600 MB (PRIMARYALLOC=2600M). Alle Werte werden auf das nächsthöhere Vielfache von 256 KB gerundet.

Um eine ineffiziente Speichernutzung zu vermeiden, verwendet die Operation für die dynamische Zuordnung den kleineren der in den beiden Parametern PRIMARYALLOC und MAXCAPACITY angegebenen Werte.

SMS-Routinen für die automatische Klassenauswahl können Einfluss darauf haben, ob die Werte für die Parameter PRIMARYALLOC und SECONDARYALLOC verwendet werden.

#### SECONDARYalloc

Gibt den Speicherbereich an, um den ein Dateidatenträger erweitert wird, wenn der Speicherbereich, der dem Dateidatenträger bereits zugeordnet ist, verbraucht ist. Die Datei für einen Dateidatenträger wird bis zu der Größe erweitert, die mit dem Parameter MAXCAPACITY definiert ist. Danach wird der Datenträger als voll markiert.

Da sich die sekundäre Bereichszuordnung einer linearen Datei nicht über physische Datenträger erstrecken kann, muss bei der Auswahl der Größe für die sekundäre Bereichszuordnung die Größe des physischen Datenträgers berücksichtigt werden. Beispielsweise haben physische Datenträger für ein 3390 Modell 3 eine Größe von ungefähr 2,8 GB. Um sicherzustellen, dass mit jeder Erweiterungsanforderung ungefähr der gesamte physische Datenträger belegt wird (aber nicht mehr), verwenden Sie eine Größe für die sekundäre Bereichszuordnung, die gerade unter 2,8 GB liegt. Mit einer Größe von 2600 MB für die sekundäre Bereichszuordnung wird genügend Speicherbereich für die VSAM-Datenträgerdatei, den Datenträgerkennsatz und das Datenträgerinhaltsverzeichnis zugeordnet.

Dieser Parameter ist wahlfrei. Dieser Wert muss als ganze Zahl gefolgt von einem K (KB), M (MB), G (GB) oder T (TB) angegeben werden. Der Mindestwert ist 0 KB (SECONDARYALLOC=0K). Der Standardwert ist 2600 MB. Der Maximalwert ist 16384 GB. Mit Ausnahme von 0 werden alle Werte auf das nächsthöhere Vielfache von 256 KB gerundet.

Geben Sie 0 (SECONDARYALLOC=0) an, kann der Dateidatenträger nicht über den Wert der primären Bereichszuordnung hinaus erweitert werden.

SMS-Routinen für die automatische Klassenauswahl können Einfluss darauf haben, ob die Werte für die Parameter PRIMARYALLOC und SECONDARYALLOC verwendet werden.

Wenn Sie einen Wert für den Parameter SECONDARYALLOCATION angeben, der nicht 0 ist, oder wenn Sie den Standardwert 2600M akzeptieren, muss für die SMS DATACLAS, der die PREFIX-Kennung zugeordnet ist (z. B. Qualifikationsmerkmal der höheren Ebene), das Attribut für die erweiterte Adressierbarkeit (Extended Addressability - EA) angegeben werden. Ohne das EA-Attribut beschränkt die SMS DATACLAS die Zuordnung des linearen VSAM-FILE-Datenträgers auf den primären Bereich. (Siehe die Beschreibung des Parameters PRIMARYALLOCATION). Wenn die Datei auf die primäre Bereichszuordnung beschränkt ist, kann die Datei vom z/OS Media-Server nicht erweitert werden, und der Datenträger wird als FULL markiert, bevor die maximale Kapazität erreicht ist.

Einschränkung: Stellen Sie sicher, dass sich die für die Parameter PRIMARYALLOC und SECONDARYALLOC angegebenen Werte innerhalb praktischer Grenzwerte für die Speichereinheit befinden. Der Server kann nicht überprüfen, ob die Werte praktische Grenzwerte für die Einheit überschreiten, und der Server überprüft nicht, ob die beiden Werte zusammen die aktuelle Einstellung für MAXCAPACITY überschreiten.

Tipp: Um bei der Angabe eines hohen Werts für den Parameter MAXCAPACITY Datenträger zu füllen, geben Sie hohe Werte für die Parameter PRIMARYALLOC und SECONDARYALLOC an. Verwenden Sie höhere MVS-Datenträgergrößen, um die Möglichkeit eines Erweiterungsfehlers zu reduzieren.

#### PREFIX

Gibt die Kennung der oberen Ebene des Dateinamens an, mit der Dateien von Arbeitsdatenträgern zugeordnet werden. Bei allen in dieser Einheitenklasse erstellten Arbeitsdateidatenträgern verwendet der Server dieses Präfix für die Erstellung des Dateinamens. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge des Präfix, einschließlich Punkte, beträgt 32 Zeichen.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

```
AB.CD2.E
```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für einen Dateidatenträger unter Verwendung des Standardpräfixes ist ADSM.B0000021.BFS.

Wenn Sie eine Namenskonvention für Dateinamen haben, verwenden Sie ein Präfix, das Ihrer Namenskonvention entspricht. Der folgende Wert ist beispielsweise zulässig: TSM.SERVER2.VSAMFILE.

Wenn Sie mehrere Serverinstanzen für IBM Spectrum Protect oder Tivoli Storage Manager for z/OS Media ausführen, müssen Sie einen eindeutigen Wert für den Parameter PREFIX für jede definierte Einheitenklasse verwenden.

#### MOUNTLimit

Gibt die maximale Anzahl FILE-Datenträger an, die gleichzeitig für diese Einheitenklasse geöffnet sein können. Dieser Parameter ist wahlfrei. Der Standardwert ist 20.

Wenn Sie Einheiten IBM® 3995 verwenden, die Einheiten 3390 emulieren, definieren Sie keinen höheren Wert als die Anzahl der parallelen Eingabe- oder Ausgabedatenströme, die auf den physischen Medien möglich sind.

Der in diesem Parameter angegebene Wert ist wichtig, wenn das Umschalten von einem Datenträger zu einem anderen eine große Beeinträchtigung darstellt. Das Umschalten kann beispielsweise erfolgen, wenn Sie Einheiten IBM 3995 verwenden, um Einheiten 3390 zu emulieren. Der angegebene Wert darf nicht höher als die Anzahl der physischen Laufwerke sein, die auf der Einheit verfügbar sind.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

## DEFINE DOMAIN (Neue Maßnahmendomäne definieren)

Mit diesem Befehl kann eine neue Maßnahmendomäne definiert werden. Eine Maßnahmendomäne enthält Maßnahmengruppen, Verwaltungsklassen und Kopiengruppen. Ein Client wird einer Maßnahmendomäne zugeordnet. Die AKTIVE Maßnahmengruppe in der Maßnahmendomäne bestimmt die Regeln für Clients, die der Domäne zugeordnet werden. Die Regeln steuern die Archivierungsservices, Sicherungsservices und Speicherverwaltungsservices, die für die Clients zur Verfügung gestellt werden.

Eine Maßnahmengruppe muß in der Domäne aktiviert werden, bevor die der Maßnahmendomäne zugeordneten Clients Dateien sichern, archivieren oder umlagern können.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DEFine Domain--Domänenname----->
>--+-----+----->
' -DESCRiption----Beschreibung-'
. -BACKREtention----30---. . -ARCHREtention----365--.
>--+-----+----->
' -BACKREtention----Tage-' ' -ARCHREtention----Tage-'
>--+-----+-----><
| .-,------. |
| v |
' -ACTIVEDESTination-----Name_des_Pools_für_aktive_Daten----+'
```

## Parameter

### Domänenname (Erforderlich)

Gibt den Namen der zu definierenden Maßnahmendomäne an. Die maximale Länge dieses Namens beträgt 30 Zeichen.

### DESCRiption

Beschreibung der Maßnahmendomäne. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

### BACKRETention

Gibt die Anzahl Tage an (ab dem Datum, an dem die Sicherungsversionen inaktiv wurden), die Sicherungsversionen von Dateien aufbewahrt werden sollen, die sich nicht mehr im Client-Dateisystem befinden. Dieser Parameter ist wahlfrei. Zulässige Werte sind ganze Zahlen von 0 bis 9999. Der Standardwert ist 30. Der Server verwendet den Wert für den Aufbewahrungszeitraum für Sicherung, um inaktive Versionen von Dateien zu verwalten, wenn eine der folgenden Bedingungen zutrifft:

- Eine Datei wird an eine neue Verwaltungsklasse erneut gebunden, aber die neue Verwaltungsklasse und die Standardverwaltungsklasse enthalten keine Sicherungskopiengruppe.
- Die Verwaltungsklasse, an die eine Datei gebunden ist, ist nicht mehr vorhanden. Die Standardverwaltungsklasse enthält keine Sicherungskopiengruppe.
- Die Sicherungskopiengruppe wird aus der Verwaltungsklasse gelöscht, an die eine Datei gebunden ist. Die Standardverwaltungsklasse enthält keine Sicherungskopiengruppe.

### ARCHRETention

Gibt die Anzahl Tage an (ab dem Datum der Archivierung), die Archivierungskopien aufbewahrt werden sollen. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 30000 angeben. Der Standardwert ist 365. Der Server verwendet den Wert für den Aufbewahrungszeitraum für Archivierung, um Archivierungskopien von Dateien zu verwalten, wenn eine der folgenden Bedingungen zutrifft:

- Die Verwaltungsklasse, an die eine Datei gebunden ist, ist nicht mehr vorhanden. Die Standardverwaltungsklasse enthält keine Archivierungskopiengruppe.
- Die Archivierungskopiengruppe wird aus der Verwaltungsklasse gelöscht, an die eine Datei gebunden ist. Die Standardverwaltungsklasse enthält keine Archivierungskopiengruppe.

### ACTIVEDESTination

Dieser optionale Parameter gibt die Namen der Pools für aktive Daten an, in denen aktive Versionen von Sicherungsdaten für Knoten gespeichert werden, die der Domäne zugeordnet sind. Sie können bis zu 10 Pools für aktive Daten, die durch Kommas getrennt werden müssen, für eine Domäne angeben. Leerzeichen zwischen den Namen sind nicht zulässig.

Bevor der IBM Spectrum Protect-Server Daten in einen Pool für aktive Daten schreibt, überprüft er, ob der Knoten, der Eigner der Daten ist, einer Domäne zugeordnet ist, für die der Pool für aktive Daten in der ACTIVEDESTINATION-Liste aufgelistet ist. Stellt der Server fest, dass der Knoten diese Kriterien erfüllt, werden die Daten im Pool für aktive Daten gespeichert. Werden die Kriterien vom Knoten nicht erfüllt, werden die Daten nicht im Pool für aktive Daten gespeichert. Werden mit der Funktion für simultanes Schreiben Daten in einen Pool für aktive Daten geschrieben, führt der Server die Prüfung, ob der Knoten die Kriterien erfüllt, während Sicherungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder durch Anwendungsclients unter Verwendung der IBM Spectrum Protect-API aus. Die Prüfung wird auch durchgeführt, wenn aktive Daten mit dem Befehl COPY ACTIVE DATA kopiert werden.

## Beispiel: Eine Maßnahmendomäne definieren

Eine Maßnahmendomäne mit dem Namen PROG1 und der Beschreibung "Programming Group Domain" definieren. Angeben, daß Archivierungskopien 90 Tage aufbewahrt werden sollen, wenn Verwaltungsklassen oder Archivierungskopiengruppen gelöscht werden und die Standardverwaltungsklasse keine Archivierungskopiengruppe enthält. Außerdem angeben, dass Sicherungsversionen 60 Tage aufbewahrt werden sollen, wenn Verwaltungsklassen oder Kopiengruppen gelöscht werden und die Standardverwaltungsklasse keine Sicherungskopiengruppe enthält.

```
define domain prog1
description="Programming Group Domain"
backretention=60 archretention=90
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE DOMAIN

| Befehl             | Beschreibung                                       |
|--------------------|--|
| ACTIVATE POLICYSET | Wertet eine Maßnahmengruppe aus und aktiviert sie. |
| COPY DOMAIN        | Erstellt eine Kopie einer Maßnahmendomäne.         |



2. ACSDRVID ist erforderlich für Laufwerke in ACSLS-Kassettenarchiven. Dieser Parameter ist nicht gültig für Nicht-ACSLs-Kassettenarchive.
3. Der Parameter CLEANFREQUENCY ist nur für Laufwerke in SCSI-Kassettenarchiven gültig.
4. Der Parameterwert CLEANFREQUENCY=ASNEEDED funktioniert nicht bei allen Bandlaufwerken. Weitere Informationen enthält die Parameterbeschreibung.

## Parameter

---

### Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, dem das Laufwerk zugeordnet ist. Dieser Parameter ist erforderlich für alle Laufwerke, einschließlich eigenständiger Laufwerke. Das angegebene Kassettenarchiv muss zuvor mit dem Befehl DEFINE LIBRARY definiert werden.

### Laufwerkname (Erforderlich)

Gibt den Namen an, der dem Laufwerk zugeordnet ist. Die maximale Länge dieses Namens beträgt 30 Zeichen.

### SERIAL

Gibt die Seriennummer des Laufwerks an, das definiert wird. Dieser Parameter ist wahlfrei. Der Standardwert ist AUTODETECT.

Bei SERIAL=AUTODETECT wird die vom Laufwerk bei der Definition des Pfads gemeldete Seriennummer als Seriennummer verwendet.

Bei SERIAL=*Seriennummer* wird die eingegebene Seriennummer verwendet, um zu überprüfen, ob der Pfad zum Laufwerk korrekt ist, wenn der Pfad definiert wird.

Anmerkung: Je nach Leistungsspektrum der Einheit wird SERIAL=AUTODETECT möglicherweise nicht unterstützt. In diesem Fall wird die Seriennummer als leer gemeldet.

### ONLine

Gibt an, ob das Laufwerk für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

#### Yes

Gibt an, dass das Laufwerk für die Verwendung verfügbar ist.

#### No

Gibt an, dass das Laufwerk nicht für die Verwendung verfügbar ist.

### ELEMent

Gibt die Elementadresse eines Laufwerks in einem SCSI- oder VTL-Archiv (VTL - Virtual Tape Library) an. Der Server verwendet die Elementadresse, um die physische Adresse des Laufwerks mit der SCSI- oder VTL-Adresse des Laufwerks zu verbinden. Der Standardwert ist AUTODETECT.

Bei ELEMENT=AUTODETECT wird die Elementnummer automatisch vom Server erkannt, wenn der Pfad zu dem Laufwerk definiert ist.


Zum Lokalisieren der Elementadresse für die Archivkonfiguration die Informationen des Herstellers zu Rate ziehen.

#### Einschränkung:

- Der Parameter ELEMENT ist nur für Laufwerke in SCSI-Kassettenarchiven oder virtuellen Bandarchiven (VTLs) gültig, wenn das Laufwerk kein an ein Netz angeschlossenes SCSI-Laufwerk (NAS) ist.
- Dieser Parameter ist nicht gültig, wenn der Befehl von einem Kassettenarchivclientserver ausgegeben wird (d. h., wenn der Kassettenarchivtyp SHARED ist).
- Je nach Leistungsspektrum des Kassettenarchivs wird ELEMENT=AUTODETECT möglicherweise nicht unterstützt. In diesem Fall müssen Sie die Elementadresse angeben.

### ACSDRVID

Gibt die ID des Laufwerks an, auf das in einem ACSLS-Kassettenarchiv zugegriffen wird. Die Laufwerk-ID ist eine Zahlengruppe, die die physische Adresse eines Laufwerks in einem ACSLS-Kassettenarchiv angibt. Diese Laufwerk-ID muss als *a,l,p,d*, angegeben werden, wobei *a* die ACSID, *l* das LSM (Library Storage Module), *p* die Anzeigennummer und *d* die Laufwerk-ID ist. Der Server benötigt die Laufwerk-ID, um die physische Adresse des Laufwerks mit der SCSI-Adresse des Laufwerks zu verbinden. Die StorageTek-Dokumentation enthält ausführliche Informationen.

Einschränkung: Um ACSLS-Funktionen verwenden zu können, ist die Installation von StorageTek Library Attach-Software erforderlich.

### CLEANFREQuency

Gibt an, wie oft der Server die Laufwerkreinigung aktiviert. Dieser Parameter ist wahlfrei. Um die Reinigung für ein automatisiertes Kassettenarchiv nahezu vollständig zu automatisieren, müssen Sie eine Reinigungskassette haben, die in den Datenträgerbestand des Kassettenarchivs zurückgestellt wird.

Bei Verwendung der speicherarchivbasierten Reinigung wird NONE empfohlen, wenn Ihr Speicherarchivtyp diese Funktion unterstützt.

Dieser Parameter ist für extern verwaltete Kassettenarchive, wie beispielsweise 3494-Kassettenarchive oder StorageTek-Kassettenarchive, die unter ACSLS verwaltet werden, nicht gültig.

Wichtig: Es gibt einige Besonderheiten, die beachtet werden müssen, wenn die vom Server aktivierte Laufwerkreinigung bei einem SCSI-Kassettenarchiv verwendet werden soll, das eine automatische Laufwerkreinigungsunterstützung in seiner Einheitenhardware zur Verfügung stellt.

#### NONE

Gibt an, dass der Server die Reinigung dieses Laufwerks nicht verfolgt. Dieser Wert kann für Kassettenarchive verwendet werden, die über ihre eigene automatische Reinigungsunterstützung verfügen.

#### ASNEEDED

Gibt an, dass der Server das Laufwerk mit einer zurückgestellten Reinigungskassette nur lädt, wenn ein Laufwerk dem Einheitenreiber mitteilt, dass eine Reinigung erforderlich ist.

Der Parameterwert CLEANFREQUENCY=ASNEEDED funktioniert nicht bei allen Bandlaufwerken. Detaillierte Laufwerkdaten finden Sie auf der Website für unterstützte Einheiten für Ihr Betriebssystem. Wird ASNEEDED nicht unterstützt, können Sie den Gigabyte-Wert für die automatische Reinigung verwenden.

Für IBM 3592- und LTO-Laufwerke wird die speicherarchivbasierte Reinigung empfohlen. Wird die speicherarchivbasierte Reinigung nicht unterstützt, muss ASNEEDED verwendet werden. Gigabyte wird nicht empfohlen.

Einschränkung: IBM Spectrum Protect steuert nicht die Laufwerke, die mit dem NAS-Dateiserver verbunden sind. Ist ein Laufwerk nur mit einem NAS-Dateiserver verbunden (keine Verbindung zu einem Speicheragenten oder Server), geben Sie nicht ASNEEDED für die Häufigkeit der Reinigung an.

#### Gigabyte

Gibt in Gigabyte an, wieviel Daten auf dem Laufwerk verarbeitet werden, bevor der Server das Laufwerk mit einer Reinigungskassette lädt. Der Server setzt den Zähler für die verarbeiteten Gigabyte zurück, wenn eine Reinigungskassette in das Laufwerk geladen wird.

Wichtig: Bei CLEANFREQUENCY=Gigabyte kann die Laufwerkreinigung erfolgen, bevor die Einstellung für Gigabyte erreicht ist, wenn das Laufwerk den Einheitenreiber benachrichtigt, dass eine Reinigung erforderlich ist.

Lesen Sie die Empfehlungen des Laufwerkherstellers bezüglich der Reinigung. Werden Empfehlungen für die Reinigungshäufigkeit in Stunden der Verwendung gegeben, führen Sie wie folgt eine Umrechnung in einen Gigabytewert durch:

1. Verwenden Sie den Wert für Byte pro Sekunde des Laufwerks, um einen Wert für Gigabyte pro Stunde zu ermitteln.
2. Multiplizieren Sie den Wert für Gigabyte pro Stunde mit den empfohlenen Stunden der Verwendung zwischen den Reinigungen.
3. Verwenden Sie das Ergebnis als Wert für die Reinigungshäufigkeit.

Bei Verwendung der Reinigungshäufigkeit, die von IBM® für IBM Laufwerke empfohlen wird, wird sichergestellt, dass die Reinigung der Laufwerke nicht zu oft durchgeführt wird.

Geben Sie für IBM 3590-Laufwerke einen Gigabyte-Wert für die Reinigungshäufigkeit an, um eine adäquate Reinigung der Laufwerke sicherzustellen.

## Beispiel: Ein Laufwerk für ein Kassettenarchiv definieren

---

Ein Laufwerk in einem manuellen Kassettenarchiv mit dem Kassettenarchivnamen LIB01 und dem Laufwerknamen DRIVE01 definieren.

```
define drive lib01 drive01
```

#### AIX-Betriebssysteme

```
define path server01 drive01 srctype=server desttype=drive  
library=lib01 device=/dev/rmt0
```

#### Linux-Betriebssysteme

```
define path server01 drive01 srctype=server desttype=drive  
library=lib01 device=/dev/tmscsi/mt0
```

#### Windows-Betriebssysteme

```
define path server01 drive01 srctype=server desttype=drive  
library=lib01 device=mt3.0.0.0
```

## Beispiel: Ein Laufwerk in einem ACSLS-Kassettenarchiv definieren

---

Ein Laufwerk in einem ACSLS-Kassettenarchiv mit dem Kassettenarchivnamen ACSLIB und dem Laufwerknamen ACSDRV1 definieren.

```
define drive acslib acsdrv1 acsdrvid=1,2,3,4
```

#### AIX-Betriebssysteme

```
define path server01 acsdrv1 srctype=server desttype=drive  
library=acslib device=/dev/rmt0
```

#### Linux-Betriebssysteme

```
define path server01 acsdrv1 srctype=server desttype=drive  
library=acslib device=/dev/tmscsi/mt0
```

#### Windows-Betriebssysteme

```
define path server01 acsdrv1 srctype=server desttype=drive  
library=acslib device=mt3.0.0.0
```

## Beispiel: Ein Laufwerk in einem automatisierten Kassettenarchiv definieren

Ein Laufwerk in einem automatisierten Kassettenarchiv mit dem Kassettenarchivnamen AUTO8MMLIB und dem Laufwerknamen DRIVE01 definieren.

```
define drive auto8mmlib drive01 element=82
```

#### AIX-Betriebssysteme

```
define path server01 drive01 srctype=server desttype=drive  
library=auto8mmlib device=/dev/rmt0
```

#### Linux-Betriebssysteme

```
define path server01 drive01 srctype=server desttype=drive  
library=auto8mmlib device=/dev/tmscsi/mt0
```

#### Windows-Betriebssysteme

```
define path server01 drive01 srctype=server desttype=drive  
library=auto8mmlib device=mt3.0.0.0
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE DRIVE

| Befehl            | Beschreibung  |
|-------------------|---|
| DEFINE LIBRARY    | Definiert ein automatisiertes oder manuelles Kassettenarchiv.       |
| DEFINE PATH       | Definiert einen Pfad von einer Quelle zu einem Ziel.                |
| DELETE DRIVE      | Löscht ein Laufwerk aus einem Kassettenarchiv.                      |
| DELETE LIBRARY    | Löscht ein Kassettenarchiv.   |
| PERFORM LIBACTION | Definiert alle Laufwerke und Pfade für ein Kassettenarchiv.         |
| QUERY DRIVE       | Zeigt Informationen zu Laufwerken an.                               |
| QUERY LIBRARY     | Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an. |
| QUERY PATH        | Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.     |
| UPDATE DRIVE      | Ändert die Attribute eines Laufwerks.                               |
| UPDATE PATH       | Ändert die zu einem Pfad gehörigen Attribute.                       |

## DEFINE EVENTSERVER (Server als Ereignisserver definieren)

Mit diesem Befehl kann ein Server als Ereignisserver definiert werden.

Wird ein Ereignisserver definiert, kann ein IBM Spectrum Protect-Server Ereignisse an einen anderen IBM Spectrum Protect-Server senden, der diese Ereignisse protokolliert.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-DEFine EVENTSERVER--Servername-----><
```

## Parameter

---

Servername (Erforderlich)

Gibt den Namen des Ereignis-Servers an. Der angegebene Server muss bereits mit dem Befehl DEFINE SERVER definiert worden sein.

## Beispiel: Den Ereignisserver definieren

---

ASTRO als Ereignisserver definieren.

```
define eventserver astro
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für DEFINE EVENTSERVER

| Befehl             | Beschreibung   |
|--------------------|--|
| DEFINE SERVER      | Definiert einen Server für die Übertragung zwischen Servern. |
| DELETE EVENTSERVER | Löscht Verweise auf den Ereignisserver.                      |
| DISABLE EVENTS     | Inaktiviert bestimmte Ereignisse für Empfänger.              |
| ENABLE EVENTS      | Aktiviert bestimmte Ereignisse für Empfänger.                |
| PING SERVER        | Testet die Verbindungen zwischen Servern..                   |
| QUERY EVENTSERVER  | Zeigt den Namen des Ereignisservers an.                      |
| QUERY SERVER       | Zeigt Informationen über Server an.                          |

### Zugehörige Informationen:

☛ Unternehmensweite Ereignisprotokollierung: Ereignisse auf einem anderen Server protokollieren

## DEFINE GRPMEMBER (Server zu einer Servergruppe hinzufügen)

---

Mit diesem Befehl kann ein Server als Teil einer Servergruppe hinzugefügt werden. Es kann auch eine Servergruppe zu einer anderen Servergruppe hinzugefügt werden. Mit Hilfe einer Servergruppe können Befehle an mehrere Server weitergeleitet werden, indem nur der Name der Servergruppe angegeben wird.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
          .-,-----.  
          v          |  
>>-DEFine GRPMEMber--Gruppenname----Name_des_Teils-+-----><
```

## Parameter

---

Gruppenname (Erforderlich)

Gibt den Namen der Servergruppe an, der das Teil hinzugefügt wird.

Name\_des\_Teils (Erforderlich)

Gibt die Namen der Server oder Gruppen an, die der Gruppe hinzugefügt werden sollen. Sollen mehrere Server und Gruppen angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Die Server oder Servergruppen müssen bereits für den Server definiert sein.



## Beispiel: Einen Server für eine Servergruppe definieren

Den Server SANJOSE für Server-Gruppe CALIFORNIA definieren.

```
define grpmember california sanjose
```

## Beispiel: Einen Server und eine Servergruppe für eine Servergruppe definieren

Den Server TUCSON und die Server-Gruppe CALIFORNIA für Server-Gruppe WEST\_COMPLEX definieren.

```
define grpmember west_complex tucson,california
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE GRPMEMBER



| Befehl             | Beschreibung   |
|--------------------|--|
| DEFINE SERVER      | Definiert einen Server für die Übertragung zwischen Servern. |
| DEFINE SERVERGROUP | Definiert eine neue Servergruppe.                            |
| DELETE GRPMEMBER   | Löscht einen Server aus einer Servergruppe.                  |
| DELETE SERVERGROUP | Löscht eine Servergruppe.                                    |
| MOVE GRPMEMBER     | Versetzt einen Teil einer Servergruppe.                      |
| QUERY SERVER       | Zeigt Informationen über Server an.                          |
| RENAME SERVERGROUP | Benennt eine Servergruppe um.                                |
| UPDATE SERVERGROUP | Aktualisiert eine Servergruppe.                              |

## DEFINE LIBRARY (Kassettenarchiv definieren)




Mit diesem Befehl kann ein Kassettenarchiv definiert werden. Ein Kassettenarchiv besteht aus einem oder mehreren Laufwerken und unter Umständen auch automatischen Einheiten (je nach Kassettenarchivtyp), über die auf Speicherdatenträger zugegriffen werden kann.


Auf ein Kassettenarchiv kann nur von einer Quelle zugegriffen werden: einem IBM Spectrum Protect-Server oder einer Einheit zum Versetzen von Daten. Auf die Laufwerke in einem Kassettenarchiv können jedoch mehrere Quellen zugreifen.

Die folgenden Kassettenarchivtypen können für den Server definiert werden. Syntax- und Parameterbeschreibungen sind für jeden Typ verfügbar.

- DEFINE LIBRARY (349X-Kassettenarchiv definieren)
- DEFINE LIBRARY (ACSLs-Kassettenarchiv definieren)
- DEFINE LIBRARY (Externes Kassettenarchiv definieren)
- DEFINE LIBRARY (Kassettenarchiv FILE definieren)
- DEFINE LIBRARY (Manuelles Kassettenarchiv definieren)
- DEFINE LIBRARY (SCSI-Kassettenarchiv definieren)
- DEFINE LIBRARY (Gemeinsam genutztes Kassettenarchiv definieren)
- DEFINE LIBRARY (VTL-Speicherarchiv definieren)
-  AIX-Betriebssysteme  Linux-Betriebssysteme DEFINE LIBRARY (Speicherarchivtyp ZOSMEDIA definieren)

Ausführliche und aktuelle Informationen zur Kassettenarchivunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

-  AIX-Betriebssysteme  Windows-Betriebssysteme Supported devices for AIX and Windows
-  Linux-Betriebssysteme Supported devices for Linux

 Windows-Betriebssysteme

Um Banddatenträger in SCSI-Speicherarchiven automatisch zu kennzeichnen, verwenden Sie den Parameter AUTOLABEL in den Befehlen DEFINE LIBRARY und UPDATE LIBRARY. Wird dieser Parameter verwendet, ist es nicht erforderlich, eine Gruppe von Bändern vorab zu kennzeichnen. Außerdem ist die Verwendung dieses Parameters effizienter als die Verwendung des Befehls LABEL LIBVOLUME, der es erfordert, dass Datenträger separat bereitgestellt werden. Wenn Sie den Parameter AUTOLABEL verwenden, müssen Sie Bänder zurückstellen, indem Sie CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME angeben.

Ein Kennsatz darf keine eingebetteten Leerzeichen oder Punkte enthalten und muss gültig sein, wenn er als Dateiname auf den Datenträgern verwendet wird.

Sie müssen CD-ROM-, Zip- oder Jaz-Datenträger mit den Dienstprogrammen des Einheitenherstellers oder den Windows-Dienstprogrammen kennzeichnen, da IBM Spectrum Protect keine Dienstprogramme zum Formatieren oder Kennzeichnen dieser Datenträgertypen bereitstellt. Die Dienstprogramme des Betriebssystems schließen das Plattenverwaltungsprogramm (Disk Administrator) (eine grafische Benutzerschnittstelle) und den Befehl zum Zuordnen von Kennsätzen ein.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE LIBRARY

| Befehl             | Beschreibung  |
|--------------------|---|
| AUDIT LIBRARY      | Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet. |
| CHECKIN LIBVOLUME  | Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.                            |
| CHECKOUT LIBVOLUME | Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.                          |
| DEFINE DRIVE       | Ordnet ein Laufwerk einem Kassettenarchiv zu.   |
| DEFINE PATH        | Definiert einen Pfad von einer Quelle zu einem Ziel.  |
| DEFINE SERVER      | Definiert einen Server für die Übertragung zwischen Servern.  |
| DELETE DRIVE       | Löscht ein Laufwerk aus einem Kassettenarchiv.  |
| DELETE LIBRARY     | Löscht ein Kassettenarchiv.   |
| DELETE PATH        | Löscht einen Pfad von einer Quelle zu einem Ziel.   |
| LABEL LIBVOLUME    | Kennzeichnet Datenträger in manuellen oder automatisierten Kassettenarchiven.                       |
| PERFORM LIBACTION  | Definiert alle Laufwerke und Pfade für ein Kassettenarchiv.   |
| QUERY DRIVE        | Zeigt Informationen zu Laufwerken an.   |
| QUERY LIBRARY      | Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.                                 |
| QUERY LIBVOLUME    | Zeigt Informationen zu einem Datenträger im Kassettenarchiv an.                                     |
| QUERY PATH         | Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.                                     |
| UPDATE DRIVE       | Ändert die Attribute eines Laufwerks.   |
| UPDATE LIBRARY     | Ändert die Attribute eines Kassettenarchivs.  |
| UPDATE LIBVOLUME   | Ändert den Status eines Speicherdatenträgers.   |
| UPDATE PATH        | Ändert die zu einem Pfad gehörigen Attribute.   |

## DEFINE LIBRARY (349X-Kassettenarchiv definieren)

Verwenden Sie diese Syntax, um ein 349X-Kassettenarchiv zu definieren.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-DEFine LIBRARY--Speicherarchivname--LIBType-----349X----->
      .-SHARED-----No----- .-RESETDrives-----No-----
>-----+-----+-----+-----+-----+-----+----->
      '-SHARED-----+Yes-+-' | (1) |
          '-No--'      '-RESETDrives-----+Yes-+-----'
                          '-No--'
```

```

.-AUTOLabel---Yes-----
>-----+----->
' -AUTOLabel---+No-----+
      +-Yes-----+
      '-OVERWRITE-'

.-SCRATCHCAteGory---301----
>-----+----->
' -SCRATCHCAteGory---Nummer-'

.-PRIVATECAteGory---300----
>-----+----->
' -PRIVATECAteGory---Nummer-'

>-----+-----<
' -WORMSCRatchcategory---Nummer-'

```

#### Anmerkungen:

1. Der Standardwert des Parameters RESETDRIVES ist situationsabhängig. Wenn der Parameter SHARED auf NO gesetzt ist, ist NO der Wert des Parameters RESETDRIVES. Wenn der Parameter SHARED auf YES gesetzt ist, ist YES der Wert des Parameters RESETDRIVES.


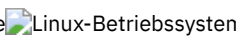
## Parameter


---

### Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

### LIBType=349X (Erforderlich)

  Gibt an, dass das Kassettenarchiv ein IBM 3494 oder 3495 Tape Library Dataserver ist.

 Gibt an, dass das Kassettenarchiv ein IBM 3494 Tape Library Dataserver oder ein IBM Tape System Library Manager ist, der einen 3494 Tape Library Dataserver emuliert.

Einschränkung: IBM 3494-Kassettenarchive unterstützen nur jeweils einen eindeutigen Einheitentyp.

### SHAREd

Gibt an, ob dieses Kassettenarchiv mit anderen Servern in einem Speicherbereichsnetz (Storage Area Network = SAN) gemeinsam genutzt wird. Dieser Parameter ist erforderlich, wenn Sie ein Kassettenarchiv für den Kassettenarchivmanager definieren.

#### YES

Gibt an, dass dieses Kassettenarchiv mit anderen Servern gemeinsam genutzt werden kann. Wird YES angegeben, lädt der Kassettenarchivmanagerserver Datenträger, die von anderen Servern angefordert werden, und verfolgt die Laufwerk- und Datenträgerzuordnung zu anderen Servern.

#### NO

Gibt an, dass dieses Kassettenarchiv nicht mit anderen Servern gemeinsam genutzt werden kann. SHARED=NO ist erforderlich, wenn das Kassettenarchiv durch die Übergabe von Befehlen über einen NAS-Dateiserver gesteuert wird.

### AUTOLabel

Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

Einschränkung: Wenn Sie ein Kassettenarchiv definieren, das über Laufwerke verfügt, die an eine NAS-Einheit (NAS = Network-attached Storage) angeschlossen sind, müssen Sie den Befehl LABEL LIBVOLUME verwenden, um die Datenträger für dieses Kassettenarchiv zu kennzeichnen.

#### No

Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

#### Yes

Gibt an, dass der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

### OVERWRITE

Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze nur dann, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

### SCRATCHCAtegory

Gibt die Kategorienummer für Arbeitsdatenträger im Kassettenarchiv an. Dieser Parameter ist wahlfrei. Der Standardwert ist 301 (wird auf der Einheit IBM 3494 zu X'12D', da sie Hexadezimalwerte verwendet). Es kann eine Zahl von 1 bis 65279 angegeben werden. Diese Zahl muss eindeutig sein. Sie kann nicht mit anderen Anwendungen oder definierten Kassettenarchiven gemeinsam genutzt werden, und sie muss sich von den anderen Kategorienummern in diesem Kassettenarchiv unterscheiden.

### PRIVATECAtegory

Gibt die Kategorienummer für private Datenträger an, die nach Namen geladen werden müssen. Dieser Parameter ist wahlfrei. Der Standardwert ist 300 (dieser Wert wird auf der Einheit IBM 3494 zu X'12C', da sie Hexadezimalwerte verwendet). Es kann eine Zahl von 1 bis 65279 angegeben werden. Diese Zahl muss eindeutig sein. Sie kann nicht mit anderen Anwendungen oder definierten Kassettenarchiven gemeinsam genutzt werden, und sie muss sich von den anderen Kategorienummern in diesem Kassettenarchiv unterscheiden.


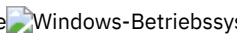
### WORMSCRatchcategory


Gibt die Kategorienummer an, die für WORM-Arbeitsdatenträger in dem Kassettenarchiv verwendet werden soll. Dieser Parameter ist erforderlich, wenn WORM-Datenträger verwendet werden. Es kann eine Zahl von 1 bis 65279 angegeben werden. Diese Zahl muss eindeutig sein. Sie kann nicht mit anderen Anwendungen oder definierten Kassettenarchiven gemeinsam genutzt werden, und sie muss sich von den anderen Kategorienummern in diesem Kassettenarchiv unterscheiden. Dieser Parameter ist nur bei Verwendung von WORM-Datenträgern 3592 gültig.

Einschränkung: Ist WORMSCRATCHCATEGORY nicht definiert und ist der Parameter WORM für die Einheitenklasse auf YES gesetzt, schlägt die Ladeoperation mit einer Fehlernachricht fehl.

### RESETDrives

Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird. Wenn beispielsweise ein Speicheragent nicht mehr verfügbar ist, aber noch den Pfad zu einem Laufwerk belegt, kann der Server mit der persistenten Reserve die Reservierung des Speicheragenten unterbrechen und auf das Laufwerk zugreifen.

  Wird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

 Wird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

In der folgenden Tabelle sind die drei möglichen Konfigurationen für Laufwerke beschrieben, die an NAS-Einheiten angeschlossen werden können.

Tabelle 1. Konfigurationen für Laufwerke, die an NAS-Einheiten angeschlossen sind

| Konfiguration der Speicherarchivereinheit   | Verhalten für persistente Reserve  |
|---|--|
| Die Speicherarchivereinheit wird an den IBM Spectrum Protect-Server angeschlossen, und die Bandlaufwerke werden vom Server und der NAS-Einheit gemeinsam genutzt. | Die Zurückstellung der Laufwerkreservierung wird unterstützt, wenn die NAS-Einheit die persistente Reserve unterstützt und diese aktiviert ist. Weitere Informationen zum Definieren der persistenten Reserve finden Sie in der Dokumentation für Ihre NAS-Einheit.  |
| Die Speicherarchivereinheit wird an den IBM Spectrum Protect-Server angeschlossen, und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen.            | Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben. |

#### Yes

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

#### No

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.



Yes

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

## Beispiel: Ein Kassettenarchiv 3494 definieren


Ein Kassettenarchiv mit dem Namen `my3494` mit der Arbeitsdatenträgerkategorie 550, der privaten Kategorie 600 und der WORM-Arbeitsdatenträgerkategorie 400 definieren.

```
define library my3494 libtype=349x scratchcategory=550
privatecategory=600 wormscratchcategory=400
```

## DEFINE LIBRARY (ACSLs-Kassettenarchiv definieren)

Verwenden Sie diese Syntax, um ein ACSLS-Kassettenarchiv zu definieren.

### Berechtigungsklasse

 Um ACSLS-Funktionen verwenden zu können, ist die Installation von StorageTek Library Attach-Software erforderlich.

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-DEFine LIBRary--Speicherarchivname--LIBType----ACSLs----->
. -SHARed-----No----- . -RESEtDrives-----No-----
>-+-----+-----+-----+-----+-----+-----+-----+----->
' -SHARed-----+Yes-+- ' | (1) |
      '-No--'      '-RESEtDrives-----+Yes-+-----'
                        '-No--'

. -AUTOLabel-----Yes-----
>-+-----+-----+-----+-----+-----+-----+-----+-----><
' -AUTOLabel-----+No-----+-----+-----+-----+-----+-----+----->
      +-Yes-----+
      '-OVERWRITE-'
```

Anmerkungen:

1. Der Standardwert des Parameters RESEtDRIVES ist situationsabhängig. Wenn der Parameter SHARed auf NO gesetzt ist, ist NO der Wert des Parameters RESEtDRIVES. Wenn der Parameter SHARed auf YES gesetzt ist, ist YES der Wert des Parameters RESEtDRIVES.

### Parameter

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType=ACSLs (Erforderlich)

Gibt an, dass es sich bei dem Kassettenarchiv um ein StorageTek-Kassettenarchiv handelt, das durch StorageTek Automated Cartridge System Library Software (ACSLs) gesteuert wird.

SHARed

Gibt an, ob dieses Kassettenarchiv mit anderen Servern in einem Speicherbereichsnetz (Storage Area Network = SAN) gemeinsam genutzt wird. Dieser Parameter ist erforderlich, wenn Sie ein Kassettenarchiv für den Kassettenarchivmanager definieren.

YES

Gibt an, dass dieses Kassettenarchiv mit anderen Servern gemeinsam genutzt werden kann. Wird YES angegeben, lädt der Kassettenarchivmanagerserver Datenträger, die von anderen Servern angefordert werden, und verfolgt die Laufwerk- und



Datenträgerzuordnung zu anderen Servern.


NO

Gibt an, dass dieses Kassettenarchiv nicht mit anderen Servern gemeinsam genutzt werden kann. SHARED=NO ist erforderlich, wenn das Kassettenarchiv durch die Übergabe von Befehlen über einen NAS-Dateiserver gesteuert wird.

#### RESETDrives

Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird. Wenn beispielsweise ein Speicheragent nicht mehr verfügbar ist, aber noch den Pfad zu einem Laufwerk belegt, kann der Server mit der persistenten Reserve die Reservierung des Speicheragenten unterbrechen und auf das Laufwerk zugreifen.

  Wird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

 Wird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberbene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

In der folgenden Tabelle sind die drei möglichen Konfigurationen für Laufwerke beschrieben, die an NAS-Einheiten angeschlossen werden können.

Tabelle 1. Konfigurationen für Laufwerke, die an NAS-Einheiten angeschlossen sind

| Konfiguration der Speicherarchiveinheit   | Verhalten für persistente Reserve  |
|---|--|
| Die Speicherarchiveinheit wird an den IBM Spectrum Protect-Server angeschlossen, und die Bandlaufwerke werden vom Server und der NAS-Einheit gemeinsam genutzt. | Die Zurückstellung der Laufwerkreservierung wird unterstützt, wenn die NAS-Einheit die persistente Reserve unterstützt und diese aktiviert ist. Weitere Informationen zum Definieren der persistenten Reserve finden Sie in der Dokumentation für Ihre NAS-Einheit.  |
| Die Speicherarchiveinheit wird an den IBM Spectrum Protect-Server angeschlossen, und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen.            | Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben. |

Yes

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.



Yes

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

#### AUTOLabel

Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

Einschränkung: Wenn Sie ein Kassettenarchiv definieren, das über Laufwerke verfügt, die an eine NAS-Einheit (NAS = Network-attached Storage) angeschlossen sind, müssen Sie den Befehl LABEL LIBVOLUME verwenden, um die Datenträger für dieses Kassettenarchiv zu kennzeichnen.

No

Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes

Gibt an, dass der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE

Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

ACSID (Erforderlich)

Gibt die Nummer dieses StorageTek-Kassettenarchivs an, das von ACSSA (Automatic Cartridge System System Administrator) zugeordnet wird. Hierbei kann es sich um eine Zahl von 0 bis 126 handeln. Geben Sie den Befehl QUERY ACS auf dem System aus, um die Nummer für die Kassettenarchiv-ID abzufragen. Dieser Parameter ist erforderlich.

Weitere Informationen enthält die StorageTek-Dokumentation.

## Beispiel: Ein gemeinsam genutztes ACSLS-Kassettenarchiv definieren

---

Ein Kassettenarchiv mit dem Namen ACSLIB, dem Kassettenarchivtyp ACSLS und der ACSID 1 definieren.

```
define library acslib libtype=acsls acsid=1 shared=yes
```

## DEFINE LIBRARY (Externes Kassettenarchiv definieren)

---

Verwenden Sie diese Syntax, um ein externes Kassettenarchiv zu definieren.

### Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

---

```
>>-DEFine LIBRary--Kassettenarchivname--LIBType-----EXternal---->
. -AUTOLabel-----Yes-----
>-----+-----+-----<
' -AUTOLabel-----+No-----+ '
      +-Yes-----+
      '-OVERWRITE- '
```

### Parameter



---

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType=EXternal (Erforderlich)

Gibt an, dass das Kassettenarchiv von einem externen Datenträgerverwaltungssystem verwaltet wird. Dieser Kassettenarchivtyp unterstützt keine mit dem Befehl DEFINE DRIVE erstellten Definitionen. Vielmehr bestimmt das externe Datenträgerverwaltungssystem das geeignete Laufwerk für Datenträgerzugriffsoperationen.

  In einer IBM Spectrum Protect for Storage Area Networks-Umgebung gibt dieser Parameter an, dass StorageTek Automated Cartridge System Library Software (ACSL) oder Library Station Software das Kassettenarchiv steuert. Software, wie beispielsweise Gresham EDT-DistribuTAPE, erlaubt es mehreren Servern, das Kassettenarchiv gemeinsam zu benutzen. Die Laufwerke in diesem Kassettenarchiv sind nicht für IBM Spectrum Protect definiert. ACSLS identifiziert das Laufwerk für Datenträgeroperationen.

AUTOLabel

Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

No

Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes




Gibt an, dass der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE




Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

## Beispiel: Ein externes Kassettenarchiv für eine SAN-Konfiguration definieren

Für eine IBM Spectrum Protect for Storage Area Networks-Konfiguration das Kassettenarchiv EXTLIB mit dem Kassettenarchivtyp EXTERNAL definieren. Bei Verwendung von Gresham Enterprise DistribuTAPE befindet sich die ausführbare Datei des externen Kassettenarchivmanagers in dem folgenden Verzeichnis:

-  AIX-Betriebssysteme/usr/lpp/dtelm/bin/elm
-  Linux-Betriebssysteme/opt/OMIdtelm/bin/elm
-  Windows-Betriebssystemec:\program files\GES\EDT\bin\elm.exe

Wenn Sie den IBM® Tape System Library Manager verwenden, befindet sich die ausführbare Datei des externen Kassettenarchivmanagers in dem folgenden Verzeichnis:

-  AIX-Betriebssysteme  Linux-Betriebssysteme/opt/IBM/TSLM/client/tsm/elm
-  Windows-Betriebssysteme...\IBM\rmm\client\tsm\elm.exe

Weitere Informationen befinden sich im *IBM Tape System Library Manager User's Guide* unter <http://www-01.ibm.com/support/docview.wss?uid=pub1ga32220802>.

1. Das Kassettenarchiv definieren:

```
define library extlib libtype=external
```

2. Den Pfad definieren:

 AIX-Betriebssysteme

```
define path server1 extlib srctype=server desttype=library  
externalmanager="/usr/lpp/dtelm/bin/elm"
```

 Linux-Betriebssysteme

```
define path server1 extlib srctype=server desttype=library  
externalmanager="/opt/OMIdtelm/bin/elm"
```

 Windows-Betriebssysteme

```
define path server1 extlib srctype=server desttype=library  
externalmanager="c:\program files\GES\EDT\bin\elm.exe"
```

## DEFINE LIBRARY (Kassettenarchiv FILE definieren)

Verwenden Sie diese Syntax, um ein Kassettenarchiv FILE zu definieren.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-DEFine LIBRARY--Speicherarchivname--LIBType-----FILE----->  
.-SHAREd-----No-----.  
>+-----+-----+-----+-----><  
'-SHAREd-----+Yes-+-'  
'-No--'
```





Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

No

Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes



Gibt an, daß der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.


OVERWRITE

Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

RESETDrives

Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird. Wenn beispielsweise ein Speicheragent nicht mehr verfügbar ist, aber noch den Pfad zu einem Laufwerk belegt, kann der Server mit der persistenten Reserve die Reservierung des Speicheragenten unterbrechen und auf das Laufwerk zugreifen.

  Wird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

 Wird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

Yes

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.



Yes

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

## Beispiel: Ein manuelles Kassettenarchiv definieren

---

Ein Kassettenarchiv mit Namen MANUALMOUNT und Kassettenarchivtyp MANUAL soll definiert werden.

```
define library manualmount libtype=manual
```

## DEFINE LIBRARY (SCSI-Kassettenarchiv definieren)

---

Verwenden Sie diese Syntax, um ein SCSI-Kassettenarchiv zu definieren.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-DEFine LIBRARY--Speicherarchivname--LIBType---SCSI----->
. -SHARED-----No----- . -RESETDrives-----No-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -SHARED-----+Yes-+- ' | (1) |
      '-No--'      '-RESETDrives-----+Yes-+-----'
                        '-No--'

. -AUTOLabel---No----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -AUTOLabel---+No-----+ '
      +-Yes-----+
      '-OVERWRITE- '

. -RELABELSCRatch---No----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -RELABELSCRatch---+No--+-'
      '-Yes- '

. -SERial-----AUTODetect----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+-----><
' -SERial-----+AUTODetect---+-'
      '-Seriennummer- '

```

Anmerkungen:

1. Der Standardwert des Parameters RESETDRIVES ist situationsabhängig. Wenn der Parameter SHARED auf NO gesetzt ist, ist NO der Wert des Parameters RESETDRIVES. Wenn der Parameter SHARED auf YES gesetzt ist, ist YES der Wert des Parameters RESETDRIVES.

## Parameter

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType=SCSI (Erforderlich)

Gibt an, dass das Speicherarchiv über einen SCSI-gesteuerten Datenträgerwechsler verfügt. Zum Bereitstellen von Datenträgern in Laufwerken bei diesem Typ von Speicherarchiv verwendet der Server die Datenträgerwechslereinheit.

SHARED

Gibt an, ob dieses Kassettenarchiv mit anderen Servern in einem Speicherbereichsnetz (Storage Area Network = SAN) gemeinsam genutzt wird. Dieser Parameter ist erforderlich, wenn Sie ein Kassettenarchiv für den Kassettenarchivmanager definieren.

YES

Gibt an, dass dieses Kassettenarchiv mit anderen Servern gemeinsam genutzt werden kann. Wird YES angegeben, lädt der Kassettenarchivmanagerserver Datenträger, die von anderen Servern angefordert werden, und verfolgt die Laufwerk- und Datenträgerzuordnung zu anderen Servern.

NO

Gibt an, dass dieses Kassettenarchiv nicht mit anderen Servern gemeinsam genutzt werden kann. SHARED=NO ist erforderlich, wenn das Kassettenarchiv durch die Übergabe von Befehlen über einen NAS-Dateiserver gesteuert wird.

AUTOLabel

Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

Einschränkung: Wenn Sie ein Kassettenarchiv definieren, das über Laufwerke verfügt, die an eine NAS-Einheit (NAS = Network-attached Storage) angeschlossen sind, müssen Sie den Befehl LABEL LIBVOLUME verwenden, um die Datenträger für dieses Kassettenarchiv zu kennzeichnen.

No

Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes

Gibt an, dass der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE

Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

RELABELSCRatch

Gibt an, ob der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht wurden und wieder als Arbeitsdatenträger verwendet werden. Wird dieser Parameter auf YES gesetzt, wird eine Operation LABEL LIBVOLUME gestartet und der vorhandene Datenträgerkennsatz wird überschrieben. Dieser Parameter ist optional und für die Verwendung mit einem VTL-Speicherarchiv (VTL = Virtual Tape Library) bestimmt.

Haben Sie sowohl virtuelle als auch reale Datenträger in Ihrem VTL, werden beide Typen mit einem neuen Kennsatz versehen, wenn dieser Parameter aktiviert ist. Enthält das VTL reale Datenträger, kann die Angabe dieser Option Auswirkungen auf die Leistung haben.

Einschränkung: Wenn Sie ein Kassettenarchiv definieren, das über Laufwerke verfügt, die an eine NAS-Einheit (NAS = Network-attached Storage) angeschlossen sind, müssen Sie den Befehl LABEL LIBVOLUME verwenden, um die Datenträger für dieses Kassettenarchiv zu kennzeichnen.

No



Gibt an, dass der Server Datenträger nicht mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden.


Yes

Gibt an, dass der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden.

RESETDrives

Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird. Wenn beispielsweise ein Speicheragent nicht mehr verfügbar ist, aber noch den Pfad zu einem Laufwerk belegt, kann der Server mit der persistenten Reserve die Reservierung des Speicheragenten unterbrechen und auf das Laufwerk zugreifen.

 AIX-Betriebssysteme  Windows-Betriebssysteme Wird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

 Linux-Betriebssysteme Wird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

In der folgenden Tabelle sind die drei möglichen Konfigurationen für Laufwerke beschrieben, die an NAS-Einheiten angeschlossen werden können.

Tabelle 1. Konfigurationen für Laufwerke, die an NAS-Einheiten angeschlossen sind

| Konfiguration der Speicherarchivereinheit   | Verhalten für persistente Reserve  |
|---|--|
| Die Speicherarchivereinheit wird an den IBM Spectrum Protect-Server angeschlossen, und die Bandlaufwerke werden vom Server und der NAS-Einheit gemeinsam genutzt. | Die Zurückstellung der Laufwerkreservierung wird unterstützt, wenn die NAS-Einheit die persistente Reserve unterstützt und diese aktiviert ist. Weitere Informationen zum Definieren der persistenten Reserve finden Sie in der Dokumentation für Ihre NAS-Einheit.  |
| Die Speicherarchivereinheit wird an den IBM Spectrum Protect-Server angeschlossen, und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen.            | Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben. |

| Konfiguration der Speicherarchivereinheit   | Verhalten für persistente Reserve  |
|---|--|
| Die Speicherarchivereinheit wird an die NAS-Einheit angeschlossen und der Zugriff erfolgt indirekt durch NDMP (Network Data Management Protocol), und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen. | Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben. |

Yes

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.

 Linux-Betriebssysteme

Yes

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

SERIAL

Gibt die Seriennummer des Speicherarchivs an, das definiert wird. Dieser Parameter ist wahlfrei. Der Standardwert ist AUTODETECT.

Wird SERIAL=AUTODETECT angegeben, wird bei der Definition des Pfads zu dem Speicherarchiv die vom Speicherarchiv gemeldete Seriennummer als Seriennummer verwendet.

Ist SERIAL=*Seriennummer*, wird die eingegebene Nummer mit der Nummer verglichen, die vom Server erkannt wurde.

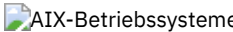
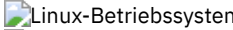
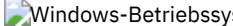
Achtung: Je nach Leistungsspektrum der Einheit wird SERIAL=AUTODETECT möglicherweise nicht unterstützt. In diesem Fall wird die Seriennummer als leer gemeldet.

## Beispiel: Ein SCSI-Kassettenarchiv definieren

Das Kassettenarchiv SCsilIB mit dem Kassettenarchivtyp SCSI definieren.

```
define library scsilib libtype=scsi
```

Das Kassettenarchiv erfordert einen Pfad. Der Einheitenname des Speicherarchivs ist:

-  /dev/lb0
-  /dev/tmsmcsi/lb0
-  lb3.0.0.0

Den Pfad definieren:

 AIX-Betriebssysteme

```
define path server1 scsilib srctype=server desttype=library
device=/dev/lb0
```

 Linux-Betriebssysteme

```
define path server1 scsilib srctype=server desttype=library
device=/dev/tmsmcsi/lb0
```

 Windows-Betriebssysteme

```
define path server1 scsilib srctype=server desttype=library
device=lb3.0.0.0
```

## DEFINE LIBRARY (Gemeinsam genutztes Kassettenarchiv definieren)

Verwenden Sie diese Syntax, um ein gemeinsam genutztes Kassettenarchiv zu definieren.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-DEFine LIBRARY--Speicherarchivname--LIBType----SHARED----->
>--PRIMarylibmanager----Servername-----<<
```

### Parameter

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType=SHARED (Erforderlich)

Gibt an, dass das Kassettenarchiv mit einem anderen IBM Spectrum Protect-Server über ein Speicherbereichsnetz (Storage Area Network = SAN) oder eine duale SCSI-Verbindung zu Kassettenarchivlaufwerken gemeinsam benutzt wird.

Wichtig: Geben Sie diesen Kassettenarchivtyp an, wenn das Kassettenarchiv auf einem Kassettenarchivclient definiert wird.

PRIMarylibmanager

Gibt den Namen des IBM Spectrum Protect-Servers an, der für die Steuerung des Zugriffs auf Kassettenarchivressourcen zuständig ist. Sie müssen diesen Server mit dem Befehl DEFINE SERVER definieren, bevor Sie ihn als Kassettenarchivmanager verwenden können. Dieser Parameter ist nur bei LIBTYPE=SHARED erforderlich und gültig.

### Beispiel: Ein gemeinsam genutztes Kassettenarchiv definieren

In einem Speicherbereichsnetz ein Kassettenarchiv mit dem Namen SHAREDTSM für einen Kassettenarchivclientserver mit dem Namen LIBMGR1 definieren.

```
define library sharedtsm libtype=shared primarylibmanager=libmgr1
```

## DEFINE LIBRARY (VTL-Speicherarchiv definieren)

Verwenden Sie diese Syntax, um ein Speicherarchiv zu definieren, das über einen SCSI-gesteuerten Datenträgerwechsler verfügt, der durch ein virtuelles Bandarchiv (Virtual Tape Library - VTL) dargestellt wird.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-DEFine LIBRARY--Speicherarchivname--LIBType----VTL----->
.-SHARED----No----- .-RESETDrives----No-----
>+-----+-----+-----+-----+-----+-----+-----+----->
' -SHARED----+-Yes-+' | (1) |
      '-No--'      '-RESETDrives----+-Yes-+'
                        '-No--'

.-AUTOLabel----No-----
>+-----+-----+-----+-----+-----+-----+-----+----->
' -AUTOLabel----+-No-+'
      +-Yes-----+
      '-OVERWRITE-'

.-RELABELSCRatch----Yes-----
>+-----+-----+-----+-----+-----+-----+-----+----->
' -RELABELSCRatch----+-No-+'
      '-Yes-'
```

```

.-SERial-----AUTODetect-----
>-----+-----+-----+-----><
'-SERial-----+--AUTODetect---+-'
      '-Seriennummer-'

```

Anmerkungen:

1. Der Standardwert des Parameters RESETDRIVES ist situationsabhängig. Wenn der Parameter SHARED auf NO gesetzt ist, ist NO der Wert des Parameters RESETDRIVES. Wenn der Parameter SHARED auf YES gesetzt ist, ist YES der Wert des Parameters RESETDRIVES.

## Parameter

---

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType=VTL (Erforderlich)

Gibt an, dass das Speicherarchiv über einen SCSI-gesteuerten Datenträgerwechsler verfügt, der durch ein virtuelles Bandarchiv (Virtual Tape Library - VTL) dargestellt wird. Zum Bereitstellen von Datenträgern in Laufwerken bei diesem Typ von Speicherarchiv verwendet der Server die Datenträgerwechslereinheit.

Wenn Sie ein VTL-Speicherarchiv definieren, darf Ihre Umgebung keine gemischten Datenträger enthalten und es müssen Pfade zwischen allen Laufwerken in dem Speicherarchiv und allen definierten Servern, einschließlich Speicheragenten, die das Speicherarchiv verwenden, definiert sein. Wenn eine dieser Bedingungen nicht zutrifft, kann die Gesamtleistung in demselben Maße wie beim Kassettenarchivtyp SCSI abnehmen. Dies ist besonders in Zeiten hoher Belastung der Fall.

SHARED

Gibt an, ob dieses Kassettenarchiv mit anderen Servern in einem Speicherbereichsnetz (Storage Area Network = SAN) gemeinsam genutzt wird. Dieser Parameter ist erforderlich, wenn Sie ein Kassettenarchiv für den Kassettenarchivmanager definieren.

YES


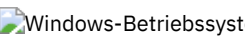
Gibt an, dass dieses Kassettenarchiv mit anderen Servern gemeinsam genutzt werden kann. Wird YES angegeben, lädt der Kassettenarchivmanagerserver Datenträger, die von anderen Servern angefordert werden, und verfolgt die Laufwerk- und Datenträgerzuordnung zu anderen Servern.


NO

Gibt an, dass dieses Kassettenarchiv nicht mit anderen Servern gemeinsam genutzt werden kann. SHARED=NO ist erforderlich, wenn das Kassettenarchiv durch die Übergabe von Befehlen über einen NAS-Dateiserver gesteuert wird.

RESETDrives

Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird. Wenn beispielsweise ein Speicheragent nicht mehr verfügbar ist, aber noch den Pfad zu einem Laufwerk belegt, kann der Server mit der persistenten Reserve die Reservierung des Speicheragenten unterbrechen und auf das Laufwerk zugreifen.

 **AIX-Betriebssysteme**  **Windows-Betriebssysteme** Wird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

 **Linux-Betriebssysteme** Wird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

 **AIX-Betriebssysteme**  **Windows-Betriebssysteme**

Yes

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.

## Linux-Betriebssysteme

Yes

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

### AUTOLabel

Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

Einschränkung: Wenn Sie ein Kassettenarchiv definieren, das über Laufwerke verfügt, die an eine NAS-Einheit (NAS = Network-attached Storage) angeschlossen sind, müssen Sie den Befehl LABEL LIBVOLUME verwenden, um die Datenträger für dieses Kassettenarchiv zu kennzeichnen.

No

Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes

Gibt an, dass der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

### OVERWRITE

Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

### RELABELSCRatch

Gibt an, ob der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht wurden und wieder als Arbeitsdatenträger verwendet werden. Wird dieser Parameter auf YES gesetzt, wird eine Operation LABEL LIBVOLUME gestartet und der vorhandene Datenträgerkennsatz wird überschrieben.

Haben Sie sowohl virtuelle als auch reale Datenträger in Ihrem VTL, werden beide Typen mit einem neuen Kennsatz versehen, wenn dieser Parameter aktiviert ist. Enthält das VTL reale Datenträger, kann die Angabe dieser Option Auswirkungen auf die Leistung haben.

Einschränkung: Wenn Sie ein Kassettenarchiv definieren, das über Laufwerke verfügt, die an eine NAS-Einheit (NAS = Network-attached Storage) angeschlossen sind, müssen Sie den Befehl LABEL LIBVOLUME verwenden, um die Datenträger für dieses Kassettenarchiv zu kennzeichnen.

Yes

Gibt an, dass der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden. YES ist der Standardwert.

No

Gibt an, dass der Server Datenträger nicht mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden.

### SERIAL

Gibt die Seriennummer des Speicherarchivs an, das definiert wird. Dieser Parameter ist wahlfrei. Der Standardwert ist AUTODETECT.

Wird SERIAL=AUTODETECT angegeben, wird bei der Definition des Pfads zu dem Speicherarchiv die vom Speicherarchiv gemeldete Seriennummer als Seriennummer verwendet.

Ist SERIAL=*Seriennummer*, wird die eingegebene Nummer mit der Nummer verglichen, die vom Server erkannt wurde.

Achtung: Je nach Leistungsspektrum der Einheit wird SERIAL=AUTODETECT möglicherweise nicht unterstützt. In diesem Fall wird die Seriennummer als leer gemeldet.

## Beispiel: Ein VTL-Speicherarchiv definieren




---

Ein Speicherarchiv mit dem Namen VTLLIB mit dem Speicherarchivtyp VTL definieren.

```
define library vtllib libtype=vtl
```



Das Kassettenarchiv erfordert einen Pfad. Der Einheitenname des Speicherarchivs ist:

-  AIX-Betriebssysteme/dev/lb0
-  Linux-Betriebssysteme/dev/tsm SCSI/lb0
-  Windows-Betriebssysteme/lb3.0.0.0


Den Pfad definieren:

 AIX-Betriebssysteme

```
define path server1 vtllib srctype=server desttype=library  
device=/dev/lb0
```

 Linux-Betriebssysteme

```
define path server1 vtllib srctype=server desttype=library  
device=/dev/tsm SCSI/lb0
```

 Windows-Betriebssysteme

```
define path server1 vtllib srctype=server desttype=library  
device=lb3.0.0.0
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

## DEFINE LIBRARY (Speicherarchivtyp ZOSMEDIA definieren)

---

Verwenden Sie diese Syntax, um ein Speicherarchiv zu definieren, das eine TAPE- oder FILE-Speicherressource darstellt, die von Tivoli Storage Manager for z/OS Media verwaltet wird.

Definieren Sie ein Speicherarchiv des Typs ZOSMEDIA, wenn das Speicherarchiv ausschließlich von Tivoli Storage Manager for z/OS Media verwaltet werden soll. Das Speicherarchiv wird dem IBM Spectrum Protect-Server als logische Speichereinheit angezeigt, für die keine Laufwerkdefinitionen erforderlich sind. Eine Pfaddefinition ist für den Server und alle Speicheragenten erforderlich, die auf die ZOSMEDIA-Speicherarchivressource zugreifen müssen.

### Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

---

```
>>-DEFine LIBRary--Speicherarchivname--LIBType----ZOSMEDIA----<<
```

### Parameter

---

Speicherarchivname (Erforderlich)

Gibt den Namen des Speicherarchivs an, das definiert werden soll.

LIBType=ZOSMEDIA (Erforderlich)

Gibt an, dass der Speicherarchivtyp ZOSMEDIA lautet, der eine TAPE- oder FILE-Speicherressource darstellt, die von Tivoli Storage Manager for z/OS Media verwaltet wird.

### Beispiel: ein ZOSMEDIA-Speicherarchiv konfigurieren

---

Das folgende Beispiel zeigt die Schritte, die zum Definieren und Konfigurieren eines zosmedia-Speicherarchivs erforderlich sind. Die Konfiguration umfasst diese Komponenten:

- Einen Server mit dem Namen sahara
- Ein Speicherarchiv mit dem Namen zebra, das mit dem Typ ZOSMEDIA definiert ist
- Einen z/OS Media-Server mit dem Namen oasis
- Einen Speicheragenten mit dem Namen mirage

Definieren Sie ein Speicherarchiv mit dem Namen ZEBRA mit dem Speicherarchivtyp ZOSMEDIA:

```
define library zebra libtype=zosmedia
```

Den z/OS Media-Server definieren:

```
define server oasis serverpassword=sanddune
hladdress=9.289.19.67 lladdress=1777
```

Der Server erfordert einen Pfad zu der Speicherarchivressource, die von Tivoli Storage Manager for z/OS Media verwaltet wird:

```
define path sahara zebra srctype=server
desttype=library zosmediaserver=oasis
```

Der Speicheragent erfordert einen Pfad zu der Speicherarchivressource, die von Tivoli Storage Manager for z/OS Media verwaltet wird:

```
define path mirage zebra srctype=server
desttype=library zosmediaserver=oasis
```

## DEFINE MACHINE (Maschineninformationen für die Wiederherstellung nach einem Katastrophenfall definieren)

---

Mit diesem Befehl können Fehlerbehebungsinformationen für einen Server oder eine Client-Knoten-Maschine gesichert werden. Diese Informationen werden in der Wiederherstellungsplandatei berücksichtigt, um den Benutzer bei der Wiederherstellung der Maschinen zu unterstützen.

### Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

---

```
>>-DEFine MACHine--Maschinename----->
>+-----+-----+-----+-----+----->
  '-DESCription----Beschreibung-'  '-BUilding----Gebäude-'
>+-----+-----+-----+-----+----->
  '-FLoor----Stockwerk-'  '-ROom----Raum-'

  .-PRIority----50-----  .-ADSMServer----No-----
>+-----+-----+-----+-----+-----<
  '-PRIority----Zahl---'  '-ADSMServer----+No--+-'
                                     '-Yes-'
```

### Parameter

---

Maschinenname (Erforderlich)

Gibt den Maschinennamen an. Der Name kann bis zu 64 Zeichen umfassen.

DESCription

Gibt eine Maschinenbeschreibung an. Dieser Parameter ist wahlfrei. Der Text kann bis zu 255 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

BUilding

Gibt das Gebäude an, in dem sich diese Maschine befindet. Dieser Parameter ist wahlfrei. Der Text kann bis zu 16 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

FLoor

Gibt das Stockwerk an, auf dem sich diese Maschine befindet. Dieser Parameter ist wahlfrei. Der Text kann bis zu 16 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

ROom

Gibt den Raum an, in dem sich diese Maschine befindet. Dieser Parameter ist wahlfrei. Der Text kann bis zu 16 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

PRIority

Gibt die Zurückschreibungspriorität für die Maschine als ganze Zahl von 1 bis 99 an. Die höchste Priorität ist 1. Dieser Parameter ist wahlfrei. Der Standardwert ist 50.

ADSMServer

Gibt an, ob die Maschine ein IBM Spectrum Protect-Server ist. Es kann nur eine Maschine als IBM Spectrum Protect-Server definiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No

Diese Maschine ist kein IBM Spectrum Protect-Server.

Yes

Diese Maschine ist ein IBM Spectrum Protect-Server.

## Beispiel: Informationen zur Wiederherstellung einer Maschine nach einem Katastrophenfall definieren

Die Maschine DISTRICT5 definieren und ein Gebäude, ein Stockwerk und einen Raum angeben. Diese Maschine enthält kritische Daten und hat die höchste Priorität.

```
define machine district5 building=101 floor=27  
room=datafacilities priority=1
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE MACHINE

| Befehl                       | Beschreibung  |
|------------------------------|---|
| DEFINE MACHNODEASSOCIATION   | Ordnet einen IBM Spectrum Protect-Knoten einer Maschine zu.   |
| DEFINE RECMEDMACHASSOCIATION | Ordnet Wiederherstellungsdatenträger einer Maschine zu.   |
| DELETE MACHINE               | Löscht eine Maschine.   |
| INSERT MACHINE               | Fügt Maschinenkenndaten oder Wiederherstellungsanweisungen in die IBM Spectrum Protect-Datenbank ein. |
| QUERY MACHINE                | Zeigt Informationen über Maschinen an.  |
| UPDATE MACHINE               | Ändert die Informationen zu einer Maschine.   |

## DEFINE MACHNODEASSOCIATION (Knoten einer Maschine zuordnen)

Mit diesem Befehl können Client-Knoten einer Maschine zugeordnet werden. Während der Fehlerbehebung können anhand dieser Informationen die Client-Knoten identifiziert werden, die sich auf den zerstörten Maschinen befunden haben.

Die Maschine muss in IBM Spectrum Protect definiert sein, und die Knoten müssen für IBM Spectrum Protect registriert sein.

Zum Abrufen der Informationen den Befehl QUERY MACHINE ausgeben. Diese Informationen werden in der Wiederherstellungsplandatei berücksichtigt, um den Benutzer bei der Wiederherstellung der Clientmaschinen zu unterstützen.

Ein Knoten bleibt so lange einer Maschine zugeordnet, bis der Knoten, die Maschine oder die Zuordnung selbst gelöscht wird.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>--DEFine MACHNODEAssociation--Maschinenname-----Knotenname-+----><
```

## Parameter

Maschinenname (Erforderlich)

Gibt den Maschinennamen an.

Knotenname (Erforderlich)

Gibt die Knotennamen an. Ein Knoten kann nur einer Maschine zugeordnet sein. Sollen mehrere Knoten angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.

## Beispiel: Einer Maschine einen Knoten zuordnen

Den Knoten ACCOUNTSPAYABLE der Maschine DISTRICT5 zuordnen.

```
define machnodeassociation district5 accountspayable
```



Gibt die Maßnahmengruppe an, zu der die Verwaltungsklasse gehört. Für die aktive Maßnahmengruppe (ACTIVE) kann keine Verwaltungsklasse definiert werden.

Klassenname (Erforderlich)

Gibt den Namen der neuen Verwaltungsklasse an. Die maximale Länge dieses Namens beträgt 30 Zeichen. Als Klassenname kann weder *default* noch *grace\_period* verwendet werden.

SPACEMGTECHnique

Gibt an, ob eine Datei, die diese Verwaltungsklasse verwendet, für die Umlagerung ausgewählt werden kann. Dieser Parameter ist wahlfrei. Der Standardwert ist NONE. Dieser Parameter ist nur für IBM Spectrum Protect for Space Management-Clients gültig, nicht für Clients für Sichern/Archivieren oder Anwendungscients. Gültige Werte:

AUTOMATIC

Gibt an, dass die Datei sowohl für die automatische Umlagerung als auch für die selektive Umlagerung auswählbar ist.

SElective

Gibt an, dass die Datei nur für die selektive Umlagerung auswählbar ist.

NONE

Gibt an, dass die Datei nicht für die Umlagerung auswählbar ist.

AUTOMIGNOnuse

Gibt die Anzahl Tage an, die nach dem letzten Zugriff auf eine Datei verstreichen müssen, bevor die Datei für die automatische Umlagerung ausgewählt werden kann. Dieser Parameter ist wahlfrei. Der Standardwert ist 0. Lautet der Wert für SPACEMGTECHNIQUE nicht AUTOMATIC, ignoriert der Server dieses Attribut. Sie können eine ganze Zahl im Bereich von 0 bis 9999 angeben.

Dieser Parameter ist nur für IBM Spectrum Protect for Space Management-Clients gültig, nicht für Clients für Sichern/Archivieren oder Anwendungscients.

MIGREQUIRESBkup

Gibt an, ob eine Sicherungsversion einer Datei vorhanden sein muß, damit die Datei umgelagert werden kann. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Dieser Parameter ist nur für IBM Spectrum Protect for Space Management-Clients gültig, nicht für Clients für Sichern/Archivieren oder Anwendungscients. Gültige Werte:

Yes

Gibt an, dass eine Sicherungsversion vorhanden sein muss.

No

Gibt an, dass eine Sicherungsversion wahlfrei ist.

MIGDESTination

Gibt den primären Speicherpool an, in dem der Server anfänglich Dateien speichert, die von IBM Spectrum Protect for Space Management-Clients umgelagert werden. Dieser Parameter ist nur für IBM Spectrum Protect for Space Management-Clients gültig; er ist nicht für Clients für Sichern/Archivieren oder Anwendungscients gültig. Der Standardwert ist SPACEMGPOOL. Ihre Auswahl für das Ziel kann von Faktoren abhängen, wie z. B.:

- Anzahl Clientknoten, die in den Speicherpool umgelagert werden. Wenn viele Benutzerdateien in demselben Speicherpool gespeichert werden, können Datenträgerkonflikte auftreten, wenn Benutzer versuchen, Dateien in den Speicherpool umzulagern oder Dateien aus dem Speicherpool zurückzurufen.
- Wie schnell die Dateien zurückgerufen werden müssen. Wenn Sie unmittelbaren Zugriff auf umgelagerte Versionen benötigen, können Sie einen Plattenspeicherpool als Ziel angeben.

Der Befehl schlägt fehl, wenn Sie einen Kopierspeicherpool oder einen Pool für aktive Daten als Ziel angeben.

DESCription

Beschreibung der Verwaltungsklasse. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

## Beispiel: Eine Verwaltungsklasse für eine bestimmte Maßnahmengruppe und Maßnahmendomäne definieren

---

Eine Verwaltungsklasse mit dem Namen MCLASS1 für Maßnahmengruppe SUMMER in der Maßnahmendomäne PROG1 definieren. Für IBM Spectrum Protect for Space Management-Clients sowohl die automatische Umlagerung als auch die selektive Umlagerung erlauben, und umgelagerte Dateien in dem Speicherpool SMPPOOL speichern. Die Beschreibung "Technical Support Mgmt Class" hinzufügen.

```
define mgmtclass prog1 summer mclass1
spacemgtechnique=automatic migdestination=smpool
description="technical support mgmt class"
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für DEFINE MGMTCLASS

| Befehl              | Beschreibung  |
|---------------------|---|
| ASSIGN DEFMGMTCLASS | Ordnet eine Verwaltungsklasse als Standardklasse für eine angegebene Maßnahmengruppe zu.                                      |
| COPY MGMTCLASS      | Erstellt eine Kopie einer Verwaltungsklasse.  |
| DEFINE COPYGROUP    | Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse. |
| DEFINE POLICYSET    | Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.   |
| DELETE MGMTCLASS    | Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe.                     |
| QUERY COPYGROUP     | Zeigt die Attribute einer Kopiengruppe an.  |
| QUERY MGMTCLASS     | Zeigt Informationen zu Verwaltungsklassen an.   |
| QUERY POLICYSET     | Zeigt Informationen über Maßnahmengruppen an.   |
| UPDATE COPYGROUP    | Ändert ein oder mehrere Attribute einer Kopiengruppe.   |
| UPDATE MGMTCLASS    | Ändert die Attribute einer Verwaltungsklasse.   |

## DEFINE NODEGROUP (Knotengruppe definieren)

Verwenden Sie diesen Befehl, um eine Knotengruppe zu definieren. Eine *Knotengruppe* ist eine Gruppe von Clientknoten, die wie eine einzelne Entität bearbeitet werden. Ein Knoten kann ein Mitglied einer oder mehrerer Knotengruppen sein.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

### Syntax

```
>>-DEFine NODEGroup--Gruppenname----->
>--+-----+----->
  '-DESCription----Beschreibung-'<
```

### Parameter

#### Gruppenname

Gibt den Namen der Knotengruppe an, die erstellt werden soll. Die maximale Länge des Namens beträgt 64 Zeichen. Der angegebene Name darf nicht mit dem Namen eines vorhandenen Clientknotens übereinstimmen.

#### DESCription

Gibt eine Beschreibung der Knotengruppe an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

### Beispiel: Eine Knotengruppe definieren

Die Knotengruppe `group1` definieren.

```
define nodegroup group1
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE NODEGROUP

| Befehl                 | Beschreibung   |
|------------------------|--|
| DEFINE BACKUPSET       | Definiert eine zuvor generierte Sicherungsgruppe für einen Server. |
| DEFINE NODEGROUPMEMBER | Fügt einer Knotengruppe einen Clientknoten hinzu.                  |

| Befehl                 | Beschreibung  |
|------------------------|---|
| DELETE BACKUPSET       | Löscht eine Sicherungsgruppe.   |
| DELETE NODEGROUP       | Löscht eine Knotengruppe.   |
| DELETE NODEGROUPMEMBER | Löscht einen Clientknoten aus einer Knotengruppe.                           |
| GENERATE BACKUPSET     | Generiert eine Sicherungsgruppe mit den Daten eines Clients.                |
| QUERY BACKUPSET        | Zeigt Sicherungsgruppen an.   |
| QUERY NODEGROUP        | Zeigt Informationen zu Knotengruppen an.                                    |
| UPDATE BACKUPSET       | Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum. |
| UPDATE NODEGROUP       | Aktualisiert die Beschreibung einer Knotengruppe.                           |

## DEFINE NODEGROUPMEMBER (Eintrag in der Knotengruppe definieren)

Verwenden Sie diesen Befehl, um einer Knotengruppe einen Clientknoten hinzuzufügen. Eine *Knotengruppe* ist eine Gruppe von Clientknoten, die wie eine einzelne Entität bearbeitet werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

### Syntax

```

      .- - - - - .
      v         |
>>-DEFine NODEGROUPMember--Gruppenname---Knotenname-+-----><

```

### Parameter

#### Gruppenname

Gibt den Namen der Knotengruppe an, der ein Clientknoten hinzugefügt werden soll.

#### Knotenname

Gibt den Namen des Clientknotens an, der der Knotengruppe hinzugefügt werden soll. Sie können einen oder mehrere Namen angeben. Mehrere Namen sind durch Kommas voneinander zu trennen; verwenden Sie keine Leerzeichen zwischen den Namen. Sie können auch Platzhalterzeichen verwenden, wenn mehrere Namen angegeben werden.

### Beispiel: Knoten einer Knotengruppe definieren

Die beiden Knoten `node1` und `node2` für die Knotengruppe `group1` definieren.

```
define nodegroupmember group1 node1,node2
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE NODEGROUPMEMBER



| Befehl                 | Beschreibung   |
|------------------------|--|
| DEFINE BACKUPSET       | Definiert eine zuvor generierte Sicherungsgruppe für einen Server. |
| DEFINE NODEGROUP       | Definiert eine Gruppe von Knoten.                                  |
| DELETE BACKUPSET       | Löscht eine Sicherungsgruppe.                                      |
| DELETE NODEGROUP       | Löscht eine Knotengruppe.  |
| DELETE NODEGROUPMEMBER | Löscht einen Clientknoten aus einer Knotengruppe.                  |
| GENERATE BACKUPSET     | Generiert eine Sicherungsgruppe mit den Daten eines Clients.       |
| QUERY BACKUPSET        | Zeigt Sicherungsgruppen an.  |
| QUERY NODEGROUP        | Zeigt Informationen zu Knotengruppen an.                           |

| Befehl           | Beschreibung  |
|------------------|---|
| UPDATE BACKUPSET | Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum. |
| UPDATE NODEGROUP | Aktualisiert die Beschreibung einer Knotengruppe.                           |




## DEFINE PATH (Pfad definieren)

Verwenden Sie diesen Befehl, um einen Pfad für eine Quelle für den Zugriff auf ein Ziel zu definieren. Die Quelle und das Ziel müssen definiert werden, bevor Sie einen Pfad definieren können. Ist beispielsweise ein Pfad zwischen einem Server und einem Laufwerk erforderlich, müssen Sie zuerst den Befehl DEFINE DRIVE und dann den Befehl DEFINE PATH ausgeben. Ein Pfad muss definiert werden, nachdem Sie den Befehl DEFINE DRIVE ausgegeben haben, damit der Server das Laufwerk verwenden kann.

Syntax- und Parameterbeschreibungen sind für die folgenden Pfadtypen verfügbar.

- DEFINE PATH (Pfad definieren, wenn das Ziel ein Laufwerk ist)
- DEFINE PATH (Pfad definieren, wenn das Ziel ein Kassettenarchiv ist)
-  AIX-Betriebssysteme  Linux-Betriebssysteme DEFINE PATH (Pfad definieren, wenn das Ziel ein ZOSMEDIA-Kassettenarchiv ist)

Ausführliche und aktuelle Informationen zur Einheitenunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

-  AIX-Betriebssysteme  Windows-Betriebssysteme Supported devices for AIX and Windows
-  Linux-Betriebssysteme Supported devices for Linux

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE PATH

| Befehl            | Beschreibung  |
|-------------------|---|
| DEFINE DATAMOVER  | Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server. |
| DEFINE DRIVE      | Ordnet ein Laufwerk einem Kassettenarchiv zu.                                       |
| DEFINE LIBRARY    | Definiert ein automatisiertes oder manuelles Kassettenarchiv.                       |
| DELETE PATH       | Löscht einen Pfad von einer Quelle zu einem Ziel.                                   |
| PERFORM LIBACTION | Definiert alle Laufwerke und Pfade für ein Kassettenarchiv.                         |
| QUERY PATH        | Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.                     |
| UPDATE DATAMOVER  | Ändert die Definition einer Einheit zum Versetzen von Daten.                        |
| UPDATE PATH       | Ändert die zu einem Pfad gehörigen Attribute.                                       |

## DEFINE PATH (Pfad definieren, wenn das Ziel ein Laufwerk ist)

Verwenden Sie diese Syntax, wenn Sie einen Pfad zu einem Laufwerk definieren.

### Berechtigungsklasse



Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-DEFine PATH--Quellennamen--Zielname----->
>--SRCType-----+--DATAMover-+---+-----+----->
      '-SERVer----'   '-AUTODetect-----+--No---+'
                          '-Yes-'
>--DESTType-----DRive--LIBRARY-----Kassettenarchivname----->
>----DEVIce-----+--Einheitennamen-+----->
```





| Quelle zum Ziel   | Beispiel  |
|---|---|
| Server zu einem Laufwerk (kein FILE-Laufwerk)   |  AIX-Betriebssysteme<br><br>/dev/mt3<br><br> Windows-Betriebssysteme<br><br>mt3 |
| Speicheragent (auf einem Windows-System) zu einem Laufwerk (kein FILE-Laufwerk)                             | mt3   |
| Speicheragent zu einem Laufwerk, wenn das Laufwerk ein logisches Laufwerk in einem FILE-Kassettenarchiv ist | FILE  |
| NAS-Einheit zum Versetzen von Daten zu einem Laufwerk   | NetApp NAS-Dateiserver: rst01<br><br>EMC Celerra NAS-Dateiserver: c436t011<br><br>IBM® System Storage N Series: rst01   |





 Linux-Betriebssysteme Die Quelle verwendet den Einheitennamen für den Zugriff auf das Laufwerk. Für Beispiele siehe Tabelle 2.


Tabelle 2. Beispiele für Einheitennamen


| Quelle zum Ziel   | Beispiel   |
|---|--|
| Server zu einem Laufwerk (kein FILE-Laufwerk)   | /dev/tmscsi/mt3  |
| Speicheragent zu einem Laufwerk (kein FILE-Laufwerk)  | /dev/tmscsi/mt3  |
| Speicheragent zu einem Laufwerk, wenn das Laufwerk ein logisches Laufwerk in einem FILE-Kassettenarchiv ist | FILE   |
| NAS-Einheit zum Versetzen von Daten zu einem Laufwerk   | NetApp NAS-Dateiserver: rst01<br><br>EMC Celerra NAS-Dateiserver: c436t011<br><br>IBM System Storage N Series: rst01 |

Wichtig:

-  AIX-Betriebssysteme  Linux-Betriebssysteme Für 349X-Kassettenarchive ist der Aliasname ein symbolischer Name, der in der Datei /etc/ibmatl.conf angegeben ist.  Windows-Betriebssysteme Für 349X-Kassettenarchive ist der Aliasname ein symbolischer Name, der in der Datei c:\winnt\ibmatl.conf angegeben ist. Weitere Informationen enthält das Handbuch *IBM Tape Device Drivers Installation and User's Guide*, das von der Site der IBM Systemunterstützung unter <http://www.ibm.com/support/docview.wss?uid=ssg1S7002972> heruntergeladen werden kann.
- Informationen über Namen für Einheiten, die mit einem NAS-Dateiserver verbunden sind, enthält die Produktinformation für den Dateiserver. Beispiel: Stellen Sie für einen NetApp-Dateiserver unter Verwendung von Telnet eine Verbindung zu dem Dateiserver her und geben Sie den Befehl SYSCONFIG aus. Verwenden Sie diesen Befehl, um Einheitenamen für Laufwerke zu bestimmen:

```
sysconfig -t
```

 Windows-Betriebssysteme GENERICTAPE

 Windows-Betriebssysteme Gibt an, ob das Bandlaufwerk, das verwendet werden soll, den Einheitenklassentyp GENERICTAPE hat. Ist die Einheit ein Bandlaufwerk und wird sie nicht von IBM Spectrum Protect, aber für das Windows-Betriebssystem unterstützt, können Sie sie mit dem generischen Bandformat verwenden. Um das Laufwerk zu verwenden, geben Sie GENERICTAPE=Yes an, wenn Sie einen Pfad zu dem Laufwerk definieren. Der Standardwert ist 'No'. Gültige Werte sind:

Yes

Gibt an, dass das Bandlaufwerk, das verwendet werden soll, den Einheitenklassentyp GENERICTAPE hat.

No

Gibt an, dass das Bandlaufwerk, das verwendet werden soll, nicht den Einheitenklassentyp GENERICTAPE hat.

ONLine

Gibt an, ob der Pfad für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Gültige Werte:

Yes

Gibt an, dass der Pfad für die Verwendung verfügbar ist.

No

Gibt an, dass der Pfad nicht für die Verwendung verfügbar ist.

Die Quelle und das Ziel müssen verfügbar sein, um den Pfad verwenden zu können.

Ist beispielsweise der Pfad von einer Einheit zum Versetzen von Daten zu einem Laufwerk online, aber ist entweder die Einheit zum Versetzen von Daten oder das Laufwerk offline, kann der Pfad nicht verwendet werden.

## DIRectory

Gibt die Verzeichnisposition(en) an, an der/denen der Speicheragent die Dateien liest und schreibt, die Speicherdatenträger für die Einheitenklasse FILE darstellen, die dem FILE-Kassettenarchiv zugeordnet ist. Der Parameter DIRECTORY wird auch für Einheiten des Typs REMOVABLEFILE verwendet. Für Einheiten des Typs REMOVABLEFILE stellt der Parameter DIRECTORY in Verbindung mit dem Parameter DRIVE dem Server (kein Speicheragent) Informationen zur Verfügung, die den Zugriff auf die Einheit beschreiben. Dieser Parameter ist wahlfrei.


Für einen Pfad von einem Speicheragenten zu einer FILE-Einheit ist dieser Parameter nur gültig, wenn *alle* folgenden Bedingungen zutreffen:

- Der Quellentyp ist SERVER (d. h., ein Speicheragent, der für diesen Server als Server definiert wurde).
- Der Quellename ist der Name eines Speicheragenten, *nicht* der Servername.
- Das Ziel ist ein logisches Laufwerk, das Teil eines FILE-Kassettenarchivs ist, das bei der Definition der Einheitenklasse erstellt wurde.

Haben Sie mehrere Verzeichnisse für die Einheitenklasse angegeben, die dem FILE-Kassettenarchiv zugeordnet ist, müssen Sie dieselbe Anzahl Verzeichnisse für jeden Pfad zum FILE-Kassettenarchiv angeben. Sie dürfen keine vorhandenen Verzeichnisse auf dem Server, den der Speicheragent verwendet, ändern oder versetzen, damit die Einheitenklasse und der Pfad synchronisiert bleiben. Das Hinzufügen von Verzeichnissen ist zulässig. Wird eine abweichende Anzahl Verzeichnisse angegeben, kann dies einen Laufzeitfehler verursachen.

Der Standardwert für DIRECTORY ist das Verzeichnis des Servers zum Zeitpunkt der Befehlsausgabe. Die Windows-Registrierungsdatenbank wird zum Lokalisieren des Standardwerts verwendet.

Verwenden Sie eine Namenskonvention, mit der Sie das Verzeichnis einem bestimmten physischen Laufwerk zuordnen können. Damit kann sichergestellt werden, dass Ihre Konfiguration für die gemeinsame Benutzung des FILE-Kassettenarchivs zwischen dem Server und dem Speicheragenten gültig ist. Befindet sich der Speicheragent auf einem Windows-System, verwenden Sie eine allgemeine Namenskonvention. Verfügt der Speicheragent nicht über die Berechtigung für den Zugriff auf fernen Speicher, treten Ladefehler im Speicheragenten auf.

 Windows-Betriebssystem Das dem Speicheragentendienst zugeordnete Konto muss ein Konto in der Gruppe der lokalen Administratoren oder ein Konto in der Gruppe der Domänenadministratoren sein. Befindet sich das Konto in der Gruppe der lokalen Administratoren, müssen Benutzer-ID und Kennwort den Angaben eines Kontos entsprechen, das über Berechtigungen für den Zugriff auf Speicher verfügt, der von dem System bereitgestellt wird, das den fernen Sharepunkt verwaltet. Wenn beispielsweise ein SAMBA-Server Zugriff auf fernen Speicher bereitstellt, müssen Benutzer-ID und Kennwort in der SAMBA-Konfiguration der Benutzer-ID und dem Kennwort des lokalen Administrators entsprechen, der dem Speicheragentendienst zugeordnet ist.

```
define devclass file devtype=file shared=yes mountlimit=1
directory=d:\filedir\dir1
define path stal filel srctype=server desttype=drive
library=filel device=file
directory=\\192.168.1.10\filedir\dir1
```

In dem vorherigen Beispiel erstellt der Befehl DEFINE DEVCLASS das gemeinsam genutzte Dateisystem in dem Verzeichnis, auf das der Server als D:\FILEDIR\DIR1 zugreift. Der Speicheragent verwendet jedoch den UNC-Namen \\192.168.1.10\FILEDIR\DIR1. Das bedeutet, dass das System mit TCP/IP-Adresse 192.168.1.10 dasselbe Verzeichnis gemeinsam nutzt, wobei FILEDIR als gemeinsam genutzter Name verwendet wird. Außerdem verfügt der Speicheragentendienst über ein Konto, das auf diesen Speicher zugreifen kann. Der Zugriff ist möglich, weil das Konto einem lokalen Konto mit derselben Benutzer-ID und demselben Kennwort wie 192.168.1.10 zugeordnet ist oder weil es einem Domänenkonto zugeordnet ist, das sowohl auf dem Speicheragenten als auch auf 192.168.1.10 verfügbar ist. Sie können gegebenenfalls 192.168.1.10 durch einen symbolischen Namen wie folgt ersetzen:

Beispiel.IhreFirma.com

Achtung:

1. Speicheragenten greifen auf FILE-Datenträger zu, indem ein Verzeichnisname in einem Datenträgernamen durch einen Verzeichnisnamen eines Verzeichnisses in der Liste ersetzt wird, die mit dem Befehl DEFINE PATH zur Verfügung gestellt wird. Mit diesem Parameter angegebene Verzeichnisse werden auf dem Server nicht geprüft.
2. IBM Spectrum Protect erstellt keine Shares oder Berechtigungen und lädt nicht das Zieldateisystem. Sie müssen diese Aktionen ausführen, bevor Sie den Speicheragenten starten.

## Beispiel: Einen Pfad von einem Server zu einem Laufwerk definieren

Einen Pfad von einem Server zu einem Laufwerk definieren. In diesem Fall lautet der Servername *NET1*, der Laufwerkname *TAPEDRV6*, der Kassettenarchivname *NETLIB* und der Einheitenname *mt4*. Geben Sie für AUTODETECT NO an.

```
define path net1 tapedrv6 srctype=server autodetect=no desttype=drive
  library=netlib device=mt4
```

## Beispiel: Einen Pfad von einer Einheit zum Versetzen von Daten zu einem Laufwerk für die Sicherung und Zurückschreibung definieren

---

Einen Pfad von der Einheit zum Versetzen von Daten, die ein NAS-Dateiserver ist, zu dem Laufwerk definieren, das von dem NAS-Dateiserver für Sicherungs- und Zurückschreibungsoperationen verwendet wird. In diesem Beispiel hat die NAS-Einheit zum Versetzen von Daten den Namen *NAS1*, der Laufwerkname lautet *TAPEDRV3*, das Kassettenarchiv ist *NASLIB* und der Einheitenname für das Laufwerk lautet *rst01*.

```
define path nas1 tapedrv3 srctype=datamover desttype=drive library=naslib
  device=rst01
```

 Linux-Betriebssysteme

## Beispiel: Einen Pfad von einem Speicheragenten zu einem Laufwerk für die Sicherung und Zurückschreibung definieren

---

Einen Pfad von dem Speicheragenten *SA1* zu dem Laufwerk definieren, das vom Speicheragenten für Sicherungs- und Zurückschreibungsoperationen verwendet wird. In diesem Beispiel lautet das Kassettenarchiv *TSMLIB*, das Laufwerk ist *TAPEDRV4* und der Einheitenname für das Laufwerk ist */dev/tmsmcsi/mt3*.

```
define path sa1 tapedrv4 srctype=server desttype=drive library=tsmlib
  device=/dev/tmsmcsi/mt3
```

 AIX-Betriebssysteme  Windows-Betriebssysteme

## Beispiel: Einen Pfad von einem Speicheragenten zu einem Laufwerk für die Sicherung und Zurückschreibung definieren

---

Einen Pfad von dem Speicheragenten *SA1* zu dem Laufwerk definieren, das vom Speicheragenten für Sicherungs- und Zurückschreibungsoperationen verwendet wird. In diesem Beispiel lautet das Kassettenarchiv *TSMLIB*, das Laufwerk ist *TAPEDRV4* und der Einheitenname für das Laufwerk ist */dev/mt3*.

```
define path sa1 tapedrv4 srctype=server desttype=drive library=tsmlib
  device=/dev/mt3
```


 AIX-Betriebssysteme  Windows-Betriebssysteme

## Beispiel: Einen Pfad definieren, um einem Speicheragenten den Zugriff auf den gemeinsam genutzten Plattenspeicher zu ermöglichen

---

Einen Pfad definieren, der es dem Speicheragenten ermöglicht, auf Dateien in einem Plattenspeicher zuzugreifen, der mit dem Server gemeinsam genutzt wird. Laufwerk *FILE9* ist für Kassettenarchiv *FILE1* auf dem Server definiert. Der Speicheragent *SA1* greift auf *FILE9* zu. Auf dem Speicheragenten befinden sich diese Daten im Verzeichnis *\\192.168.1.10\filedata*.

 AIX-Betriebssysteme Die Daten für *FILE9* befinden sich auf dem Server unter */tsmdata/filedata*.


 Windows-Betriebssysteme Die Daten für *FILE9* befinden sich auf dem Server unter *d:\tsmdata\filedata*.

```
define path sa1 file9 srctype=server desttype=drive library=file1 device=file
  directory="\\192.168.1.10\filedata"
```

## Beispiel: Einen Speicheragenten für die Verwendung eines FILE-Kassettenarchivs konfigurieren

---

Das folgende Beispiel verdeutlicht die Bedeutung übereinstimmender Einheitenklassen und Pfade, um sicherzustellen, dass Speicheragenten auf neu erstellte FILE-Datenträger zugreifen können.

Beispiel: Sie möchten folgende drei Verzeichnisse für ein FILE-Kassettenarchiv verwenden:  Windows-Betriebssysteme

- c:\server
- d:\server
- e:\server



- /opt/tivoli1
- /opt/tivoli2
- /opt/tivoli3

1. Verwenden Sie den folgenden Befehl, um ein FILE-Kassettenarchiv mit dem Namen CLASSA mit einem Laufwerk mit dem Namen CLASSA1 auf SERVER1 zu definieren:

```
define devclass classa devtype=file
directory="c:\server,d:\server,e:\server"
shared=yes mountlimit=1
```



```
define devclass classa devtype=file
directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
shared=yes mountlimit=1
```

2. Sie wollen, dass der Speicheragent STA1 das FILE-Kassettenarchiv verwenden kann. Daher definieren Sie folgenden Pfad für Speicheragent STA1:

```
define path stal classal srctype=server desttype=drive device=file
directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
\\192.168.1.10\e\server" library=classa
```



```
define path stal classal srctype=server desttype=drive device=file
directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
```

In diesem Szenario ersetzt der Speicheragent STA1 den Verzeichnisnamen c:\server durch den Verzeichnisnamen \\192.168.1.10\c\server, um auf FILE-Datenträger zuzugreifen, die sich in dem Verzeichnis c:\server auf dem Server befinden.

In diesem Szenario ersetzt der Speicheragent STA1 den Verzeichnisnamen /opt/tivoli1 durch den Verzeichnisnamen /opt/ibm1/, um auf FILE-Datenträger zuzugreifen, die sich in dem Verzeichnis /opt/tivoli1 auf dem Server befinden.

3. FILE-Datenträger c:\server\file1.dsm wird durch SERVER1 erstellt. Wenn Sie das erste Verzeichnis für die Einheitenklassen später mit folgendem Befehl ändern:

```
update devclass classa directory="c:\otherdir,d:\server,e:\server"
```

kann SERVER1 weiterhin auf FILE-Datenträger c:\server\file1.dsm zugreifen, der Speicheragent STA1 jedoch nicht, weil in der PATH-Verzeichnisliste kein übereinstimmender Verzeichnisname mehr vorhanden ist. Ist kein Verzeichnisname in der Verzeichnisliste verfügbar, die der Einheitenklasse zugeordnet ist, kann der Speicheragent den Zugriff auf einen FILE-Datenträger in diesem Verzeichnis verlieren. Obwohl der Server zum Lesen noch auf den Datenträger zugreifen kann, kann der fehlgeschlagene Zugriff des Speicheragenten auf den FILE-Datenträger dazu führen, dass Operationen nur auf einem LAN-Pfad wiederholt werden können oder dass sie fehlschlagen.

4. Wird der FILE-Datenträger /opt/tivoli1/file1.dsm auf SERVER1 erstellt und wird der Befehl

```
update devclass classa directory="/opt/otherdir,/opt/tivoli2,
/opt/tivoli3"
```

ausgegeben, kann SERVER1 weiterhin auf FILE-Datenträger /opt/tivoli1/file1.dsm zugreifen, der Speicheragent STA1 jedoch nicht, weil in der PATH-Verzeichnisliste kein übereinstimmender Verzeichnisname mehr vorhanden ist. Ist kein Verzeichnisname in der Verzeichnisliste verfügbar, die der Einheitenklasse zugeordnet ist, kann der Speicheragent den Zugriff auf einen FILE-Datenträger in diesem Verzeichnis verlieren. Obwohl der Server zum Lesen noch auf den Datenträger zugreifen kann, kann der fehlgeschlagene Zugriff des Speicheragenten auf den FILE-Datenträger dazu führen, dass Operationen nur auf einem LAN-Pfad wiederholt werden können oder dass sie fehlschlagen.

## DEFINE PATH (Pfad definieren, wenn das Ziel ein Kassettenarchiv ist)

Verwenden Sie diese Syntax, wenn Sie einen Pfad zu einem Kassettenarchiv definieren.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

```
>>-DEFine PATH--Quellenname--Zielname----->
                                     (1)
>--SRCType-----+--DATAMover-----+----->
      '-SERVer-----'   '-AUTODetect-----+No--+-'
                                     '-Yes-'

>--DESTType-----LIBRary--+--DEVIce-----+Einheitename----->
      '-EXTERNALManager-----+Pfadname-'

      .-ONLine-----Yes-----
>-----+----->
      '-ONLine-----+Yes--+-'
      '-No--'
```

Anmerkungen:

1. DATAMOVER gilt nur für NAS-Einheiten.

## Parameter

---

Quellenname (Erforderlich)

Gibt den Namen der Quelle des Pfads an. Dieser Parameter ist erforderlich.

Zielname (Erforderlich)

Gibt den Namen des Ziels an. Dieser Parameter ist erforderlich.

Achtung: Um einen Pfad von einer NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv zu definieren, muss das Kassettenarchiv den Typ (LIBTYPE) SCSI, 349x oder ACSLS haben.

SRCType (Erforderlich)

Gibt den Typ der Quelle an. Dieser Parameter ist erforderlich. Gültige Werte:

DATAMover

Gibt an, dass eine Einheit zum Versetzen von Daten die Quelle ist.

SERVer

Gibt an, dass ein Speicheragent die Quelle ist.

AUTODetect

Gibt an, ob die Seriennummer für ein Laufwerk oder Kassettenarchiv automatisch zu dem Zeitpunkt in der Datenbank aktualisiert wird, zu dem der Pfad definiert wird. Dieser Parameter ist wahlfrei. Dieser Parameter ist nur für Pfade gültig, die von dem lokalen Server zu einem Laufwerk oder Kassettenarchiv definiert sind. Gültige Werte:

No

Gibt an, dass die Seriennummer nicht automatisch aktualisiert wird. Die Seriennummer wird dennoch mit der Angabe verglichen, die bereits für die Einheit in der Datenbank vorhanden ist. Der Server gibt eine Nachricht aus, wenn keine Übereinstimmung gefunden wird.

Yes

Gibt an, dass die Seriennummer automatisch aktualisiert wird, um dieselbe Seriennummer widerzuspiegeln, die das Laufwerk an IBM Spectrum Protect meldet.

Wichtig:

1. Wurde die Seriennummer bei der Definition des Laufwerks oder des Kassettenarchivs nicht definiert, versucht der Server immer, die Seriennummer zu ermitteln, und AUTODETECT nimmt standardmäßig den Wert YES an. Wurde zuvor eine Seriennummer eingegeben, erhält AUTODETECT den Standardwert NO.
2. Die Verwendung von AUTODETECT=YES in diesem Befehl bedeutet, dass die in der Laufwerk- oder Kassettenarchivdefinition angegebene Seriennummer mit der ermittelten Seriennummer aktualisiert wird.
3. Je nach Leistungsspektrum der Einheit wird der Parameter AUTODETECT möglicherweise nicht unterstützt.

DESTType=LIBRary (Erforderlich)

Gibt an, dass ein Kassettenarchiv das Ziel ist. Dieser Parameter ist erforderlich.

DEVIce

Gibt den Namen der Einheit an, die der Quelle bekannt ist, oder FILE an, wenn die Einheit ein logisches Laufwerk in einem Kassettenarchiv FILE ist.

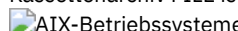
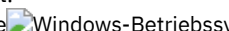



  Die Quelle verwendet den Einheitennamen für den Zugriff auf das Kassettenarchiv. Für Beispiele siehe Tabelle 1.

Tabelle 1. Beispiele für Einheitenamen

| Quelle zum Ziel   | Beispiel  |
|---|---|
| Server zu einem Kassettenarchiv   |  AIX-Betriebssysteme<br>/dev/lb4<br> Linux-Betriebssysteme<br>/dev/tmscsi/lb4<br> Windows-Betriebssysteme<br>lb4.1 |
| Speicheragent zu einem Laufwerk, wenn das Laufwerk ein logisches Laufwerk in einem FILE-Kassettenarchiv ist | FILE  |
| NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv  | mc0   |





 Die Quelle verwendet den Einheitennamen für den Zugriff auf das Kassettenarchiv. Für Beispiele siehe Tabelle 2.

Tabelle 2. Beispiele für Einheitennamen

| Quelle zum Ziel  | Beispiel        |
|--|-----------------|
| Server zu einem Kassettenarchiv                              | /dev/tmscsi/lb4 |
| NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv | mc0             |

Wichtig:


-   Für 349X-Kassettenarchive ist der Aliasname ein symbolischer Name, der in der Datei /etc/ibmatl.conf angegeben ist.  Für 349X-Kassettenarchive ist der Aliasname ein symbolischer Name, der in der Datei c:\winnt\ibmatl.conf angegeben ist. Weitere Informationen enthält das Handbuch *IBM Tape Device Drivers Installation and User's Guide*, das von der Site der IBM® Systemunterstützung unter <http://www.ibm.com/support/docview.wss?uid=ssg1S7002972> heruntergeladen werden kann.
- Informationen über Namen für Einheiten, die mit einem NAS-Dateiserver verbunden sind, enthält die Produktinformation für den Dateiserver. Beispiel: Stellen Sie für einen NetApp-Dateiserver unter Verwendung von Telnet eine Verbindung zu dem Dateiserver her und geben Sie den Befehl SYSCONFIG aus. Verwenden Sie diesen Befehl, um Einheitennamen für Laufwerke zu bestimmen:

```
sysconfig -t
```

Verwenden Sie diesen Befehl, um den Einheitennamen für ein Kassettenarchiv zu bestimmen:

```
sysconfig -m
```

#### EXTERNALManager

Gibt den Standort des externen Kassettenarchivmanagers an, an den IBM Spectrum Protect Zugriffsanforderungen für Datenträger senden kann. Der Wert dieses Parameters muss zwischen einfachen Anführungszeichen stehen. Geben Sie beispielsweise Folgendes ein: 

```
/usr/lpp/GESedt-acsls/bin/elmdt
```

   
/opt/GESedt-acsls/bin/elmdt

   
C:\Programme\GES\EDT-ACSLs\bin\elmdt.exe

Dieser Parameter ist erforderlich, wenn das Kassettenarchiv ein externes Kassettenarchiv ist.

#### ONLine

Gibt an, ob der Pfad für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Gültige Werte:

Yes

Gibt an, dass der Pfad für die Verwendung verfügbar ist.

No


Gibt an, dass der Pfad nicht für die Verwendung verfügbar ist.

Die Quelle und das Ziel müssen verfügbar sein, um den Pfad verwenden zu können.


Achtung: Ist der Pfad zu einem Kassettenarchiv offline, kann der Server nicht auf das Kassettenarchiv zugreifen. Wird der Server angehalten und erneut gestartet, während der Pfad zu dem Kassettenarchiv offline ist, wird das Kassettenarchiv nicht initialisiert.

## Beispiel: Einen Pfad von einem Server zu einem Kassettenarchiv definieren

---

Einen Pfad von dem Server SATURN zu dem SCSI-Kassettenarchiv SCsilIB definieren.  AIX-Betriebssysteme

```
define path saturn scsilib srctype=server
desttype=library device=/dev/lb3
```

 Linux-Betriebssysteme

```
define path saturn scsilib srctype=server
desttype=library device=/dev/tmscsi/lb3
```

 Windows-Betriebssysteme

```
define path saturn scsilib srctype=server
desttype=library device=lb3.0.0.0
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

## DEFINE PATH (Pfad definieren, wenn das Ziel ein ZOSMEDIA-Kassettenarchiv ist)

---

Verwenden Sie diese Syntax, wenn Sie einen Pfad zu einem ZOSMEDIA-Kassettenarchiv definieren. Sie müssen zuerst den z/OS Media-Server in Ihrer Konfiguration mit dem Befehl DEFINE SERVER definieren.

### Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

---

```
>>-DEFine PATH--Quellename--Zielname--SRCType-----SERVer----->
>--DESTType-----LIBRARY--ZOSMEDIASERVER-----Servername----->
  .-ONLine-----Yes-----
>+-----+-----+-----+-----+-----+-----+-----+----->
  '-ONLine-----+Yes-+-'
    '-No--'
```

### Parameter

---

Quellename (Erforderlich)

Gibt den Namen der Quelle des Pfads an.

Zielname (Erforderlich)

Gibt den Namen des ZOSMEDIA-Kassettenarchivs an.

SRCType=SERVer (Erforderlich)

Gibt an, dass ein Speicheragent oder ein Server die Quelle ist.

DESTType=LIBRARY (Erforderlich)

Gibt an, dass ein Kassettenarchiv das Ziel ist.

ZOSMEDIAServer (Erforderlich)

Gibt den Namen des Servers an, der einen Tivoli Storage Manager for z/OS Media-Server darstellt.

ONLine

Gibt an, ob der Pfad für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Gültige Werte:

Yes

Gibt an, dass der Pfad für die Verwendung verfügbar ist.

No

Gibt an, dass der Pfad nicht für die Verwendung verfügbar ist.

Die Quelle und das Ziel müssen verfügbar sein, um den Pfad verwenden zu können.



Achtung: Ist der Pfad zu einem Kassettenarchiv offline, kann der Server nicht auf das Kassettenarchiv zugreifen. Wird der Server angehalten und erneut gestartet, während der Pfad zu dem Kassettenarchiv offline ist, wird das Kassettenarchiv nicht initialisiert.

Kann während der Initialisierung des IBM Spectrum Protect-Servers nicht auf den z/OS Media-Server zugegriffen werden, wird der Kassettenarchivpfad offline gesetzt. Verwenden Sie den Befehl UPDATE PATH und geben Sie ONLINE=YES an, um das ZOSMEDIA-Kassettenarchiv wieder anzuhängen.

## DEFINE POLICYSET (Maßnahmengruppe definieren)

Mit diesem Befehl kann eine Maßnahmengruppe in einer Maßnahmendomäne definiert werden. Eine Maßnahmengruppe enthält Verwaltungsklassen, die Kopiengruppen enthalten. Für jede Maßnahmendomäne können eine oder mehrere Maßnahmengruppen definiert werden.

Um eine Maßnahmengruppe zu aktivieren, muss der Befehl ACTIVATE POLICYSET verwendet werden. In einer Maßnahmendomäne kann nur eine Maßnahmengruppe aktiv sein. Die Kopiengruppen und Verwaltungsklassen innerhalb der aktiven Maßnahmengruppe bestimmen die Regeln, nach denen Client-Knoten Sicherungsoperationen, Archivierungsoperationen und Speicherverwaltungsoperationen ausführen und nach denen die gespeicherten Client-Dateien verwaltet werden.

Bevor eine Maßnahmengruppe mit dem Befehl ACTIVATE POLICYSET aktiviert wird, muss mit dem Befehl VALIDATE POLICYSET überprüft werden, ob sie vollständig und gültig ist.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Maßnahmengruppe gehört.

### Syntax

```
>>-DEFine Policyset--Domänenname--Name_der_Maßnahmengruppe----->
>-+-----+-----<
  '-DESCRiption-----Beschreibung-'
```

### Parameter

Domänenname (Erforderlich)

Gibt den Namen der Maßnahmendomäne an, zu der die Maßnahmengruppe gehört.

Name\_der\_Maßnahmengruppe (Erforderlich)

Gibt den Namen der Maßnahmengruppe an. Die maximale Länge dieses Namens beträgt 30 Zeichen. Eine Maßnahmengruppe mit dem Namen ACTIVE kann nicht definiert werden.

DESCRiption

Gibt eine Beschreibung für die neue Maßnahmengruppe an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

### Beispiel: Eine Maßnahmengruppe definieren

Eine Maßnahmengruppe mit dem Namen SUMMER für die Maßnahmendomäne PROG1 definieren und die Beschreibung "Programming Group Policies" einschließen.

```
define policyset prog1 summer
description="Programming Group Policies"
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE POLICYSET

| Befehl             | Beschreibung  |
|--------------------|---|
| ACTIVATE POLICYSET | Wertet eine Maßnahmengruppe aus und aktiviert sie.                    |
| COPY MGMTCLASS     | Erstellt eine Kopie einer Verwaltungsklasse.                          |
| COPY POLICYSET     | Erstellt eine Kopie einer Maßnahmengruppe.                            |
| DEFINE DOMAIN      | Definiert eine Maßnahmendomäne, der Clients zugeordnet werden können. |

| Befehl             | Beschreibung  |
|--------------------|---|
| DEFINE MGMTCLASS   | Definiert eine Verwaltungsklasse.   |
| DELETE POLICYSET   | Löscht eine Maßnahmengruppe einschließlich ihrer Verwaltungsklassen und Kopiengruppen aus einer Maßnahmendomäne.        |
| QUERY POLICYSET    | Zeigt Informationen über Maßnahmengruppen an.   |
| UPDATE POLICYSET   | Ändert die Beschreibung einer Maßnahmengruppe.  |
| VALIDATE POLICYSET | Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert. |

## DEFINE PROFASSOCIATION (Profilzuordnung definieren)

Mit diesem Befehl können auf einem Konfigurationsmanager ein oder mehrere Objekte einem Konfigurationsprofil für die Verteilung an subscribierende verwaltete Server zugeordnet werden. Nach der Subskription eines verwalteten Servers für ein Profil sendet der Konfigurationsmanager dem Profil zugeordnete Objektdefinitionen an den verwalteten Server, wo sie in der Datenbank gespeichert werden. Auf diese Weise in der Datenbank eines verwalteten Servers erstellte Objekte werden zu verwalteten Objekten. Ein Objekt kann mehreren Profilen zugeordnet werden.

Mit diesem Befehl können eine anfängliche Gruppe von Profilzuordnungen definiert und vorhandenen Zuordnungen weitere Zuordnungen hinzugefügt werden.

Einem Profil können die folgenden Arten von Objekten zugeordnet werden:

- Administratorregistrierungen und -berechtigungen
- Maßnahmendomänen, die die Maßnahmengruppen der Domänen einschließen, Verwaltungsklassen, Kopiengruppen und Clientzeitpläne
- Verwaltungszeitpläne
- Server-Befehlsprozeduren
- Client-Optionsgruppen
- Serverdefinitionen
- Server-Gruppendefinitionen

Tipp: Der Konfigurationsmanager verteilt keine Statusinformationen für ein Objekt an verwaltete Server. Beispielsweise wird die Anzahl Tage seit dem letzten Zugriff eines Administrators auf den Server nicht an verwaltete Server verteilt. Diese Art der Informationen wird in den Datenbanken der einzelnen verwalteten Server verwaltet.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-DEFine PROFASSOCIation--Profilname----->
>-----+-----+-----+----->
  '-ADMinS-----+*-----+-'
      | .-,----- . |
      | V             | |
      '---Administratorname---+'
>-----+-----+-----+----->
  '-DObains-----+*-----+-'
      | .-,----- . |
      | V             | |
      '---Domänennamen---+'
>-----+-----+-----+----->
  '-ADSCHeds-----+*-----+-'
      | .-,----- . |
      | V             | |
      '---Zeitplannamen---+'
>-----+-----+-----+----->
  '-SCRipts-----+*-----+-'
      | .-,----- . |
```

```

          | v          | |
          '---Scriptname-+-'
>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
  '-CLOptsets--+-+*-----+-----+-----+-----+-----+-----+----->
          | .-,-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
          | v          | |
          '---Optionsgruppenname-+-'

>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
  '-SERVers--+-+*-----+-----+-----+-----+-----+-----+----->
          | .-,-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
          | v          | |
          '---Servername-+-'

>-----+-----+-----+-----+-----+-----+-----+-----+-----+-----><
  '-SERVERGroups--+-+*-----+-----+-----+-----+-----+-----+-----><
          | .-,-----+-----+-----+-----+-----+-----+-----+-----+-----+-----><
          | v          | |
          '---Gruppenname-+-'

```

## Parameter

### Profilname (Erforderlich)

Gibt den Namen des Konfigurationsprofils an.

### ADMins

Gibt Administratoren an, die dem Profil zugeordnet werden sollen. Es können Platzhalterzeichen in den Namen verwendet werden. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Verwenden Sie die globale Definition, einen einzelnen Stern (\*), um alle Administratoren anzugeben, die für den Konfigurationsmanager registriert sind. Wird die globale Definition angegeben und werden später weitere Administratoren hinzugefügt, werden sie automatisch über das Profil verteilt.

Der Konfigurationsmanager verteilt den Administratorkennnamen, das Kennwort, die Kontaktinformationen und die Berechtigungen der Administratoren, die dem Profil zugeordnet sind. Folgendes wird vom Konfigurationsmanager nicht verteilt:

- Der Administrator mit dem Namen SERVER\_CONSOLE, auch wenn eine globale Definition verwendet wird
- Der gesperrte oder entsperrte Status eines Administrators

Sind dem Profil bereits Administratoren zugeordnet, gilt folgendes:

- Wird eine Liste mit Administratoren angegeben und ist bereits eine Liste vorhanden, kombiniert IBM Spectrum Protect die neue Liste mit der vorhandenen Liste.
- Wird eine globale Definition angegeben und ist bereits eine Liste mit Administratoren vorhanden, ersetzt IBM Spectrum Protect die Liste durch die globale Definition.
- Wird eine Liste mit Administratoren angegeben und wurde zuvor eine globale Definition angegeben, ignoriert IBM Spectrum Protect die Liste. Zum Entfernen der globalen Definition den Befehl DELETE PROFASSOCIATION mit dem Parameter ADMINS=\* ausgeben.

### DOMains

Gibt Maßnahmendomänen an, die dem Profil zugeordnet werden sollen. Es können Platzhalterzeichen in den Namen verwendet werden. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Verwenden Sie die globale Definition, einen einzelnen Stern (\*), um alle Domänen anzugeben, die auf dem Konfigurationsmanager definiert sind. Wird die globale Definition angegeben und werden später weitere Domänen hinzugefügt, werden sie automatisch über das Profil verteilt.

Der Konfigurationsmanager verteilt Domäneninformationen, zu denen Definitionen von Maßnahmendomänen, Maßnahmengruppen, Verwaltungsklassen, Kopiengruppen und Clientzeitplänen gehören. Der Konfigurationsmanager verteilt nicht die AKTIVE Maßnahmengruppe. Administratoren auf einem verwalteten Server können eine beliebige Maßnahmengruppe innerhalb einer verwalteten Domäne auf einem verwalteten Server aktivieren.

Sind dem Profil bereits Domänen zugeordnet, gilt folgendes:

- Wird eine Liste mit Domänen angegeben und ist bereits eine Liste vorhanden, kombiniert IBM Spectrum Protect die neue Liste mit der vorhandenen Liste.
- Wird eine globale Definition verwendet und ist bereits eine Liste mit Domänen vorhanden, ersetzt IBM Spectrum Protect die Liste durch die globale Definition.
- Wird eine Liste mit Domänen angegeben und wurde zuvor eine globale Definition angegeben, ignoriert IBM Spectrum Protect die Liste. Zum Entfernen der globalen Definition den Befehl DELETE PROFASSOCIATION mit dem Parameter DOMAINS=\* ausgeben.

Wichtig: Client-Operationen, wie beispielsweise Sichern und Archivieren, schlagen fehl, wenn keine Zielpools vorhanden sind. Daher müssen verwaltete Server, die für dieses Profil subscribieren, über Definitionen für alle Speicherpools verfügen, die als Zielorte in den zugeordneten Domänen angegeben sind. Mit dem Befehl `RENAME STGPOOL` können vorhandene Speicherpools so umbenannt werden, dass sie den verteilten Zielnamen entsprechen.

#### ADSCHeds

Gibt Verwaltungszeitpläne an, die dem Profil zugeordnet werden sollen. Es können Platzhalterzeichen in den Namen verwendet werden. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Verwenden Sie die globale Definition, einen einzelnen Stern (\*), um alle Verwaltungszeitpläne anzugeben, die auf dem Konfigurationsmanager definiert sind. Wird die globale Definition angegeben und werden später weitere Verwaltungszeitpläne hinzugefügt, werden sie automatisch über das Profil verteilt.

Tipp: Verwaltungszeitpläne sind nicht aktiv, wenn sie von einem Konfigurationsmanager verteilt werden. Ein Administrator auf einem verwalteten Server muss jeden Zeitplan aktivieren, damit er auf diesem Server ausgeführt wird.

Sind dem Profil bereits Verwaltungszeitpläne zugeordnet, gilt folgendes:

- Wird eine Liste mit Verwaltungszeitplänen angegeben und ist bereits eine Liste vorhanden, kombiniert IBM Spectrum Protect die neue Liste mit der vorhandenen Liste.
- Wird eine globale Definition verwendet und ist bereits eine Liste mit Verwaltungszeitplänen vorhanden, ersetzt IBM Spectrum Protect die Liste durch die globale Definition.
- Wird eine Liste mit Verwaltungszeitplänen angegeben und wurde zuvor eine globale Definition angegeben, ignoriert IBM Spectrum Protect die Liste. Zum Entfernen der globalen Definition den Befehl `DELETE PROFASSOCIATION` mit dem Parameter `ADSCHEDS=*` ausgeben.

#### SCRipts

Gibt Server-Befehlsprozeduren an, die dem Profil zugeordnet werden sollen. Es können Platzhalterzeichen in den Namen verwendet werden. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Verwenden Sie die globale Definition, einen einzelnen Stern (\*), um alle Prozeduren anzugeben, die auf dem Konfigurationsmanager definiert sind. Wird die globale Definition angegeben und werden später weitere Prozeduren hinzugefügt, werden sie automatisch über das Profil verteilt.

Sind dem Profil bereits Prozeduren zugeordnet, gilt folgendes:

- Wird eine Liste mit Prozeduren angegeben und ist bereits eine Liste vorhanden, kombiniert IBM Spectrum Protect die neue Liste mit der vorhandenen Liste.
- Wird eine globale Definition verwendet und ist bereits eine Liste mit Prozeduren vorhanden, ersetzt IBM Spectrum Protect die Liste durch die globale Definition.
- Wird eine Liste mit Prozeduren angegeben und wurde zuvor eine globale Definition angegeben, ignoriert IBM Spectrum Protect die Liste. Zum Entfernen der globalen Definition den Befehl `DELETE PROFASSOCIATION` mit dem Parameter `SCRIPTS=*` ausgeben.

#### CLOptsets

Gibt Clientoptionsgruppen an, die dem Profil zugeordnet werden sollen. Es können Platzhalterzeichen in den Namen verwendet werden. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Verwenden Sie die globale Definition, einen einzelnen Stern (\*), um alle Clientoptionsgruppen anzugeben, die auf dem Konfigurationsmanager definiert sind. Wird die globale Definition angegeben und werden später weitere Client-Optionsgruppen hinzugefügt, werden sie automatisch über das Profil verteilt.

Sind dem Profil bereits Client-Optionsgruppen zugeordnet, gilt folgendes:

- Wird eine Liste mit Client-Optionsgruppen angegeben und ist bereits eine Liste vorhanden, kombiniert IBM Spectrum Protect die neue Liste mit der vorhandenen Liste.
- Wird eine globale Definition verwendet und ist bereits eine Liste mit Client-Optionsgruppen vorhanden, ersetzt IBM Spectrum Protect die Liste durch die globale Definition.
- Wird eine Liste mit Client-Optionsgruppen angegeben und wurde zuvor eine globale Definition angegeben, ignoriert IBM Spectrum Protect die Liste. Zum Entfernen der globalen Definition den Befehl `DELETE PROFASSOCIATION` mit dem Parameter `CLOPSETS=*` ausgeben.

#### SERVers

Gibt Server-Definitionen an, die dem Profil zugeordnet werden sollen. Die Definitionen werden an verwaltete Server verteilt, die für dieses Profil subscribieren. Es können Platzhalterzeichen in den Namen verwendet werden. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Verwenden Sie die globale Definition, einen einzelnen Stern (\*), um alle Server anzugeben, die auf dem Konfigurationsmanager definiert sind. Wird die globale Definition angegeben und werden später weitere Server hinzugefügt, werden sie automatisch über das Profil verteilt.

Der Konfigurationsmanager verteilt die folgenden Serverattribute: Übertragungsmethode, IP-Adresse, Anschlussadresse, Serverkennwort, URL und die Beschreibung. Für verteilte Serverdefinitionen ist das Attribut `ALLOWREPLACE` auf dem verwalteten Server immer auf `YES` gesetzt, unabhängig von dem Wert dieses Parameters auf dem Konfigurationsmanager. Auf dem verwalteten Server kann der Befehl `UPDATE SERVER` verwendet werden, um alle anderen Attribute zu definieren.

Sind dem Profil bereits Server zugeordnet, gilt folgendes:

- Wird eine Liste mit Servern angegeben und ist bereits eine Liste vorhanden, kombiniert IBM Spectrum Protect die neue Liste mit der vorhandenen Liste.
- Wird eine globale Definition verwendet und ist bereits eine Liste mit Servern vorhanden, ersetzt IBM Spectrum Protect die Liste durch die globale Definition.
- Wird eine Liste mit Servern angegeben und wurde zuvor eine globale Definition angegeben, ignoriert IBM Spectrum Protect die Liste. Zum Entfernen der globalen Definition den Befehl DELETE PROFASSOCIATION mit dem Parameter SERVERS=\* ausgeben.

Wichtig:

1. Eine Serverdefinition auf einem verwalteten Server wird nicht durch eine Definition von dem Konfigurationsmanager ersetzt, es sei denn, es wurde das Ersetzen der Definition auf dem verwalteten Server erlaubt. Um das Ersetzen zu erlauben, die Serverdefinition auf dem verwalteten Server aktualisieren, indem der Befehl UPDATE SERVER mit ALLOWREPLACE=YES verwendet wird.
2. Wenn ein Konfigurationsmanager eine Serverdefinition an einen verwalteten Server verteilt und eine Servergruppe mit demselben Namen auf dem verwalteten Server vorhanden ist, ersetzt die verteilte Serverdefinition die Servergruppendefinition.

#### SERVERGroups

Gibt Server-Gruppen an, die dem Profil zugeordnet werden sollen. Es können Platzhalterzeichen in den Namen verwendet werden. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Verwenden Sie die globale Definition, einen einzelnen Stern (\*), um alle Servergruppen anzugeben, die auf dem Konfigurationsmanager definiert sind. Wird die globale Definition angegeben und werden später weitere Server-Gruppen hinzugefügt, werden sie automatisch über das Profil verteilt.

Tipp: Ein Konfigurationsmanager verteilt eine Servergruppendefinition nicht an einen verwalteten Server, wenn dieser über eine Serverdefinition mit demselben Namen wie die Servergruppe verfügt.

Sind dem Profil bereits Server-Gruppen zugeordnet, gilt folgendes:

- Wird eine Liste mit Server-Gruppen angegeben und ist bereits eine Liste vorhanden, kombiniert IBM Spectrum Protect die neue Liste mit der vorhandenen Liste.
- Wird eine globale Definition verwendet und ist bereits eine Liste mit Server-Gruppen vorhanden, ersetzt IBM Spectrum Protect die Liste durch die globale Definition.
- Wird eine Liste mit Server-Gruppen angegeben und wurde zuvor eine globale Definition angegeben, ignoriert IBM Spectrum Protect die Liste. Zum Entfernen der globalen Definition den Befehl DELETE PROFASSOCIATION mit dem Parameter SERVERGROUPS=\* ausgeben.

### Beispiel: Eine bestimmte Domäne einem bestimmten Profil zuordnen

Die Domäne MARKETING dem Profil DELTA zuordnen.

```
define profassociation delta domains=marketing
```

### Beispiel: Alle Domänen einem bestimmten Profil zuordnen

Es wurde bereits eine Liste mit Domänen dem Profil GAMMA zugeordnet. Jetzt sollen alle Domänen, die auf dem Konfigurationsmanager definiert sind, dem Profil zugeordnet werden.

```
define profassociation gamma domains=*
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE PROFASSOCIATION

| Befehl                 | Beschreibung   |
|------------------------|--|
| COPY PROFILE           | Erstellt eine Kopie eines Profils.   |
| DEFINE PROFILE         | Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.  |
| DELETE PROFASSOCIATION | Löscht die Zuordnung zwischen einem Objekt und einem Profil.                     |
| DELETE PROFILE         | Löscht ein Profil aus einem Konfigurationsmanager.                               |
| LOCK PROFILE           | Verhindert die Verteilung eines Konfigurationsprofils.                           |
| NOTIFY SUBSCRIBERS     | Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin. |
| QUERY PROFILE          | Zeigt Informationen über Konfigurationsprofile an.                               |

| Befehl            | Beschreibung   |
|-------------------|--|
| SET CONFIGMANAGER | Gibt an, ob ein Server ein Konfigurationsmanager ist.                    |
| UNLOCK PROFILE    | Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server. |
| UPDATE PROFILE    | Ändert die Beschreibung eines Profils.                                   |

## DEFINE PROFILE (Profil definieren)

Mit diesem Befehl kann auf einem Konfigurationsmanager ein Profil (eine Gruppe von Konfigurationsdaten) definiert werden, das an verwaltete Server verteilt werden kann.

Nach der Definition eines Profils können mit dem Befehl DEFINE PROFASSOCIATION Objekte angegeben werden, die an subscribierende verwaltete Server für das Profil verteilt werden sollen.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DEFine PROFIle--Profilname----->
>--+-----+-----><
  '-DESCRiption-----Beschreibung-'
```

### Parameter

Profilname (Erforderlich)

Gibt den Namen des Profils an. Die maximale Länge des Namens beträgt 30 Zeichen.

DESCRiption

Gibt eine Beschreibung des Profils an. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Dieser Parameter ist wahlfrei.

### Beispiel: Ein neues Profil definieren

Das Profil ALPHA mit der Beschreibung "Programming Center" definieren.

```
define profile alpha
description="Programming Center"
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE PROFILE

| Befehl                 | Beschreibung   |
|------------------------|--|
| COPY PROFILE           | Erstellt eine Kopie eines Profils.                                       |
| DEFINE PROFASSOCIATION | Ordnet Objekte einem Profil zu.  |
| DEFINE SUBSCRIPTION    | Subskribiert einen verwalteten Server für ein Profil.                    |
| DELETE PROFASSOCIATION | Löscht die Zuordnung zwischen einem Objekt und einem Profil.             |
| DELETE PROFILE         | Löscht ein Profil aus einem Konfigurationsmanager.                       |
| LOCK PROFILE           | Verhindert die Verteilung eines Konfigurationsprofils.                   |
| QUERY PROFILE          | Zeigt Informationen über Konfigurationsprofile an.                       |
| SET CONFIGMANAGER      | Gibt an, ob ein Server ein Konfigurationsmanager ist.                    |
| UNLOCK PROFILE         | Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server. |
| UPDATE PROFILE         | Ändert die Beschreibung eines Profils.                                   |

## DEFINE RECMEDMACHASSOCIATION (Wiederh.-Datenträger Maschine zuordnen)

Mit diesem Befehl können Wiederherstellungsdatenträger einer oder mehreren Maschinen zugeordnet werden. Einer Maschine werden Wiederherstellungsdatenträger zugeordnet, damit der Speicherort der Boot-Datenträger und die Liste der Datenträgernamen zur Verfügung stehen, wenn für die Maschine eine Wiederherstellung erforderlich ist. Zum Abrufen der Informationen den Befehl QUERY MACHINE ausgeben. Diese Informationen werden in der Wiederherstellungsplandatei berücksichtigt, um den Benutzer bei der Wiederherstellung der Clientmaschinen zu unterstützen.

Sollen einer Maschine Wiederherstellungsdatenträger zugeordnet werden, müssen die Maschine und die Datenträger in IBM Spectrum Protect definiert sein. Eine Maschine bleibt so lange den Datenträgern zugeordnet, bis die Zuordnung, die Datenträger oder die Maschine gelöscht wird bzw. werden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DEFine RECMEDMACHAssociation--Datenträgername----->
      .-,-----
      v          |
>---Maschinennamen-----<
```

### Parameter

Datenträgername (Erforderlich)

Gibt den Namen des Wiederherstellungsdatenträgers an, dem Maschinen zugeordnet werden.

Maschinennamen (Erforderlich)

Gibt den Namen der Maschinen an, die dem Wiederherstellungsdatenträger zugeordnet werden sollen. Eine Maschine kann mehreren Wiederherstellungsdatenträgern zugeordnet werden. Soll eine Liste mit Maschinen angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.

### Beispiel: Wiederherstellungsdatenträgern Maschinen zuordnen

Die Maschinen DISTRICT1 und DISTRICT5 dem Wiederherstellungsdatenträger DIST5RM zuordnen.

```
define recmedmachassociation dist5rm
district1,district5
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE RECMEDMACHASSOCIATION

| Befehl                       | Beschreibung   |
|------------------------------|--|
| DEFINE MACHINE               | Definiert eine Maschine für DRM.   |
| DEFINE RECOVERYMEDIA         | Definiert die Datenträger, die für die Wiederherstellung einer Maschine erforderlich sind. |
| DELETE MACHINE               | Löscht eine Maschine.  |
| DELETE RECMEDMACHASSOCIATION | Löscht die Zuordnung zwischen Wiederherstellungsdatenträgern und einer Maschine.           |
| DELETE RECOVERYMEDIA         | Löscht Wiederherstellungsdatenträger.  |
| QUERY MACHINE                | Zeigt Informationen über Maschinen an.   |
| QUERY RECOVERYMEDIA          | Zeigt die für die Maschinenwiederherstellung verfügbaren Datenträger an.                   |

## DEFINE RECOVERYMEDIA (Wiederherstellungsdatenträger definieren)

Mit diesem Befehl können die Datenträger definiert werden, die für die Wiederherstellung einer Maschine benötigt werden. Derselbe Datenträger kann mehreren Maschinen zugeordnet werden. Zum Anzeigen der Informationen den Befehl QUERY MACHINE verwenden. Diese Informationen werden in der Wiederherstellungsplandatei berücksichtigt, um den Benutzer bei der Wiederherstellung der Client-Maschinen zu unterstützen.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-DEfine RECOVERYMedia--Datenträgername----->
>+-----+-----+-----+-----+----->
|           .-,----- . |
|           v           | |
|'-VOLumenames-----Datenträgername-+-'|
>+-----+-----+-----+-----+----->
|'-DESCription-----Beschreibung- '|
|
|           .-Type-----Other----- .
>+-----+-----+-----+-----+----->
|'-LLocation-----Position- ' |'-Type-----+Other-+-'|
|                                     '|-BOot--'|
>+-----+-----+-----+-----+----->
|'-PRoDuct-----Produktname- '|
>+-----+-----+-----+-----+-----><
|'-PRoDUCTInfo-----Produktinformationen- '|
```

## Parameter

### Datenträgername (Erforderlich)

Gibt den Namen des Wiederherstellungsdatenträgers an, der definiert werden soll. Der Name kann bis zu 30 Zeichen umfassen.

### VOLumenames

Gibt die Namen der Datenträger an, die die wiederherstellbaren Daten enthalten (z. B. Abbildkopien des Betriebssystems). Dieser Parameter ist erforderlich, wenn der Datenträgertyp BOOT angegeben wird. Die Namen der Boot-Datenträger in der Reihenfolge angeben, in der sie zur Wiederherstellungszeit in die Maschine eingelegt werden sollen. Die maximale Länge der Datenträgernamensliste beträgt 255 Zeichen. Die Liste in Anführungszeichen einschließen, wenn sie Leerzeichen enthält.

### DESCription

Gibt die Beschreibung der Wiederherstellungsdatenträger an. Dieser Parameter ist wahlfrei. Die maximale Länge beträgt 255 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

### Location

Gibt den Standort der Wiederherstellungsdatenträger an. Dieser Parameter ist wahlfrei. Die maximale Länge beträgt 255 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

### Type

Gibt den Typ von Wiederherstellungsdatenträger an. Dieser Parameter ist wahlfrei. Der Standardwert ist OTHER.

### BOot

Gibt an, daß dies ein Boot-Datenträger ist. Der Benutzer muß Datenträgernamen angeben, wenn der Typ BOOT lautet.

### Other

Gibt an, daß dies kein Boot-Datenträger ist. Beispielsweise eine CD, die Handbücher zum Betriebssystem enthält.

### PRoDuct

Gibt den Namen des Produkts an, das auf diesen Datenträger geschrieben hat. Dieser Parameter ist wahlfrei. Die maximale Länge beträgt 16 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

### PRoDUCTInfo

Gibt Informationen zum Produkt an, das auf die Datenträger geschrieben hat. Hierbei handelt es sich um Informationen, die möglicherweise zum Wiederherstellen der Maschine benötigt werden. Dieser Parameter ist wahlfrei. Die maximale Länge beträgt 255 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

## Beispiel: Die Datenträger definieren, die für die Wiederherstellung einer Maschine benötigt werden



Den Wiederherstellungsdatenträger DIST5RM definieren. Eine Beschreibung und den Standort einschließen.

```
define recoverymedia dist5rm
description="district 5 base system image"
location="district 1 vault"
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE RECOVERYMEDIA

| Befehl                       | Beschreibung   |
|------------------------------|--|
| DEFINE RECMEDMACHASSOCIATION | Ordnet Wiederherstellungsdatenträger einer Maschine zu.                  |
| DELETE RECOVERYMEDIA         | Löscht Wiederherstellungsdatenträger.                                    |
| QUERY RECOVERYMEDIA          | Zeigt die für die Maschinenwiederherstellung verfügbaren Datenträger an. |
| UPDATE RECOVERYMEDIA         | Ändert die Attribute von Wiederherstellungsdatenträgern.                 |

## DEFINE SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl definieren)

Mit diesem Befehl kann ein Zeitplan für einen Client oder Verwaltungsbefehl erstellt werden.

Der Befehl DEFINE SCHEDULE hat zwei Formen: Eine Form, wenn der Zeitplan Clientoperationen betrifft, und eine Form, wenn der Zeitplan Verwaltungsbefehle betrifft. Innerhalb dieser beiden Formen können Sie entweder Zeitpläne mit klassischer Darstellung oder Zeitpläne mit erweiterter Darstellung auswählen. Syntax und Parameter der jeweiligen Form werden separat definiert.

Für jeden Zeitplan wird ein Startfenster angegeben. Das Startfenster ist der Zeitraum, in dem der Zeitplan eingeleitet werden muß. Die Verarbeitung des Zeitplans wird nicht unbedingt innerhalb dieses Fensters beendet. Wenn der Server beim Start dieses Fensters nicht aktiv ist, aber vor Ende des definierten Fensters gestartet wird, wird der Zeitplan beim Neustart des Servers ausgeführt. Optionen, die jeder Zeitplandarstellung (klassisch und erweitert) zugeordnet sind, bestimmen, wann die Startfenster beginnen sollen.

Tabelle 1. Zugehörige Befehle für DEFINE SCHEDULE

| Befehl               | Beschreibung  |
|----------------------|---|
| COPY SCHEDULE        | Erstellt eine Kopie eines Zeitplans.  |
| DEFINE ASSOCIATION   | Ordnet Clients einem Zeitplan zu.   |
| DELETE SCHEDULE      | Löscht einen Zeitplan aus der Datenbank.  |
| QUERY EVENT          | Zeigt Informationen über geplante und abgeschlossene Ereignisse für ausgewählte Clients an.                             |
| QUERY SCHEDULE       | Zeigt Informationen über Zeitpläne an.  |
| SET MAXCMDRETRIES    | Gibt die maximale Anzahl Wiederholungen nach der fehlgeschlagenen Ausführung eines geplanten Befehls an.                |
| SET MAXSCHEDSESSIONS | Gibt die maximale Anzahl Client-/Serversitzungen an, die bei der Arbeit mit einem Verarbeitungszeitplan verfügbar sind. |
| SET RETRYPERIOD      | Gibt die Zeitspanne zwischen Wiederholungsversuchen des Client-Schedulers an.   |
| UPDATE SCHEDULE      | Ändert die Attribute eines Zeitplans.   |

- DEFINE SCHEDULE (Clientzeitplan definieren)  
Verwenden Sie den Befehl DEFINE SCHEDULE, um einen Clientzeitplan zu definieren. IBM Spectrum Protect verwendet diesen Zeitplan, um in angegebenen Intervallen oder an angegebenen Tagen verschiedene Clientoperationen für Ihre Client-Workstations automatisch auszuführen. Nach der Definition eines Zeitplans den Befehl DEFINE ASSOCIATION verwenden, um den Client dem Zeitplan zuzuordnen.
- DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)  
Mit dem Befehl DEFINE SCHEDULE kann ein neuer Zeitplan für die Verarbeitung eines Verwaltungsbefehls erstellt werden.

## DEFINE SCHEDULE (Clientzeitplan definieren)

Verwenden Sie den Befehl DEFINE SCHEDULE, um einen Clientzeitplan zu definieren. IBM Spectrum Protect verwendet diesen Zeitplan, um in angegebenen Intervallen oder an angegebenen Tagen verschiedene Clientoperationen für Ihre Client-Workstations automatisch

auszuführen. Nach der Definition eines Zeitplans den Befehl DEFINE ASSOCIATION verwenden, um den Client dem Zeitplan zuzuordnen.

Sie müssen den Client-Scheduler auf der Client-Workstation starten, damit IBM Spectrum Protect den Zeitplan verarbeiten kann.

Nicht alle Clients können alle geplanten Operationen ausführen, auch wenn Sie den Zeitplan auf dem Server definieren und ihn dem Client zuordnen können. Ein Macintosh-Client kann beispielsweise keinen Zeitplan ausführen, wenn es sich bei der Aktion um das Zurückschreiben oder Abrufen von Dateien oder um das Ausführen einer ausführbaren Prozedur handelt. Eine ausführbare Prozedur wird auch als Befehlsdatei, Stapeldatei oder Prozedur auf anderen Client-Betriebssystemen bezeichnet.

IBM Spectrum Protect kann nicht mehrere Zeitpläne gleichzeitig für denselben Clientknoten ausführen.

## Berechtigungsklasse

Zum Definieren eines Clientzeitplans ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der der Zeitplan gehört.

## Syntax

Klassischer Clientzeitplan

```
>>DEFine SCHEDULE--Domänenname--Zeitplanname----->
>+-----+-----+-----+-----+-----+----->
' -Type-----Client-' '-DESCRIPTION-----Beschreibung-'
. -ACTION-----Incremental-----,
>+-----+-----+-----+-----+-----+----->
' -ACTION-----Incremental-----+-'
+ -Selective-----+
+ -Archive-----+-----+-----+
| | | | |
| | | | |
| | | | |
| | | | |
+ -Backup-----+-----+-----+-----+
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
+ -RESTore-----+-----+-----+-----+
+ -RETRieve-----+-----+-----+-----+
+ -IMAGEBACKup-----+-----+-----+-----+
+ -IMAGERESTore-----+-----+-----+-----+
+ -Command-----+-----+-----+-----+
+ -Macro-----+-----+-----+-----+
' -Deploy-----+-----+-----+-----+'
>+-----+-----+-----+-----+-----+----->
' -OPTions-----Optionszeichenfolge-'
>+-----+-----+-----+-----+-----+----->
| | (1) | |
' -OBJects-----Objektzeichenfolge-'
. -PRIority-----5-----, . -STARTDate-----aktuelles_Datum-.
>+-----+-----+-----+-----+-----+----->
' -PRIority-----Zahl-' '-STARTDate-----Datum-----+'
. -STARTTime-----aktuelle_Zeit-. . -DURation-----1-----.
>+-----+-----+-----+-----+-----+----->
' -STARTTime-----Zeit-----' '-DURation-----Zahl-'
. -DURUnits-----Hours-----, . -MAXRUNTime-----0-----.
>+-----+-----+-----+-----+-----+----->
' -DURUnits-----+Minutes-----+' '-MAXRUNTime-----Anzahl-'
+ -Hours-----+
+ -Days-----+
' -INDefinite-'
. -SCHEDStyle-----Classic-. . -PERiod-----1-----.
>+-----+-----+-----+-----+-----+----->
' -SCHEDStyle-----Classic-' '-PERiod-----Zahl-'
```



```

.-DURUnits-----Hours----- .-MAXRUNtime-----0-----.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-DURUnits-----+Minutes-+' '-MAXRUNtime-----Anzahl-'
      +-Hours----+
      '-Days----'

.-Month-----ANY----- .
>--SCHEDStyle-----Enhanced-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
      '-Month-----+ANY-----+'
              +-JAnuary---+
              +-February--+
              +-MARch-----+
              +-APRil-----+
              +-May-----+
              +-JUNe-----+
              +-JULy-----+
              +-AUGust-----+
              +-September-+
              +-October---+
              +-November--+
              '-December--'

.-DAYOFMonth-----ANY----- .-WEEKofmonth-----ANY----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-DAYOFMonth-----+ANY-+' '-WEEKofmonth-----+ANY-----+'
      '-Day-'              +-First--+
                          +-Second+
                          +-Third--+
                          +-FOurth+
                          '-Last---'

.-DAYofweek-----ANY----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-DAYofweek-----+ANY-----+'
      +-WEEKDay---+
      +-WEEKEnd---+
      +-SUnDay----+
      +-Monday----+
      +-TUesday---+
      +-WednesDay-+
      +-THursday--+
      +-Friday----+
      '-SATurday--'

.-EXPIration-----Never----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----><
'-EXPIration-----+Never-+'
      '-Datum-'

```

Anmerkungen:

1. Der Parameter OBJECTS ist bei ACTION=INCREMENTAL optional, für andere Aktionen jedoch erforderlich.

## Parameter

Domänenname (Erforderlich)

Gibt den Namen der Maßnahmendomäne an, zu der dieser Zeitplan gehört.

Zeitplanname (Erforderlich)

Gibt den Namen des Zeitplans an, der definiert werden soll. Für den Namen können bis zu 30 Zeichen angegeben werden.

Type=Client

Gibt an, daß ein Zeitplan für einen Client definiert wird. Dieser Parameter ist wahlfrei.

DESCRIPTION

Gibt eine Beschreibung des Zeitplans an. Dieser Parameter ist wahlfrei. Für die Beschreibung können bis zu 255 Zeichen angegeben werden. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

ACTION

Gibt die Aktion an, die bei der Verarbeitung dieses Zeitplans ausgeführt wird. Gültige Werte:

Incremental

Gibt an, daß der Zeitplan alle Dateien sichert, die neu sind oder sich seit der letzten Teilsicherung geändert haben. Mit "Incremental" werden auch alle Dateien gesichert, für die alle vorhandenen Sicherungen möglicherweise verfallen sind.

Selective

Gibt an, daß der Zeitplan nur Dateien sichert, die mit dem Parameter OBJECTS angegeben werden.

Archive

Gibt an, daß der Zeitplan Dateien archiviert, die mit dem Parameter OBJECTS angegeben werden.

#### Backup

Gibt an, dass der Zeitplan Dateien sichert, die mit dem Parameter OBJECTS angegeben werden.

#### REStore

Gibt an, daß der Zeitplan Dateien zurückschreibt, die mit dem Parameter OBJECTS angegeben werden.

Wenn Sie ACTION=RESTORE für eine geplante Operation angeben, und ist die Option REPLACE auf PROMPT gesetzt, erfolgt keine Aufforderung. Wird die Option auf PROMPT gesetzt, werden die Dateien übersprungen.

Wenn Sie eine zweite Dateispezifikation angeben, agiert diese zweite Dateispezifikation als Zielort für die Zurückschreibung. Müssen mehrere Gruppen von Dateien zurückgeschrieben werden, planen Sie eine für jede Dateispezifikation, die zurückgeschrieben werden muss.

#### RETRieve

Gibt an, dass der Zeitplan Dateien abrufen, die mit dem Parameter OBJECTS angegeben werden.

Hinweis: Eine zweite Datei, die angegeben wird, dient als Abrufzielort. Müssen mehrere Gruppen von Dateien abgerufen werden, erstellen Sie einen separaten Zeitplan für jede Dateigruppe.

#### IMAGEBACKup

Gibt an, daß der Zeitplan logische Datenträger sichert, die mit dem Parameter OBJECTS angegeben werden.

#### IMAGERESTore

Gibt an, daß der Zeitplan logische Datenträger zurückschreibt, die mit dem Parameter OBJECTS angegeben werden.

#### Command

Gibt an, dass der Zeitplan einen Client-Betriebssystembefehl oder ein Script verarbeitet, der bzw. das mit dem Parameter OBJECTS angegeben wird.

#### Macro

Gibt an, daß ein Client ein Makro verarbeitet, dessen Dateiname im Parameter OBJECTS angegeben ist.

#### SUBACTion

Sie können einen der folgenden Werte angeben:

""

Wenn eine Nullzeichenfolge (zwei Anführungszeichen) mit ACTION=BACKUP angegeben wird, ist die Sicherung eine Teilsicherung.

#### FASTBacK

Gibt an, dass eine FastBack-Clientoperation, die durch den Parameter ACTION angegeben wird, für die Verarbeitung geplant werden soll. Der Wert des Parameters ACTION muss ARCHIVE oder BACKUP sein.

#### SYSTEMStAte

Gibt an, dass eine Clientsystemstatussicherung geplant ist.

#### VApp

Gibt an, dass eine vApp-Clientsicherung geplant ist. Eine vApp ist eine Sammlung von vorimplementierten virtuellen Maschinen.

#### VM

Gibt an, dass eine VMware-Clientsicherungsoperation geplant ist.

#### Deploy

Gibt an, ob Client-Workstations mit Implementierungspaketen aktualisiert werden sollen, die mit dem Parameter OBJECTS angegeben werden. Der Parameter OBJECTS muss zwei Spezifikationen enthalten: die Paketdateien, die abgerufen werden sollen, und die Position, an der sie abgerufen werden sollen. Stellen Sie sicher, dass die Objekte die Reihenfolge *Dateien Position* haben. Beispiel:

```
define schedule standard deploy_1 action=DEPLOY objects=
"\\IBM_ANR_WIN\c$\tsm\maintenance\client\v6r2\Windows\X32\v620\v6200\*
..\IBM_ANR_WIN\"
```

Die Werte für die folgenden Optionen sind eingeschränkt, wenn Sie ACTION=DEPLOY angeben:

#### PERUNITS

Geben Sie PERUNITS=ONETIME an. Wenn Sie PERUNITS=PERIOD angeben, wird der Parameter ignoriert.

#### DURUNITS

Geben Sie MINUTES, HOURS oder DAYS für den Parameter DURUNITS an. Geben Sie nicht INDEFINITE an.

#### SCHEDSTYLE

Geben Sie die Standarddarstellung CLASSIC an.


Der Befehl SCHEDULE schlägt fehl, wenn die Parameter nicht den erforderlichen Parameterwerten wie V.R.M.F entsprechen.

#### OPTions

Gibt die Clientoptionen an, die für den geplanten Befehl angegeben werden, wenn der Zeitplan verarbeitet wird. Dieser Parameter ist wahlfrei.

Für diesen Parameter können nur die Optionen angegeben werden, die für den geplanten Befehl gültig sind. Informationen zu den Optionen, die in der Befehlszeile gültig sind, befinden sich im entsprechenden Clienthandbuch. Alle Optionen, für die im Clienthandbuch angegeben ist, dass sie nur in der Anfangsbefehlszeile gültig sind, führen zu einem Fehler oder werden ignoriert, wenn der Zeitplan vom Server ausgeführt wird. Geben Sie beispielsweise die folgenden Optionen nicht an, da sie keinen Einfluss darauf haben, wann der Client den geplanten Befehl verarbeitet:

- MAXCMDRETRIES
- OPTFILE
- QUERYSCHEDPERIOD
- RETRYPERIOD
- SCHEDLOGNAME
- SCHEDMODE
- SERVERNAME
- TCPCLIENTADDRESS
- TCPCLIENTPORT

 Wenn Sie einen Scheduler-Service definieren, indem Sie den Befehl DSMCUTIL oder den Assistenten für die GUI des Clients für Sichern/Archivieren verwenden, geben Sie eine Optionsdatei an. Sie können die Optionen in dieser Optionsdatei nicht überschreiben, indem Sie den geplanten Befehl ausgeben. Sie müssen die Optionen in Ihrem Schedulerservice ändern.

Enthält die Optionszeichenfolge mehrere Optionen oder Optionen mit eingebetteten Leerzeichen, schließen Sie die gesamte Optionszeichenfolge in Hochkommas ein. Schließen Sie einzelne Optionen, die Leerzeichen enthalten, in Anführungszeichen ein. Vor der Option muss ein führendes Minuszeichen stehen. Fehler können auftreten, wenn die Optionszeichenfolge Leerzeichen enthält, die nicht korrekt in Anführungszeichen eingeschlossen sind.

Die folgenden Beispiele zeigen, wie einige Clientoptionen angegeben werden:

- Geben Sie Folgendes ein, um `subdir=yes` und `domain all-local -systemobject` anzugeben:
  - `options='-subdir=yes -domain="all-local -c: -systemobject"'`
- Geben Sie Folgendes ein, um `domain all-local -c: -d:` anzugeben:
  - `options='-domain="all-local -c: -d:"'`

 Tipp:

Für Windows-Clients, die im Stapelbetrieb ausgeführt werden: Ist die Verwendung von Anführungszeichen erforderlich, verwenden Sie den Dialogmodus oder Escapezeichen des Betriebssystems. Weitere Informationen liefern die folgenden Abschnitte:

- Eine Serie von Befehlen des Verwaltungsclients verarbeiten
- Einzelne Befehle mit dem Verwaltungsclient verarbeiten

## Objects

Gibt die Objekte an, für die die angegebene Aktion ausgeführt wird. Verwenden Sie ein einzelnes Leerzeichen zwischen jedem Objekt. Außer bei `ACTION=INCREMENTAL` ist dieser Parameter erforderlich. Ist die Aktion eine Sicherungs-, Archivierungs-, Abruf- oder Zurückschreibungsoperation, sind die Objekte Dateibereiche, Verzeichnisse oder logische Datenträger. Dient die Aktion zur Ausführung eines Befehls oder Makros, ist das Objekt der Name des auszuführenden Befehls oder Makros.

Wenn `ACTION=INCREMENTAL` ohne Angabe eines Werts für diesen Parameter angegeben wird, wird der geplante Befehl ohne angegebene Objekte aufgerufen, und der Befehl versucht, die Objekte wie in der Clientoptionsdatei definiert zu verarbeiten. Um alle Dateibereiche oder Verzeichnisse für eine Aktion auszuwählen, müssen sie explizit in der Objektzeichenfolge aufgeführt werden. Wird nur ein Stern in die Objektzeichenfolge eingegeben, erfolgt die Sicherung nur für das Verzeichnis, bei dem der Scheduler gestartet wurde.

Wichtig:

- Wenn Sie eine zweite Dateispezifikation angeben, und handelt es sich nicht um einen gültigen Zielort, empfangen Sie diesen Fehler:


```
ANS1082E Ungültige
Zieldateispezifikation <Dateispezifikation> eingegeben.
```

- Geben Sie mehr als zwei Dateispezifikationen an, empfangen Sie diesen Fehler:



```
ANS1102E Zu viele Befehlszeilenparameter an das Programm übergeben!
```

Wird für diesen Parameter `ACTION=ARCHIVE`, `INCREMENTAL` oder `SELECTIVE` angegeben, können Sie maximal 20 Dateispezifikationen auflisten.

Schließen Sie die Objektzeichenfolge in Anführungszeichen ein, wenn sie Leerzeichen enthält, und schließen Sie dann die Anführungszeichen in Hochkommas ein. Enthält die Objektzeichenfolge mehrere Dateinamen, schließen Sie jeden Dateinamen in Anführungszeichen ein und schließen Sie dann die gesamte Zeichenfolge in Hochkommas ein. Fehler können auftreten, wenn Dateinamen ein Leerzeichen enthalten, das nicht korrekt in Anführungszeichen eingeschlossen ist.

 Windows-Betriebssysteme Wenn Sie Zeichen verwenden, die für Windows-Benutzer eine besondere Bedeutung haben, wie z. B. Kommas, schließen Sie das gesamte Argument in doppelte Anführungszeichen ein und schließen Sie dann die gesamte Zeichenfolge in Hochkommas ein. Die folgenden Beispiele zeigen, wie einige Dateinamen angegeben werden:

- Geben Sie Folgendes ein, um C:\FILE 2, D:\GIF FILES und E:\MY TEST FILE anzugeben:
  - OBJECTS="C:\FILE 2" "D:\GIF FILES" "E:\MY TEST FILE"
- Geben Sie Folgendes ein, um D:\TEST FILE anzugeben:
  - OBJECTS="D:\TEST FILE"
- Geben Sie Folgendes ein, um D:TEST,FILE anzugeben:
  - OBJECTS="D:\TEST,FILE"

 AIX-Betriebssysteme  Linux-Betriebssysteme Die folgenden Beispiele zeigen, wie einige Dateinamen angegeben werden:

- Geben Sie Folgendes ein, um /home/file 2, /home/gif files und /home/my test file anzugeben:
  - OBJECTS="/home/file 2" "/home/gif files" "/home/my test file"
- Geben Sie Folgendes ein, um /home/test file anzugeben:
  - OBJECTS="/home/test file"

 Windows-Betriebssysteme Tipp:

Für Windows-Clients, die im Stapelbetrieb ausgeführt werden: Ist die Verwendung von Anführungszeichen erforderlich, verwenden Sie den Dialogmodus oder Escapezeichen des Betriebssystems. Weitere Informationen liefern die folgenden Abschnitte:

- Eine Serie von Befehlen des Verwaltungsclients verarbeiten
- Einzelne Befehle mit dem Verwaltungsclient verarbeiten

#### PRIority

Gibt den Prioritätswert für einen Zeitplan an. Dieser Parameter ist wahlfrei. Zulässige Werte sind ganze Zahlen von 1 bis 10, wobei 1 die höchste Priorität und 10 die niedrigste Priorität angibt. Der Standardwert ist 5.

Wenn zwei oder mehr Zeitpläne dieselbe Fensterstartzeit haben, legt der angegebene Wert fest, wann IBM Spectrum Protect den Zeitplan verarbeitet. Der Zeitplan mit der höchsten Priorität startet zuerst. Ein Zeitplan mit PRIORITY=3 startet beispielsweise vor einem Zeitplan mit PRIORITY=5.

#### STARTDate

Gibt das Datum für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum. Diesen Parameter zusammen mit dem Parameter STARTTIME verwenden, um anzugeben, wann das Anfangsstartfenster des Zeitplans startet.

Sie können das Datum unter Verwendung der folgenden Werte angeben:

| Wert                            | Beschreibung  | Beispiel   |
|---------------------------------|---|--|
| MM/TT/JJJJ                      | Ein bestimmtes Datum  | 09/15/1998   |
| TODAY                           | Das aktuelle Datum  | TODAY  |
| TODAY+Tage <b>oder</b><br>+Tage | Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY +3 <b>oder</b> +3.   |
| EOLM (Ende des letzten Monats)  | Der letzte Tag des Vormonats.   | EOLM   |
| EOLM-Tage                       | Der letzte Tag des Vormonats minus angegebene Tage.   | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)     | Der erste Tag des aktuellen Monats.   | BOTM   |
| BOTM+Tage                       | Der erste Tag des aktuellen Monats plus angegebene Tage.  | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

## STARTTime

Gibt die Uhrzeit für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist die aktuelle Uhrzeit. Dieser Parameter gibt in Verbindung mit dem Parameter STARTDATE den Beginn des Anfangsstartfensters an.

Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

| Wert                             | Beschreibung   | Beispiel   |
|----------------------------------|--|--|
| HH:MM:SS                         | Eine bestimmte Uhrzeit   | 10:30:08   |
| NOW                              | Die aktuelle Uhrzeit   | NOW  |
| NOW+HH:MM <b>oder</b><br>+HH:MM  | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten  | NOW+02:00 <b>oder</b> +02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW+02:00 oder STARTTIME=+02:00 ausgegeben, beginnt das Startfenster um 7:00 Uhr. |
| NOW-HH:MM <b>oder</b> -<br>HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten | NOW-02:00 <b>oder</b> -02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW-02:00 oder STARTTIME=-02:00 ausgegeben, beginnt das Startfenster um 3:00 Uhr. |

## DURation

Gibt die Anzahl Einheiten an, die die Länge des Startfensters der geplanten Operation definiert. Dieser Parameter ist wahlfrei. Dieser Wert muß zwischen 1 und 999 liegen. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter DURUNITS verwenden, um die Länge des Startfensters anzugeben. Werden beispielsweise DURATION=20 und DURUNITS=MINUTES angegeben, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Standardlänge des Startfensters beträgt 1 Stunde. Die Länge des Fensters muß kürzer sein, als der Zeitraum zwischen Fenstern.

Dieser Wert wird ignoriert, wenn DURUNITS=INDEFINITE angegeben wird.

Tipp: Definieren Sie Zeitpläne mit einer Dauer von mehr als 10 Minuten. Damit erhält der IBM Spectrum Protect-Scheduler genügend Zeit, den Zeitplan zu verarbeiten und den Client abzufragen.

## DURUnits

Gibt die Zeiteinheiten an, mit denen die Dauer des Fensters bestimmt wird, in dem der Zeitplan starten kann. Dieser Parameter ist wahlfrei. Der Standardwert ist HOURS.

Diesen Parameter zusammen mit dem Parameter DURATION verwenden, um anzugeben, wie lange das Startfenster geöffnet bleibt, um den Zeitplan zu verarbeiten. Gilt beispielsweise DURATION=20 und DURUNITS=MINUTES, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Verarbeitung des Zeitplans muß nicht unbedingt innerhalb dieses Fensters enden. Wenn der Zeitplan aus irgendeinem Grund wiederholt werden muß, müssen die Wiederholungsversuche vor Ablauf des Startfensters beginnen; andernfalls wird die Operation nicht erneut gestartet.

Der Standardwert für die Länge des Startfensters ist 1 Stunde. Sie können einen der folgenden Werte angeben:

### Minutes

Gibt an, daß die Dauer des Fensters in Minuten definiert wird.

### Hours

Gibt an, daß die Dauer des Fensters in Stunden definiert wird.

### Days

Gibt an, daß die Dauer des Fensters in Tagen definiert wird.

### INDefinite

Gibt an, daß die Dauer des Startfensters der geplanten Operation unbegrenzt ist. Der Zeitplan kann bis zu seinem Verfall zu einem beliebigen Zeitpunkt nach der geplanten Startzeit ausgeführt werden. Sie können DURUNITS=INDEFINITE nur angeben, wenn Sie PERUNITS=ONETIME angeben. Der Wert INDEFINITE ist für erweiterte Zeitpläne nicht zulässig.

## MAXRUNtime

Gibt die maximale Ausführungszeit an. Hierbei handelt es sich um die Anzahl Minuten, in denen alle Clientsitzungen, die von der geplanten Operation gestartet werden, abgeschlossen werden sollten. Sind Sitzungen nach Ablauf der maximalen Ausführungszeit noch aktiv, gibt der Server eine Warnung aus, aber die Ausführung der Sitzungen wird fortgesetzt.

Tipp: Die maximale Ausführungszeit wird ab dem Beginn des Startfensters und nicht ab der Zeit berechnet, zu der Sitzungen innerhalb des Startfensters gestartet werden.

Einschränkungen:

- Der Wert des Parameters wird nicht an Server verteilt, die von einem Manager für unternehmensweite Konfiguration verwaltet werden.
- Der Wert des Parameters wird nicht mit dem Befehl EXPORT exportiert.



Der Parameter ist wahlfrei. Sie können eine Zahl im Bereich von 0 bis 1440 angeben. Der Standardwert ist 0. Der Wert 0 bedeutet, dass die maximale Ausführungszeit unendlich ist und keine Warnung ausgegeben wird. Die maximale Ausführungszeit muss größer als die Dauer des Startfensters sein, die mit den Parametern DURATION und DURUNITS definiert wird.

Ist beispielsweise die Startzeit einer geplanten Operation 21:00 Uhr und beträgt die Dauer des Startfensters 2 Stunden, erstreckt sich das Startfenster von 21:00 Uhr bis 23:00 Uhr. Beträgt die maximale Ausführungszeit 240 Minuten (4 Stunden), sollten alle Clientsitzungen für diese Operation um 1:00 Uhr abgeschlossen sein. Sind eine oder mehrere Sitzungen nach 1:00 Uhr noch aktiv, gibt der Server eine Warnung aus.

Tipp: Alternativ können Sie den Wert 1:00 Uhr für *Ausführungszeitalert* im IBM Spectrum Protect Operations Center angeben.

#### SCHEDStyle

Dieser Parameter ist wahlfrei. SCHEDSTYLE definiert entweder das Intervall zwischen den Zeiten, zu denen ein Zeitplan ausgeführt werden kann, oder die Tage, an denen der Zeitplan ausgeführt wird. Der Standardwert ist die klassische Syntax. Gültige Werte:

##### Classic

Die Parameter für die klassische (classic) Syntax sind: PERIOD, PERUNITS und DAYOFWEEK. Diese Parameter können nicht verwendet werden: MONTH, DAYOFMONTH und WEEKOFMONTH.

##### Enhanced

Die Parameter für die erweiterte (enhanced) Syntax sind: MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK. Diese Parameter können nicht verwendet werden: PERIOD und PERUNITS.

#### PERiod

Gibt den Zeitraum zwischen Startfenstern für diesen Zeitplan an. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Zulässige Werte sind ganze Zahlen von 1 bis 999. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter PERUNITS verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle fünf Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Zeitraum zwischen den Startfenstern muß länger sein als die Dauer jedes Fensters. Der Standardwert ist 1 Tag.

Dieser Wert wird ignoriert, wenn PERUNITS=ONETIME angegeben wird.

#### PERUnits

Gibt die Zeiteinheiten an, mit denen der Zeitraum zwischen Startfenstern für diesen Zeitplan bestimmt wird. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Der Standardwert ist DAYS.

Diesen Parameter zusammen mit dem Parameter PERIOD verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle 5 Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Standardwert ist 1 Tag. Sie können einen der folgenden Werte angeben:

##### Hours

Gibt an, daß der Zeitraum zwischen Startfenstern in Stunden angegeben wird.

##### Days

Gibt an, daß der Zeitraum zwischen Startfenstern in Tagen angegeben wird.

##### Weeks

Gibt an, daß der Zeitraum zwischen Startfenstern in Wochen angegeben wird.

##### Months

Gibt an, daß der Zeitraum zwischen Startfenstern in Monaten angegeben wird.

Wird PERUNITS=MONTHS angegeben, wird die geplante Operation jeden Monat an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/04/1998 lautet, wird der Zeitplan danach am 4. jedes Monats verarbeitet. Wenn das Datum jedoch für den nächsten Monat nicht gültig ist, wird die geplante Operation am letzten gültigen Datum in dem Monat verarbeitet. Danach basieren nachfolgende Operationen auf diesem neuen Datum. Wenn das Startdatum beispielsweise 03/31/1998 lautet, wird die Operation des nächsten Monats für den 04/30/1998 geplant. Danach werden alle folgenden Operationen bis Februar am 30. des Monats ausgeführt. Da Februar nur 28 Tage hat, wird die Operation für das Datum 02/28/1999 geplant. Nachfolgende Operationen werden am 28. des Monats verarbeitet.

##### Years

Gibt an, daß der Zeitraum zwischen Startfenstern für den Zeitplan in Jahren angegeben wird.

Wird PERUNITS=YEARS angegeben, wird die geplante Operation jährlich in demselben Monat und an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/29/2004 lautet, wird die geplante Operation des nächsten Jahres am 02/28/2005 ausgeführt, da Februar nur 28 Tage hat. Danach werden folgende Operationen für den 28. Februar geplant.

##### Onetime

Gibt an, daß der Zeitplan einmal verarbeitet wird. Dieser Wert überschreibt den für den Parameter PERIOD angegebenen Wert.

## DAYofweek

Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können verschiedene Optionen für den Parameter DAYofweek angeben, abhängig davon, ob die Zeitplandarstellung als 'Klassisch' oder 'Erweitert' definiert wurde:

### Klassischer Zeitplan

Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können entweder einen Tag der Woche oder WEEKDAY, WEEKEND oder ANY angeben. Fallen Startdatum und Startzeit auf einen Tag, der nicht einem angegebenen Tag entspricht, werden das Startdatum und die Startzeit in 24-Stunden-Schritten vorverlegt, bis die Angabe im Parameter DAYOFWEEK erfüllt ist.

Wird für DAYOFWEEK nicht ANY angegeben, werden die Zeitpläne, je nach Angabe für PERIOD und PERUNITS, möglicherweise nicht zum erwarteten Zeitpunkt verarbeitet. Der Standardwert ist ANY.

### Erweiterter Zeitplan

Gibt die Tage der Woche an, an denen der Zeitplan ausgeführt werden soll. Sie können entweder mehrere Tage, die durch Kommas und ohne Leerzeichen voneinander getrennt werden, oder WEEKDAY, WEEKEND oder ANY angeben. Werden mehrere Tage angegeben, wird der Zeitplan an jedem angegebenen Tag ausgeführt. Wird WEEKDAY oder WEEKEND angegeben, müssen Sie auch entweder WEEKOFMONTH=FIRST oder WEEKOFMONTH=LAST angeben, und der Zeitplan wird nur einmal pro Monat ausgeführt.

Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan an jedem Tag der Woche oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter DAYOFWEEK muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

Gültige Werte für den Parameter DAYofweek sind:

#### ANY

Das Startfenster kann an einem beliebigen Wochentag beginnen.

#### WEEKDay

Das Startfenster kann am Montag, Dienstag, Mittwoch, Donnerstag oder Freitag beginnen.

#### WEEKEnd

Das Startfenster kann am Samstag oder Sonntag beginnen.

#### Sunday

Das Startfenster beginnt am Sonntag.

#### Monday

Das Startfenster beginnt am Montag.

#### Tuesday

Das Startfenster beginnt am Dienstag.

#### Wednesday

Das Startfenster beginnt am Mittwoch.

#### Thursday

Das Startfenster beginnt am Donnerstag.

#### Friday

Das Startfenster beginnt am Freitag.

#### Saturday

Das Startfenster beginnt am Samstag.

## MONth

Gibt die Monate des Jahres an, in denen der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Geben Sie mehrere Werte an, indem Sie Kommas und keine Leerzeichen verwenden. Der Standardwert lautet ANY. Er bedeutet, dass der Zeitplan während aller Monate des Jahres ausgeführt wird.

## DAYOFMonth

Gibt den Tag des Monats an, an dem der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Sie können entweder ANY oder eine Zahl von -31 bis 31, ausschließlich Null, angeben. Ein negativer Wert gibt einen Tag an, bei dem vom Ende des Monats zurückgezählt wird. Beispiel: Der letzte Tag des Monats ist -1, der vorletzte Tag des Monats ist -2 usw. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan an jedem angegebenen Tag des Monats ausgeführt. Geben mehrere Werte denselben Tag an, wird der Zeitplan nur einmal an diesem Tag ausgeführt.

Der Standardwert ist ANY. ANY bedeutet, dass der Zeitplan an jedem Tag des Monats oder an den Tagen ausgeführt wird, die durch andere Parameter des erweiterten Zeitplans bestimmt werden. Der Parameter DAYOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFWEEK oder WEEKOFMONTH verwendet wird.

## WEEKofmonth

Gibt die Woche des Monats an, in der der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Eine Woche wird als beliebige 7-Tage-Periode betrachtet, die nicht an einem bestimmten Tag der Woche beginnt. Sie können FIRST, SECOND, THIRD, FOURTH, LAST oder ANY angeben. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan während jeder angegebenen Woche des Monats ausgeführt. Geben mehrere Werte dieselbe Woche an, wird der Zeitplan nur einmal während dieser Woche ausgeführt.

Der Standardwert ist ANY. ANY bedeutet, dass der Zeitplan während jeder Woche des Monats oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter WEEKOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

#### EXpiration

Gibt das Datum an, nach dem dieser Zeitplan nicht mehr verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NEVER. Sie können einen der folgenden Werte angeben:

#### Never

Gibt an, dass der Zeitplan nie abläuft.

#### Ablaufdatum

Gibt das Datum im Format MM/DD/YYYY an, an dem dieser Zeitplan abläuft. Wenn ein Ablaufdatum angegeben wird, läuft der Zeitplan um 23:59:59 Uhr am angegebenen Datum ab.

## Beispiel: Einen Zeitplan für eine monatliche Teilsicherung definieren

---

Den Zeitplan MONTHLY\_BACKUP definieren, der eine Teilsicherung aller zugeordneten Knoten einleitet. Als Startdatum Dienstag, den 1. Mai 2001 angeben. Dieses Datum stimmt nicht mit dem angegebenen Wochentag (Sonntag) überein. Daher beginnt das Anfangsstartfenster am ersten Sonntag nach dem 1. Mai 2001 (05/01/2001). Das Startfenster für diesen Zeitplan dauert von 01:00 bis 03:00. Dieser monatliche Zeitplan leitet Sicherungen der Dateibereiche c: und d: für alle zugeordneten Knoten ein.

```
define schedule standard monthly_backup
description="Monthly Backup of c: and d: drives"
objects="c:\* d:\*"
startdate=05/01/2001 starttime=01:00
duration=2 durunits=hours period=1
perunits=months dayofweek=sunday
```

## Beispiel: Einen Zeitplan für eine wöchentliche Teilsicherung definieren

---

Den Zeitplan WEEKLY\_BACKUP definieren, der eine Teilsicherung aller zugeordneten Knoten einleitet. Das Anfangsstartfenster für diesen Zeitplan dauert von 23:00 Uhr am Samstag, 7. Juni 1997 (06/07/1997), bis 03:00 Uhr am Sonntag, 8. Juni 1997 (06/08/1997). Nachfolgende Fenster beginnen um 23:00 Uhr an jedem Samstag. Bei der Ausführung dieses Zeitplans werden keine Nachrichten an den Clientknoten zurückgegeben.

```
define schedule employee_records weekly_backup
startdate=06/07/1997 starttime=23:00 duration=4
durunits=hours perunits=weeks
dayofweek=saturday options=-quiet
```

## Beispiel: Einen Zeitplan definieren, mit dem ein bestimmtes Verzeichnis vierteljährlich archiviert wird

---

Einen Zeitplan definieren, der bestimmte Dateien vierteljährlich am letzten Freitag des Monats archiviert.

```
define schedule employee_records quarterly_archive
starttime=20:00 action=archive
object=/home/employee/records/*
duration=1 durunits=hour schedstyle=enhanced
month=mar,jun,sep,dec weekofmonth=last dayofweek=fri
```

## DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)

---

Mit dem Befehl DEFINE SCHEDULE kann ein neuer Zeitplan für die Verarbeitung eines Verwaltungsbefehls erstellt werden.

In den Zeitplan eines Verwaltungsbefehls können Prozeduren eingeschlossen werden, so dass die Befehle automatisch verarbeitet werden.

Anmerkung:

1. Der Befehl MACRO und der Befehl QUERY ACTLOG können nicht geplant werden.

2. Wenn Sie einen Befehl planen, der den Parameter WAIT angibt, muss der Parameter auf YES gesetzt werden, damit der Prozess für die Sitzung, die ihn gestartet hat, einen Rückkehrcode zur Verfügung stellen kann. Weitere Informationen zum Parameter WAIT befinden sich in Serverbefehlsverarbeitung.

## Berechtigungsklasse

---

Zum Definieren eines Zeitplans für Verwaltungsbefehle ist die Systemberechtigung erforderlich.

## Syntax

---

Klassischer Verwaltungszeitplan

```
>>-DEFine SChedule--Zeitplanname--+-+-----+-----+----->
                                     '-Type-----Administrative-'
                                     .-ACTIVE-----No--.
>--CMD-----Befehl--+-+-----+-----+----->
                                     '-ACTIVE-----Yes-'
                                     .-PRiority-----5----.
>+-----+-----+-----+-----+-----+-----+----->
   '-DESCription-----Beschreibung-' '-PRiority-----Zahl-'
   .-STARTDate-----aktuelles_Datum-.
>+-----+-----+-----+-----+-----+-----+----->
   '-STARTDate-----Datum-----'
   .-STARTTime-----aktuelle_Zeit-. .-DURation-----1----.
>+-----+-----+-----+-----+-----+-----+----->
   '-STARTTime-----Zeit-----' '-DURation-----Zahl-'
   .-DURUnits-----Hours----- .-MAXRUNtime-----0-----.
>+-----+-----+-----+-----+-----+-----+----->
   '-DURUnits-----+Minutes-----+' '-MAXRUNtime-----Anzahl-'
                                     +-Hours-----+
                                     +-Days-----+
                                     '-INDefinite-'
   .-SCHEDStyle-----Classic-. .-PERiod-----1----.
>+-----+-----+-----+-----+-----+-----+----->
   '-SCHEDStyle-----Classic-' '-PERiod-----Zahl-'
   .-PERUnits-----Days----- .
>+-----+-----+-----+-----+-----+-----+----->
   '-PERUnits-----+Hours-----+'
                                     +-Days-----+
                                     +-Weeks-----+
                                     +-Months-----+
                                     +-Years-----+
                                     '-Onetime-'
   .-DAYofweek-----ANY----- .
>+-----+-----+-----+-----+-----+-----+----->
   '-DAYofweek-----+ANY-----+'
                                     +-WEEKDay---+
                                     +-WEEKEnd---+
                                     +-SUNday---+
                                     +-MONday---+
                                     +-TUESday---+
                                     +-WEDnesday--+
                                     +-THURsday--+
                                     +-FRIday---+
                                     '-SATurday--'
   .-EXPIration-----Never----- .
>+-----+-----+-----+-----+-----+-----+-----><
   '-EXPIration-----+Never--+-'
                                     '-Datum-'
```

## Syntax

---

Erweiterter Verwaltungszeitplan

```

>>-DEFine SChedule--Zeitplanname--+-----+----->
                        '-Type-----Administrative-'

                        .-ACTIVE-----NO-.
>--CMD-----Befehl--+-----+----->
                        '-ACTIVE-----YES-'

                        .-PRiority-----5----.
>+-----+-----+-----+----->
  '-DESCription-----Beschreibung-'  '-PRiority-----Zahl-'

  .-STARTDate-----aktuelles_Datum-.
>+-----+-----+-----+----->
  '-STARTDate-----Datum-----'

  .-STARTTime-----aktuelle_Zeit-.  .-DURation-----1----.
>+-----+-----+-----+----->
  '-STARTTime-----Zeit-----'  '-DURation-----Zahl-'

  .-DURUnits-----Hours-----  .-MAXRUNtime-----0-----.
>+-----+-----+-----+----->
  '-DURUnits-----+Minutes-+-'  '-MAXRUNtime-----Anzahl-'
                        +-Hours-+-
                        '-Days-----'

                        .-MONth-----ANY------.
>--SCHEDStyle-----Enhanced--+-----+----->
                        '-MONth-----+ANY-----+'
                                +-January-+-
                                +-February-+-
                                +-MARch-----+
                                +-APRil-----+
                                +-May-----+
                                +-JUNE-----+
                                +-JULy-----+
                                +-AUGust----+
                                +-September-+
                                +-October---+
                                +-November--+
                                '-December--'

  .-DAYOFMonth-----ANY-----  .-WEEKofmonth-----ANY------.
>+-----+-----+-----+----->
  '-DAYOFMonth-----+ANY-+-'  '-WEEKofmonth-----+ANY-----+'
                        '-Day-'
                                +-First-+-
                                +-Second-+
                                +-Third-+-
                                +-FOurth-+
                                '-Last---'

  .-DAYofweek-----ANY------.
>+-----+-----+-----+----->
  '-DAYofweek-----+ANY-----+'
                        +-WEEKDay-+-
                        +-WEEKEnd-+-
                        +-Sunday-+-
                        +-Monday-+-
                        +-TUESday-+-
                        +-Wednesday-+
                        +-THursday-+-
                        +-Friday-+-
                        '-SATurday--'

  .-EXPIration-----Never-----.
>+-----+-----+-----+-----><
  '-EXPIration-----+Never-+-'
                        '-Datum-'

```

## Parameter

Zeitplanname (Erforderlich)

Gibt den Namen des Zeitplans an, der definiert werden soll. Für den Namen können bis zu 30 Zeichen angegeben werden.

Type=Administrative

Gibt an, daß ein Zeitplan für einen Verwaltungsbefehl definiert wird. Dieser Parameter ist wahlfrei. Ein Verwaltungsbefehl wird angenommen, wenn der Parameter CMD angegeben wird.

**CMD** (Erforderlich)

Gibt den Verwaltungsbefehl an, der für die Verarbeitung geplant werden soll. Die maximale Länge des Befehls beträgt 512 Zeichen. Den Verwaltungsbefehl in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

Einschränkung: Es können keine Umleitungszeichen mit diesem Parameter angegeben werden.

**ACTIVE**

Gibt an, ob IBM Spectrum Protect einen Zeitplan für einen Verwaltungsbefehl verarbeitet, wenn das Startfenster erscheint. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Der Zeitplan für den Verwaltungsbefehl muß mit dem Befehl UPDATE SCHEDULE in den aktiven Status versetzt werden, damit IBM Spectrum Protect den Zeitplan verarbeiten kann. Gültige Werte:

**YES**

Gibt an, daß IBM Spectrum Protect einen Zeitplan für den Verwaltungsbefehl verarbeitet, wenn das Startfenster beginnt.

**NO**

Gibt an, daß IBM Spectrum Protect keinen Zeitplan für den Verwaltungsbefehl verarbeitet, wenn das Startfenster beginnt.

**DESCRIPTION**

Gibt eine Beschreibung des Zeitplans an. Dieser Parameter ist wahlfrei. Für die Beschreibung können bis zu 255 Zeichen angegeben werden. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

**PRIORITY**

Gibt den Prioritätswert für einen Zeitplan an. Dieser Parameter ist wahlfrei. Zulässige Werte sind ganze Zahlen von 1 bis 10, wobei 1 die höchste Priorität und 10 die niedrigste Priorität angibt. Der Standardwert ist 5.

Wenn zwei oder mehr Zeitpläne dieselbe Fensterstartzeit haben, legt der angegebene Wert fest, wann IBM Spectrum Protect den Zeitplan verarbeitet. Der Zeitplan mit der höchsten Priorität startet zuerst. Ein Zeitplan mit PRIORITY=3 startet beispielsweise vor einem Zeitplan mit PRIORITY=5.

**STARTDATE**

Gibt das Datum für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum. Diesen Parameter zusammen mit dem Parameter STARTTIME verwenden, um anzugeben, wann das Anfangsstartfenster des Zeitplans startet.

Sie können das Datum unter Verwendung der folgenden Werte angeben:

| Wert                            | Beschreibung  | Beispiel   |
|---------------------------------|---|--|
| MM/TT/JJJJ                      | Ein bestimmtes Datum  | 09/15/1998   |
| TODAY                           | Das aktuelle Datum  | TODAY  |
| TODAY+Tage <b>oder</b><br>+Tage | Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY +3 <b>oder</b> +3.   |
| EOLM (Ende des letzten Monats)  | Der letzte Tag des Vormonats.   | EOLM   |
| EOLM-Tage                       | Der letzte Tag des Vormonats minus angegebene Tage.   | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)     | Der erste Tag des aktuellen Monats.   | BOTM   |
| BOTM+Tage                       | Der erste Tag des aktuellen Monats plus angegebene Tage.  | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

**STARTTIME**

Gibt die Uhrzeit für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist die aktuelle Uhrzeit. Dieser Parameter gibt in Verbindung mit dem Parameter STARTDATE den Beginn des Anfangsstartfensters an.

Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

| Wert     | Beschreibung           | Beispiel |
|----------|------------------------|----------|
| HH:MM:SS | Eine bestimmte Uhrzeit | 10:30:08 |
| NOW      | Die aktuelle Uhrzeit   | NOW      |

| Wert                             | Beschreibung   | Beispiel   |
|----------------------------------|--|--|
| NOW+HH:MM <b>oder</b><br>+HH:MM  | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten  | NOW+02:00 <b>oder</b> +02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW+02:00 oder STARTTIME=+02:00 ausgegeben, beginnt das Startfenster um 7:00 Uhr. |
| NOW-HH:MM <b>oder</b> -<br>HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten | NOW-02:00 <b>oder</b> -02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW-02:00 oder STARTTIME=-02:00 ausgegeben, beginnt das Startfenster um 3:00 Uhr. |

#### DURation

Gibt die Anzahl Einheiten an, die die Länge des Startfensters der geplanten Operation definiert. Dieser Parameter ist wahlfrei. Dieser Wert muß zwischen 1 und 999 liegen. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter DURUNITS verwenden, um die Länge des Startfensters anzugeben. Werden beispielsweise DURATION=20 und DURUNITS=MINUTES angegeben, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Standardlänge des Startfensters beträgt 1 Stunde. Die Länge des Fensters muß kürzer sein, als der Zeitraum zwischen Fenstern.

Dieser Wert wird ignoriert, wenn DURUNITS=INDEFINITE angegeben wird.

#### DURUnits

Gibt die Zeiteinheiten an, mit denen die Dauer des Fensters bestimmt wird, in dem der Zeitplan starten kann. Dieser Parameter ist wahlfrei. Der Standardwert ist HOURS.

Diesen Parameter zusammen mit dem Parameter DURATION verwenden, um anzugeben, wie lange das Startfenster geöffnet bleibt, um den Zeitplan zu verarbeiten. Gilt beispielsweise DURATION=20 und DURUNITS=MINUTES, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Verarbeitung des Zeitplans muß nicht unbedingt innerhalb dieses Fensters enden. Wenn der Zeitplan aus irgendeinem Grund wiederholt werden muß, müssen die Wiederholungsversuche vor Ablauf des Startfensters beginnen; andernfalls wird die Operation nicht erneut gestartet.

Der Standardwert für die Länge des Startfensters ist 1 Stunde. Sie können einen der folgenden Werte angeben:

##### Minutes

Gibt an, daß die Dauer des Fensters in Minuten definiert wird.

##### Hours

Gibt an, daß die Dauer des Fensters in Stunden definiert wird.

##### Days

Gibt an, daß die Dauer des Fensters in Tagen definiert wird.

##### INDefinite

Gibt an, daß die Dauer des Startfensters der geplanten Operation unbegrenzt ist. Der Zeitplan kann bis zu seinem Verfall zu einem beliebigen Zeitpunkt nach der geplanten Startzeit ausgeführt werden. Sie können DURUNITS=INDEFINITE nur angeben, wenn Sie PERUNITS=ONETIME angeben. Der Wert INDEFINITE ist für erweiterte Zeitpläne nicht zulässig.

#### MAXRUNtime

Gibt die maximale Ausführungszeit an. Hierbei handelt es sich um die Anzahl Minuten, in denen Serverprozesse, die von geplanten Befehlen gestartet werden, abgeschlossen werden müssen. Sind Prozesse nach Ablauf der maximalen Ausführungszeit noch aktiv, werden die Prozesse von der zentralen Zeitplanung abgebrochen.

##### Tipps:

- Möglicherweise werden die Prozesse nicht sofort beendet, wenn sie von der zentralen Zeitplanung abgebrochen werden. Sie werden beendet, wenn sie die Benachrichtigung über den Abbruch von der zentralen Zeitplanung registrieren.
- Die maximale Ausführungszeit wird ab dem Zeitpunkt berechnet, an dem der Serverprozess startet. Wenn mit dem Befehl für den Zeitplan mehr als ein Prozess gestartet wird, wird die maximale Ausführungszeit für jeden Prozess ab dem Zeitpunkt berechnet, an dem der jeweilige Prozess startet.
- Dieser Parameter gilt nicht für einige Prozesse, wie z. B. Prozesse zum Identifizieren doppelter Daten, deren Ausführung nach Ablauf der maximalen Ausführungszeit fortgesetzt werden kann.
- Dieser Parameter gilt nicht, wenn der geplante Befehl keinen Serverprozess startet.
- Einigen Befehlen kann eine andere Abbruchzeit zugeordnet werden. Beispielsweise kann der Befehl MIGRATE STGPOOL einen Parameter einschließen, der die Länge der Zeit angibt, die die Speicherpoolumlagerung ausgeführt wird, bevor die Umlagerung automatisch abgebrochen wird. Wenn Sie einen Befehl planen, für den eine Abbruchzeit definiert ist, und Sie außerdem eine maximale Ausführungszeit für den Zeitplan definieren, werden die Prozesse zu der Abbruchzeit abgebrochen, die zuerst erreicht wird.

Einschränkungen:

- Der Wert des Parameters wird nicht an Server verteilt, die von einem Manager für unternehmensweite Konfiguration verwaltet werden.
- Der Wert des Parameters wird nicht mit dem Befehl EXPORT exportiert.

Der Parameter ist wahlfrei. Sie können eine Zahl im Bereich von 0 bis 1440 angeben. Der Standardwert ist 0. Der Wert 0 bedeutet, dass die maximale Ausführungszeit unendlich ist und die zentrale Zeitplanung keine Prozesse abbricht. Die maximale Ausführungszeit muss größer als die Dauer des Startfensters sein, die mit den Parametern DURATION und DURUNITS definiert wird.

Ist beispielsweise die Startzeit eines geplanten Befehls 21:00 Uhr und beträgt die Dauer des Startfensters 2 Stunden, erstreckt sich das Startfenster von 21:00 Uhr bis 23:00 Uhr. Beträgt die maximale Ausführungszeit 240 Minuten (4 Stunden), müssen alle zutreffenden Serverprozesse, die von dem Befehl gestartet werden, um 1:00 Uhr abgeschlossen sein. Sind ein oder mehrere zutreffende Prozesse nach 1:00 Uhr noch aktiv, werden die Prozesse von der zentralen Zeitplanung abgebrochen.  
Tipp: Alternativ können Sie eine *Endzeit* von 1:00 Uhr im IBM Spectrum Protect Operations Center angeben.

#### SCHEDStyle

Dieser Parameter ist wahlfrei. SCHEDSTYLE definiert entweder das Intervall zwischen den Zeiten, zu denen ein Zeitplan ausgeführt werden soll, oder die Tage, an denen der Zeitplan ausgeführt werden soll. Die Darstellung kann entweder classic oder enhanced sein. Der Standardwert ist die klassische Syntax.

Für klassische Zeitpläne sind diese Parameter zulässig: PERIOD, PERUNITS und DAYOFWEEK. Für klassische Zeitpläne nicht zulässig sind: MONTH, DAYOFMONTH und WEEKOFMONTH.

Für erweiterte Zeitpläne sind diese Parameter zulässig: MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK. Diese Parameter sind nicht zulässig: PERIOD und PERUNITS.

#### PERiod

Gibt den Zeitraum zwischen Startfenstern für diesen Zeitplan an. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Zulässige Werte sind ganze Zahlen von 1 bis 999. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter PERUNITS verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle fünf Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Zeitraum zwischen den Startfenstern muß länger sein als die Dauer jedes Fensters. Der Standardwert ist 1 Tag.

Dieser Wert wird ignoriert, wenn PERUNITS=ONETIME angegeben wird.

#### PERUnits

Gibt die Zeiteinheiten an, mit denen der Zeitraum zwischen Startfenstern für diesen Zeitplan bestimmt wird. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Der Standardwert ist DAYS.

Diesen Parameter zusammen mit dem Parameter PERIOD verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle 5 Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Standardwert ist 1 Tag. Sie können einen der folgenden Werte angeben:

##### Hours

Gibt an, daß der Zeitraum zwischen Startfenstern in Stunden angegeben wird.

##### Days

Gibt an, daß der Zeitraum zwischen Startfenstern in Tagen angegeben wird.

##### Weeks

Gibt an, daß der Zeitraum zwischen Startfenstern in Wochen angegeben wird.

##### Months

Gibt an, daß der Zeitraum zwischen Startfenstern in Monaten angegeben wird.

Wird PERUNITS=MONTHS angegeben, wird die geplante Operation jeden Monat an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/04/1998 lautet, wird der Zeitplan danach am 4. jedes Monats verarbeitet. Wenn das Datum jedoch für den nächsten Monat nicht gültig ist, wird die geplante Operation am letzten gültigen Datum in dem Monat verarbeitet. Danach basieren nachfolgende Operationen auf diesem neuen Datum. Wenn das Startdatum beispielsweise 03/31/1998 lautet, wird die Operation des nächsten Monats für den 04/30/1998 geplant. Danach werden alle folgenden Operationen bis Februar am 30. des Monats ausgeführt. Da Februar nur 28 Tage hat, wird die Operation für das Datum 02/28/1999 geplant. Nachfolgende Operationen werden am 28. des Monats verarbeitet.

##### Years

Gibt an, daß der Zeitraum zwischen Startfenstern für den Zeitplan in Jahren angegeben wird.

Wird PERUNITS=YEARS angegeben, wird die geplante Operation jährlich in demselben Monat und an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/29/2004 lautet, wird die geplante Operation des nächsten Jahres am 02/28/2005 ausgeführt, da Februar nur 28 Tage hat. Danach werden folgende Operationen für den 28. Februar geplant.



#### Onetime

Gibt an, daß der Zeitplan einmal verarbeitet wird. Dieser Wert überschreibt den für den Parameter PERIOD angegebenen Wert.

#### DAYofweek

Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können verschiedene Optionen für den Parameter DAYofweek angeben, abhängig davon, ob die Zeitplandarstellung als 'Klassisch' oder 'Erweitert' definiert wurde:

##### Klassischer Zeitplan

Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können entweder einen Tag der Woche oder WEEKDAY, WEEKEND oder ANY angeben. Fallen Startdatum und Startzeit auf einen Tag, der nicht einem angegebenen Tag entspricht, werden das Startdatum und die Startzeit in 24-Stunden-Schritten vorverlegt, bis die Angabe im Parameter DAYOFWEEK erfüllt ist.

Wird für DAYOFWEEK nicht ANY angegeben, werden die Zeitpläne, je nach Angabe für PERIOD und PERUNITS, möglicherweise nicht zum erwarteten Zeitpunkt verarbeitet. Der Standardwert ist ANY.

##### Erweiterter Zeitplan

Gibt die Tage der Woche an, an denen der Zeitplan ausgeführt werden soll. Sie können entweder mehrere Tage, die durch Kommas und ohne Leerzeichen voneinander getrennt werden, oder WEEKDAY, WEEKEND oder ANY angeben. Werden mehrere Tage angegeben, wird der Zeitplan an jedem angegebenen Tag ausgeführt. Wird WEEKDAY oder WEEKEND angegeben, müssen Sie auch entweder WEEKOFMONTH=FIRST oder WEEKOFMONTH=LAST angeben, und der Zeitplan wird nur einmal pro Monat ausgeführt.

Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan an jedem Tag der Woche oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter DAYOFWEEK muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

Gültige Werte für den Parameter DAYofweek sind:

##### ANY

Das Startfenster kann an einem beliebigen Wochentag beginnen.

##### WEEKDay

Das Startfenster kann am Montag, Dienstag, Mittwoch, Donnerstag oder Freitag beginnen.

##### WEEKEnd

Das Startfenster kann am Samstag oder Sonntag beginnen.

##### SUNday

Das Startfenster beginnt am Sonntag.

##### Monday

Das Startfenster beginnt am Montag.

##### TUesday

Das Startfenster beginnt am Dienstag.

##### Wednesday

Das Startfenster beginnt am Mittwoch.

##### THursday

Das Startfenster beginnt am Donnerstag.

##### Friday

Das Startfenster beginnt am Freitag.

##### SATurday

Das Startfenster beginnt am Samstag.

#### MONTH

Gibt die Monate des Jahres an, in denen der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Geben Sie mehrere Werte an, indem Sie Kommas und keine Leerzeichen verwenden. Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan in jedem Monat des Jahres ausgeführt wird.

#### DAYOFMonth

Gibt den Tag des Monats an, an dem der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Sie können entweder ANY oder eine Zahl von -31 bis 31, ausschließlich Null, angeben. Ein negativer Wert gibt einen Tag an, bei dem vom Ende des Monats zurückgezählt wird. Beispiel: Der letzte Tag des Monats ist -1, der vorletzte Tag des Monats ist -2 usw. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan an jedem angegebenen Tag des Monats ausgeführt. Geben mehrere Werte denselben Tag an, wird der Zeitplan nur einmal an diesem Tag ausgeführt.

Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan an jedem Tag des Monats oder an den Tagen ausgeführt wird, die durch andere Parameter des erweiterten Zeitplans bestimmt werden. Der Parameter DAYOFMONTH muss den Wert ANY

haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFWEEK oder WEEKOFMONTH verwendet wird.

#### WEEKofmonth

Gibt die Woche des Monats an, in der der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Eine Woche wird als beliebige 7-Tage-Periode betrachtet, die nicht an einem bestimmten Tag der Woche beginnt. Sie können FIRST, SECOND, THIRD, FOURTH, LAST oder ANY angeben. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan während jeder angegebenen Woche des Monats ausgeführt. Geben mehrere Werte dieselbe Woche an, wird der Zeitplan nur einmal während dieser Woche ausgeführt.

Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan während jeder Woche des Monats oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter WEEKOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

#### EXpiration

Gibt das Datum an, nach dem dieser Zeitplan nicht mehr verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NEVER. Sie können einen der folgenden Werte angeben:

##### Never

Gibt an, dass der Zeitplan nie abläuft.

##### Ablaufdatum

Gibt das Datum im Format MM/DD/YYYY an, an dem dieser Zeitplan abläuft. Wenn ein Ablaufdatum angegeben wird, läuft der Zeitplan um 23:59:59 Uhr am angegebenen Datum ab.

## Beispiel: Einen Zeitplan definieren, um den primären Speicherpool alle zwei Tage zu sichern

---

Den Zeitplan BACKUP\_ARCHIVEPOOL definieren, der den primären Speicherpool ARCHIVEPOOL im Kopienspeicherpool RECOVERYPOOL sichert. Die Sicherung wird um 20:00 Uhr an jedem zweiten Tag ausgeführt.

```
define schedule backup_archivepool type=administrative
cmd="backup stgpool archivepool recoverypool"
active=yes starttime=20:00 period=2
```

## Beispiel: Einen Zeitplan definieren, um den primären Speicherpool zweimal im Monat zu sichern

---

Den Zeitplan BACKUP\_ARCHIVEPOOL definieren, der den primären Speicherpool ARCHIVEPOOL im Kopienspeicherpool RECOVERYPOOL sichert. Einen erweiterten Zeitplan auswählen und den Zeitplan am ersten und fünfzehnten Tag des Monats ausführen.

```
define schedule backup_archivepool type=administrative
cmd="backup stgpool archivepool recoverypool"
schedstyle=enhanced dayofmonth=1,15
```

## DEFINE SCRATCHPADENTRY (Scratchpadeintrag definieren)

---

Mit diesem Befehl können Sie Daten in einer neuen Zeile im Scratchpad eingeben. Das Scratchpad ist eine Datenbanktabelle, die sich auf dem Server befindet. Das Scratchpad ermöglicht es Ihnen, verschiedene Informationen in Tabellenformat zu speichern.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-DEFine SCRATCHPadentry--übergeordnete_Kategorie----->
>--untergeordnete_Kategorie--Betreff--Line ---Nummer----->
>--Data----Daten-----><
```

## Parameter

---

übergeordnete\_Kategorie (Erforderlich)

Gibt die übergeordnete Kategorie an, in der Daten gespeichert werden sollen. Geben Sie eine Textzeichenfolge aus bis zu 100 alphanumerischen Zeichen ein. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

untergeordnete\_Kategorie (Erforderlich)

Gibt die untergeordnete Kategorie an, in der Daten gespeichert werden sollen. Untergeordnete Kategorien sind Abschnitte in übergeordneten Kategorien. Geben Sie eine Textzeichenfolge aus bis zu 100 alphanumerischen Zeichen ein. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

Betreff (Erforderlich)

Gibt den Betreff an, unter dem Daten gespeichert werden sollen. Betreffs sind Abschnitte in untergeordneten Kategorien. Geben Sie eine Textzeichenfolge aus bis zu 100 alphanumerischen Zeichen ein. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

Line (Erforderlich)

Gibt die Nummer der Zeile an, in der Daten gespeichert werden sollen. Zeilen sind Abschnitte in Betreffs. Geben Sie eine ganze Zahl im Bereich von 1 bis 1000 an.

Data (Erforderlich)

Gibt die Daten an, die in der Zeile gespeichert werden sollen. Sie können bis zu 1000 Zeichen eingeben. Schließen Sie die Daten in Anführungszeichen ein, wenn die Daten ein oder mehrere Leerzeichen enthalten. Bei den Daten muss die Groß-/Kleinschreibung beachtet werden.

## Beispiel: Scratchpadeintrag definieren

Geben Sie die Abwesenheitsdaten eines Administrators, Jane, in eine Tabelle ein, in der Informationen zu den Standorten aller Administratoren gespeichert sind.

```
define scratchpentry admin_info location jane line=2 data="Nicht im Büro 1.-15.11."
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE SCRATCHPADENTRY

| Befehl                  | Beschreibung  |
|-------------------------|---|
| DELETE SCRATCHPADENTRY  | Löscht eine Zeile mit Daten aus dem Scratchpad.                 |
| QUERY SCRATCHPADENTRY   | Zeigt Informationen an, die im Scratchpad enthalten sind.       |
| SET SCRATCHPADRETENTION | Gibt den Zeitraum an, den Scratchpadeinträge aufbewahrt werden. |
| UPDATE SCRATCHPADENTRY  | Aktualisiert Daten in einer Zeile im Scratchpad.                |

## DEFINE SCRIPT (IBM Spectrum Protect-Prozedur definieren)

Mit diesem Befehl kann eine IBM Spectrum Protect-Prozedur definiert oder eine neue IBM Spectrum Protect-Prozedur unter Verwendung des Inhalts aus einer anderen Prozedur erstellt werden.

Mit diesem Befehl kann die erste Zeile für die Prozedur definiert werden. Sollen der Prozedur weitere Zeilen hinzugefügt werden, den Befehl UPDATE SCRIPT verwenden.

Tipps:

- Werden Befehle innerhalb von Prozeduren weitergeleitet, den Server oder die Server-Gruppe in runde Klammern einschließen und den Doppelpunkt übergehen. Enthält die Syntax einen Doppelpunkt, wird der Befehl bei Ausgabe des Befehls RUN nicht weitergeleitet. Stattdessen wird der Befehl nur auf dem Server ausgeführt, von dem aus der Befehl RUN ausgegeben wird.
- Die Ausgabe eines Befehls innerhalb einer IBM Spectrum Protect-Prozedur kann nicht umgeleitet werden. Führen Sie stattdessen die Prozedur aus und geben Sie dann die Befehlsumleitung an. Soll beispielsweise die Ausgabe von script1 in das Verzeichnis c:\temp\test.out übertragen werden, führen Sie wie im folgenden Beispiel die Prozedur aus und geben Sie die Befehlsumleitung an:

```
run script1 > c:\temp\test.out
```

## Berechtigungsklasse

Für diesen Befehl ist die Bediener-, Maßnahmen-, Speicher- oder Systemberechtigung erforderlich.

## Syntax

```

>>-DEFine SCRipt--Prozedurname----->
      .-Line---001----.
>--+Befehlszeile--+-----+----->
|          '-Line ---Nummer-' |
| '-File---Dateiname-----' |
>--+-----+-----<
| '-DESCription---Beschreibung-'

```

## Parameter

---

### Prozedurname (Erforderlich)

Gibt den Namen der Prozedur an, die definiert werden soll. Für den Namen können bis zu 30 Zeichen angegeben werden.

### Befehlszeile

Gibt den ersten Befehl an, der in einer Prozedur verarbeitet werden soll. Sie müssen entweder diesen Parameter (und wahlweise den Parameter LINE) oder den Parameter FILE angeben.

Der angegebene Befehl kann Substitutionsvariablen enthalten und über mehrere Zeilen fortgesetzt werden, wenn als letztes Zeichen in dem Befehl ein Fortsetzungszeichen (-) angegeben wird. Substitutionsvariablen werden mit dem Zeichen '\$' gefolgt von einer Zahl angegeben, die den Wert des Parameters angibt, wenn die Prozedur verarbeitet wird. Für die Befehlszeile können bis zu 1200 Zeichen angegeben werden. Den Befehl in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

Sie können Befehle seriell, parallel oder seriell und parallel auszuführen, indem Sie den Prozedurbefehl SERIAL oder PARALLEL für den Parameter Befehlszeile angeben. Sie können mehrere Befehle parallel ausführen und auf deren Beendigung warten, bevor Sie mit dem nächsten Befehl fortfahren. Befehle werden seriell ausgeführt, bis der parallele Befehl gefunden wird.

Ablaufanweisungen mit bedingter Logik können verwendet werden. Diese Anweisungen schließen IF, EXIT und GOTO ein.

### Line

Gibt die Zeilennummer für die Befehlszeile an. Da Befehle in mehreren Zeilen angegeben werden, wird anhand von Zeilennummern die Reihenfolge der Verarbeitung bestimmt, wenn die Prozedur ausgeführt wird. Die erste Zeile oder Zeile 001 ist der Standardwert. Dieser Parameter ist wahlfrei.

### File

Gibt den Namen der Datei an, deren Inhalt in die Prozedur gelesen wird, die definiert werden soll. Die Datei muss sich auf dem Server befinden, auf dem dieser Befehl ausgeführt wird. Wird der Parameter FILE angegeben, kann keine Befehlszeile oder Zeilennummer angegeben werden.

Eine Prozedur kann erstellt werden, indem eine andere Prozedur abgefragt wird und die Parameter FORMAT=RAW und OUTPUTFILE angegeben werden. Die Ausgabe von der Abfrage der Prozedur wird an eine Datei geleitet, die mit dem Parameter OUTPUTFILE angegeben wird. Zum Erstellen der neuen Prozedur wird der Inhalt der zu definierenden Prozedur aus der mit dem Parameter OUTPUTFILE angegebenen Datei eingelesen.

### DESCription

Gibt eine Beschreibung für die Prozedur an. Für die Beschreibung können bis zu 255 Zeichen angegeben werden. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Dieser Parameter ist wahlfrei.

## Beispiel: Eine Prozedur schreiben, um AIX-Clients anzuzeigen

---

Eine Prozedur definieren, die alle AIX-Clients anzeigt.

```

define script qaixc "select node_name from nodes where platform_name='AIX'"
desc='Display aix clients'

```

## Beispiel: Eine Prozedur schreiben und ausführen, um einen Befehl an eine Servergruppe weiterzuleiten

---

Eine Prozedur definieren und ausführen, die den Befehl QUERY STGPOOL an eine Servergruppe mit dem Namen DEV\_GROUP weiterleitet.

```

define script qu_stg "(dev_group) query stgpool"
run qu_stg

```

## Beispiel: Eine Prozedur aus einer vorhandenen Prozedur erstellen

---

Eine Prozedur definieren, deren Befehlszeilen aus einer Datei mit dem Namen MY.SCRIPT gelesen werden, und der neuen Prozedur den Namen AGADM zuordnen. Die Datei muss sich auf dem Server befinden und vom Server gelesen werden.

```
define script agadm file=my.script
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE SCRIPT

| Befehl        | Beschreibung  |
|---------------|---|
| COPY SCRIPT   | Erstellt eine Kopie einer Prozedur.                           |
| DELETE SCRIPT | Löscht eine Prozedur oder einzelne Zeilen aus einer Prozedur. |
| QUERY SCRIPT  | Zeigt Informationen über Prozeduren an.                       |
| RENAME SCRIPT | Vergibt einen neuen Namen für eine Prozedur.                  |
| RUN           | Führt ein Script aus.   |
| UPDATE SCRIPT | Ändert Zeilen oder fügt Zeilen in einer Prozedur hinzu.       |

### Zugehörige Konzepte:

Logikablaufanweisungen in einem Script verwenden

### Zugehörige Tasks:

Server-Script definieren

Befehle parallel oder seriell ausführen

Tasks gleichzeitig auf mehreren Servern ausführen

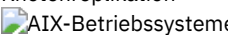

### Zugehörige Verweise:

Rückkehrcodes für die Verwendung in IBM Spectrum Protect-Scripts

## DEFINE SERVER (Server für Übertragung zwischen Servern definieren)

Verwenden Sie diesen Befehl, um einen Server für die Verwendung von Funktionen, wie z. B. virtuelle Datenträger, Knotenreplikation, Befehlsweiterleitung und LAN-unabhängige Datenversetzung, zu definieren.

Mit diesem Befehl kann ein Server für die folgenden Funktionen definiert werden:

- Unternehmensweite Konfiguration
- Unternehmensweite Ereignisprotokollierung
- Befehlsweiterleitung
- Virtuelle Datenträger
- LAN-unabhängige Datenversetzung
- Knotenreplikation
-  AIX-Betriebssysteme  Linux-Betriebssysteme Datenversetzung mit dem z/OS Media-Server
- Statusüberwachung von fernen Servern
- Alertüberwachung von fernen Servern
- Export zwischen Servern

Wenn Sie einen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden, müssen alle Zielsever für LDAP-authentifizierte Kennwörter konfiguriert werden. Auf Daten, die von einem Knoten repliziert werden, der sich mit einem LDAP-Verzeichnisserver authentifiziert, kann nicht zugegriffen werden, wenn der Zielreplikationsserver nicht korrekt konfiguriert ist. Ist Ihr Zielreplikationsserver nicht konfiguriert, können replizierte Daten von einem LDAP-Knoten auf dem Zielsever gespeichert werden. Der Zielreplikationsserver muss jedoch für die Verwendung von LDAP konfiguriert werden, wenn Sie auf die Daten zugreifen möchten.

Die Verwendung von virtuellen Datenträgern wird nicht unterstützt, wenn sich der Quellenserver und der Zielsever auf demselben IBM Spectrum Protect-Server befinden.

Dieser Befehl wird auch verwendet, um einen IBM Spectrum Protect-Speicheragenten zu definieren, als sei er ein Server.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

Für:

- Befehlsweiterleitung

- Statusüberwachung von fernen Servern
- Alertüberwachung von fernen Servern
- Export zwischen Servern



Tipp: Die Befehlsweiterleitung verwendet die ID und das Kennwort des Administrators, der den Befehl ausgibt.

```
>>-DEFine--SERver--Servername--HLAddress--IP-Adresse----->
>--LLAddress--TCP-Anschluss--+-----+----->
      '-COMMmethod--TCPIP-'
>+-----+-----+-----+----->
  '-URL--URL-'   '-DESCription--Beschreibung-'
  .-SSL--No-----
>+-----+-----+-----+----->
  '-SSL--+-No--+'
      '-Yes-'

  .-SESSIONSECurity--TRANSitional----
>+-----+-----+-----+----->
  '-SESSIONSECurity--+-STRict-----+'
      '-TRANSitional-'
```

## Syntax

Für:

- Unternehmensweite Konfiguration
- Unternehmensweite Ereignisprotokollierung
- Speicheragent
- Quellen- und Zielserver für Knotenreplikation
-  AIX-Betriebssysteme  Linux-Betriebssysteme/OS Media-Server


```
>>-DEFine--SERver--Servername--SERVERPAssword--Kennwort----->
>--HLAddress--IP-Adresse--LLAddress--TCP-Anschluss----->
>+-----+-----+-----+----->
  '-COMMmethod--TCPIP-'   '-URL--URL-'
>+-----+-----+-----+----->
  '-DESCription--Beschreibung-'
      (1)
  .-CROSSDEFine--No----- (2)
>+-----+-----+-----+----->
  '-CROSSDEFine--+-No--+'
      '-Yes-'

  .-VALIdateprotocol--No----- .-SSL--No-----
>+-----+-----+-----+----->
  '-VALIdateprotocol--+-No--+'   '-SSL--+-No--+'
      '-All-'   '-Yes-'

  .-SESSIONSECurity--TRANSitional----
>+-----+-----+-----+----->
  '-SESSIONSECurity--+-STRict-----+'
      '-TRANSitional-'

  .-TRANSFERMethod--Tcpi-----
>+-----+-----+-----+----->
  '-TRANSFERMethod--+-Tcpi-----+'
      | (3) |
      '-Fasp-----'
```

Anmerkungen:

1. Der Parameter CROSSDEFINE gilt nicht für Speicheragentendefinitionen.
2. Der Parameter VALIDATEPROTOCOL ist veraltet und gilt nur für Speicheragentendefinitionen.
3.  Linux-Betriebssysteme Der Parameter TRANSFERMETHOD ist nur auf Betriebssystemen Linux x86\_64 verfügbar.

## Syntax für virtuelle Datenträger

```
>>-DEFine--SERver--Servername--PAssword---Kenwort----->
>--HLAddress---IP-Adresse--LLAddress---TCP-Anschluss----->
>-----+-----+-----+-----+----->
  '-COMMmethod---TCPIP-'  '-URL---URL-'
>-----+-----+-----+-----+----->
  '-DELgraceperiod---Tage-'  '-NODEName---Knotenname-'
                                     .-SSL---No-----
>-----+-----+-----+-----+----->
  '-DESCription---Beschreibung-'  '-SSL---+No--+-'
                                     '-Yes-'
                                     .-SESSIONSECurity---TRANSitional-----
>-----+-----+-----+-----+-----<
  '-SESSIONSECurity---+STRict-----+-'
                                     '-TRANSitional-'
```

## Parameter

### Servername (Erforderlich)

Gibt den Namen des Servers an. Dieser Name muss auf dem Server eindeutig sein. Die maximale Länge dieses Namens beträgt 64 Zeichen.

Für die Ereignisprotokollierung zwischen Servern, die gemeinsame Speicherarchivnutzung, und die Knotenreplikation müssen Sie einen Servernamen angeben, der mit dem Namen übereinstimmt, der mit dem Befehl SET SERVERNAME auf dem Zielsystem definiert wurde.

### PAssword

Gibt das Kennwort an, das für die Anmeldung am Zielsystem für virtuelle Datenträger verwendet wird. Wenn Sie den Parameter NODENAME angeben, müssen Sie den Parameter PASSWORD angeben. Wird der Parameter PASSWORD, aber nicht der Parameter NODENAME angegeben, wird als Knotenname standardmäßig der Servername verwendet, der mit dem Befehl SET SERVERNAME angegeben wird.

### SERVERPAssword

Gibt das Kennwort des Servers an, der definiert wird. Dieses Kennwort muss mit dem Kennwort übereinstimmen, das mit dem Befehl SET SERVERPASSWORD definiert wird. Dieser Parameter ist für die unternehmensweite Konfiguration und die Ereignisprotokollierung zwischen Servern erforderlich.

### HLAddress (Erforderlich)

Gibt die IP-Adresse des Servers an (in der Schreibweise mit Trennzeichen).

Verwenden Sie nicht die Loopback-Adresse als Wert dieses Parameters. Virtuelle Datenträger werden nicht unterstützt, wenn der Quellensystem und der Zielsystem derselbe IBM Spectrum Protect-System sind.

### LLAddress (Erforderlich)

Gibt die Adresse der unteren Ebene des Servers an. Diese Adresse stimmt normalerweise mit der Adresse in der Serveroption TCPSPORT des Zielsystems überein. Bei SSL=YES muss der Anschluss bereits für die SSL-Übertragung auf dem Zielsystem definiert sein.

### COMMmethod

Gibt die Übertragungsmethode an, mit der die Verbindung zum Server hergestellt wird. Dieser Parameter ist wahlfrei.

### URL

Gibt die URL-Adresse dieses Servers an. Der Parameter ist wahlfrei.

### DELgraceperiod

Gibt die Anzahl Tage an, die ein Objekt auf dem Zielsystem verbleibt, nachdem es zum Löschen markiert wurde. Sie können einen Wert von 0 bis 9999 angeben. Der Standardwert ist 5. Dieser Parameter ist optional.

### NODEName

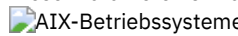


Gibt einen Knotennamen an, den der Server für die Verbindung zum Zielsystem verwenden soll. Dieser Parameter ist wahlfrei. Wenn der Parameter NODENAME angegeben wird, muss auch der Parameter PASSWORD angegeben werden. Wird der Parameter PASSWORD, aber nicht der Parameter NODENAME angegeben, wird als Knotenname standardmäßig der Servername verwendet, der mit dem Befehl SET SERVERNAME angegeben wurde.

### DESCription

Gibt eine Beschreibung des Servers an. Der Parameter ist wahlfrei. Die Beschreibung kann bis zu 255 Zeichen umfassen. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält.

### CROSSDEFine

Gibt an, ob der Server, der diesen Befehl ausführt, sich selbst für den Server definiert, der durch diesen Befehl angegeben wird. Dieser Parameter ist wahlfrei.

   Wichtig: Dieser Parameter gilt nicht für Speicheragentdefinitionen.

Wird dieser Parameter angegeben, müssen auch die Befehle SET SERVERNAME, SET SERVERPASSWORD, SET SERVERHLADDRESS, SET CROSSDEFINE und SET SERVERLLADDRESS ausgegeben werden. Der Standardwert ist NO.

Hinweis:

- Für Replikationsoperationen müssen die Namen der Quellen- und Zielreplikationsserver mit den Namen übereinstimmen, die in diesem Befehl angegeben werden.
- CROSSDEFINE kann mit SSL=YES verwendet werden, wenn alle Bedingungen, die für den Parameter SSL=YES angegeben werden, auf dem Quellen- und Zielsystem wirksam sind.

Sie können einen der folgenden Werte angeben:

No

Die Querdefinition wird nicht ausgeführt.

Yes

Die Querdefinition wird ausgeführt.

#### VALIDateprotocol (veraltet)

Gibt an, ob eine zyklische Blockprüfung die Daten validiert, die zwischen dem Speicheragenten und dem IBM Spectrum Protect-Server gesendet werden. Der Parameter ist wahlfrei. Der Standardwert ist NO.

Wichtig: Ab IBM Spectrum Protect Version 8.1.2 und Tivoli Storage Manager Version 7.1.8 wird die durch diesen Parameter aktivierte Validierung durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter SESSIONSECURITY durchgesetzt wird. Der Parameter VALIDATEPROTOCOL wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

#### SSL

Gibt den Kommunikationsmodus des Servers an. Der Standardwert ist NO.

Wichtig: Ab IBM Spectrum Protect Version 8.1.2 und Tivoli Storage Manager Version 7.1.8 verwendet der Parameter SSL SSL, um einen Teil der Kommunikation mit dem angegebenen Server zu verschlüsseln, auch wenn SSL=NO definiert ist.

Die folgenden Bedingungen und Hinweise gelten, wenn Sie den Parameter SSL angeben:

- Selbst signierte Zertifikate der Partnerserver müssen sich in der Schlüsseldatenbankdatei (cert.kdb) jedes Servers befinden, bevor die Server gestartet werden.
- Sie können mehrere Servernamen mit verschiedenen Parametern für denselben Zielsystem definieren.
- Speicheragenten können den Befehl DSMSTA SETSTORAGESEVER ausgeben und den Parameter SSL einschließen, um die Schlüsseldatenbank zu erstellen.

Sie können einen der folgenden Werte angeben:

No

Gibt eine SSL-Sitzung für die gesamte Kommunikation mit dem angegebenen Server an, außer wenn der Server Objektdaten sendet oder empfängt. Objektdaten werden mithilfe von TCP/IP gesendet und empfangen. Wird ausgewählt, dass die Objektdaten nicht verschlüsselt werden, ähnelt die Serverleistung der Kommunikation über eine TCP/IP-Sitzung und die Sitzung ist sicher.

Yes

Gibt eine SSL-Sitzung für die gesamte Kommunikation mit dem angegebenen Server an, auch wenn der Server Objektdaten sendet und empfängt.

#### SESSIONSECurity

Gibt an, ob der Server, der definiert wird, die sichersten Einstellungen verwenden muss, um mit einem IBM Spectrum Protect-Server zu kommunizieren. Dieser Parameter ist wahlfrei.

Sie können einen der folgenden Werte angeben:

#### STRict

Gibt an, dass die striktesten Sicherheitseinstellungen für den Server, der definiert wird, durchgesetzt werden. Der Wert STRICT verwendet das sicherste Kommunikationsprotokoll, das verfügbar ist. Dies ist derzeit TLS 1.2. Das TLS 1.2-Protokoll wird für SSL-Sitzungen zwischen dem angegebenen Server und einem IBM Spectrum Protect-Server verwendet. Für die Verwendung des Werts STRICT müssen die folgenden Anforderungen erfüllt werden, um sicherzustellen, dass sich der angegebene Server mit dem IBM Spectrum Protect-Server authentifizieren kann:

- Der Server, der definiert wird, und der IBM Spectrum Protect-Server müssen IBM Spectrum Protect-Software verwenden, die den Parameter SESSIONSECURITY unterstützt.



- Der Server, der definiert wird, muss für die Verwendung des TLS 1.2-Protokolls für SSL-Sitzungen zwischen sich selbst und dem IBM Spectrum Protect-Server konfiguriert werden.


Server, für die der Wert STRICT definiert ist und die diese Anforderungen nicht erfüllen, können sich nicht mit dem IBM Spectrum Protect-Server authentifizieren.

#### TRANSITIONAL

Gibt an, dass die vorhandenen Sicherheitseinstellungen für den Server durchgesetzt werden. Dies ist der Standardwert. Dieser Wert ist für die temporäre Verwendung bestimmt, während Sie Ihre Sicherheitseinstellungen aktualisieren, um die Anforderungen für den Wert STRICT zu erfüllen.

Ist SESSIONSECURITY=TRANSITIONAL definiert und hat der Server nie die Anforderungen für den Wert STRICT erfüllt, authentifiziert sich der Server weiterhin mithilfe des Werts TRANSITIONAL. Wenn ein Server jedoch die Anforderungen für den Wert STRICT erfüllt, wird der Wert des Parameters SESSIONSECURITY automatisch von TRANSITIONAL in STRICT aktualisiert. Der Server kann sich dann nicht mehr mit einer Version des Clients oder mit einem SSL/TLS-Protokoll authentifizieren, die bzw. das die Anforderungen für STRICT nicht erfüllt. Nachdem sich ein Server erfolgreich mit einem Kommunikationsprotokoll authentifiziert hat, das mehr Sicherheit bietet, kann sich der Server nicht mehr mit einem weniger sicheren Protokoll authentifizieren. Beispiel: Wenn ein Server, der nicht SSL verwendet, aktualisiert wird und sich mithilfe von TLS 1.2 erfolgreich authentifiziert, kann sich der Server nicht mehr ohne SSL-Protokoll oder mithilfe von TLS 1.1 authentifizieren. Diese Einschränkung gilt auch bei Verwendung von Funktionen wie z. B. virtuelle Datenträger, Befehlsweiterleitung oder Export zwischen Servern, wenn sich ein Knoten oder Administrator beim IBM Spectrum Protect-Server als Knoten oder Administrator von einem anderen Server authentifiziert.

#### TRANSFERMETHOD

 Gibt die Methode an, die für die Datenübertragung zwischen Servern verwendet wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

##### Tcpip

Gibt an, dass TCP/IP für die Übertragung von Daten verwendet wird. Dies ist der Standardwert.

##### Fasp

Gibt an, dass die Aspera FASP-Technologie (Fast Adaptive Secure Protocol) für die Übertragung von Daten verwendet wird. Mit der Aspera FASP-Technologie kann die Datenübertragung in einem Weitverkehrsnetz (WAN) optimiert werden. Einschränkungen:

- Bevor Sie die Aspera FASP-Technologie aktivieren, müssen Sie bestimmen, ob die Technologie für Ihre Systemumgebung geeignet ist, und die entsprechenden Lizenzen installieren. Anweisungen finden Sie unter Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann. Wenn die Lizenzen fehlen oder abgelaufen sind, schlagen Datenübertragungsoperationen fehl.
- Wenn die WAN-Leistung Ihre Geschäftsanforderungen erfüllt, aktivieren Sie nicht die Aspera FASP-Technologie.
- Wenn Sie TRANSFERMETHOD=FASP im Befehl PROTECT STGPOOL oder REPLICATE NODE angeben, überschreibt dieser Wert den Parameter TRANSFERMETHOD in den Befehlen DEFINE SERVER und UPDATE SERVER.

## Beispiel: Zwei Server definieren, die SSL für die Kommunikation verwenden sollen (manuelle Konfiguration)

Tipp: Wenn beide Server IBM Spectrum Protect-Software der Version 8.1.2 oder höher oder Tivoli Storage Manager-Software der Version 7.1.8 verwenden, wird SSL automatisch zwischen den Servern konfiguriert und die manuelle Konfiguration ist nicht erforderlich.

Wenn beide Server keine Software der Version 7.1.8 und keine Software der Version 8.1.2 oder höher verwenden, müssen Sie die beiden Server manuell für die Verwendung von SSL für die Kommunikation konfigurieren.

Die Serveradressen lauten:

- ServerA befindet sich unter `bfa.tucson.ibm.com`
- ServerB befindet sich unter `bfb.tucson.ibm.com`

Führen Sie die folgenden Schritte aus, um die beiden Server für SSL zu definieren:

1. Geben Sie die Option TCPPOPT 1500 für beide Server in der Optionsdatei `dsmserv.opt` an.
2. Starten Sie beide Server.
3. Fahren Sie beide Server herunter, um das Partnerzertifikat `cert256` zu importieren. Für ServerA befindet sich das Zertifikat im Instanzverzeichnis `/tsma`. Für ServerB befindet sich das Zertifikat im Instanzverzeichnis `/tsmb`.
4. Starten Sie beide Server. Die Datei `/tsma/cert256.arm` wird in `/tsmb/cert256.bfa.arm` unter der Adresse `bfb.tucson.ibm.com` kopiert. Die Datei `/tsmb/cert256.arm` wird in `/tsmb/cert256.bfb.arm` unter der Adresse `bfa.tucson.ibm.com` kopiert.
5. Geben Sie den folgenden Befehl aus:
  - Auf ServerA:

```
gsk8capiCmd_64 -cert -add -db cert.kdb -stashed -format ascii
-label "bfb" -file /tsma/cert256.bfb.arm
```

- o Auf ServerB:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii  
-label "bfa" -file /tsmb/cert256.bfa.arm
```

Sie können auf jedem Server die Zertifikate in der Schlüsseldatenbank anzeigen, indem Sie den folgenden Befehl ausgeben:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

6. Starten Sie die Server erneut.

7. Geben Sie den entsprechenden Befehl DEFINE SERVER aus. Geben Sie für ServerA den folgenden Beispielbefehl aus:

```
DEFINE SERVER BFB hla=bfbc.tucson.ibm.com lla=1542  
serverpa=Kennwortfürbfb SSL=YES
```

Geben Sie für ServerB den folgenden Beispielbefehl aus:

```
DEFINE SERVER BFA hla=bfa.tucson.ibm.com lla=1542  
serverpa=Kennwortfürbfa SSL=YES
```

Wird SSL nicht verwendet, geben Sie den folgenden Beispielbefehl DEFINE SERVER auf ServerA aus:

```
DEFINE SERVER BFBTCP hla=bfbc.tucson.ibm.com lla=1500  
serverpa=Kennwortfürbfb SSL=NO
```

Wird SSL nicht verwendet, geben Sie den folgenden Beispielbefehl DEFINE SERVER auf ServerB aus:

```
DEFINE SERVER BFATCP hla=bfa.tucson.ibm.com lla=1500  
serverpa=Kennwortfürbfa SSL=NO
```

## Beispiel: Einen Server für die Kommunikation mit einem anderen Server unter Verwendung der Sitzungssicherheit 'strict' definieren

---

Einen Server mit dem Namen SERVER1 definieren, um die striktesten Sicherheitseinstellungen für die Authentifizierung mit dem IBM Spectrum Protect-Server zu verwenden.

```
define server server1 sessionsecurity=strict
```

## Beispiel: Einen Zielsever definieren

---

Ein Zielsever hat die Adresse der höheren Ebene 9.116.2.67 und die Adresse der unteren Ebene 1570. Diesen Zielsever für den Quellenserver definieren, den Namen SERVER2 zuordnen und das Kennwort auf SECRET setzen. Angeben, dass Objekte 7 Tage auf dem Zielsever verbleiben, nachdem sie zum Löschen markiert wurden.

```
define server server2 password=secret  
hladdress=9.115.3.45 lladdress=1570 delgraceperiod=7
```

## Beispiel: Einen Server definieren, der Befehle von anderen Servern empfängt

---

Einen Server definieren, der von anderen Servern weitergeleitete Befehle empfangen kann. Dem Server den Namen WEST\_COMPLEX zuordnen. Die Adresse der höheren Ebene auf 9.172.12.35, die Adresse der unteren Ebene auf 1500 und die URL-Adresse auf http://west\_complex:1580/ setzen.

```
define server west_complex  
hladdress=9.172.12.35 lladdress=1500  
url=http://west_complex:1580/
```

## Beispiel: Zwei Server über Querdefinition definieren

---

Mit Hilfe der Querdefinition SERVER\_A und SERVER\_B definieren.

1. Auf SERVER\_B den Servernamen, das Kennwort sowie die Adressen der höheren und der unteren Ebene von SERVER\_B angeben. Angeben, dass Querdefinitionen zulässig sind.

```
set servername server_b  
set serverpassword mylife  
set serverhladdress 9.115.20.80  
set serverlladdress 1860  
set crossdefine on
```

2. Auf SERVER\_A den Servernamen, das Kennwort sowie die Adressen der höheren und der unteren Ebene von SERVER\_A angeben.

```

set servername server_a
set serverpassword yourlife
set serverhladdress 9.115.20.97
set serverlladdress 1500

```

### 3. SERVER\_B auf SERVER\_A definieren:


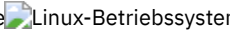






```

define server server_b hladdress=9.115.20.80 lladdress=1860
serverpassword=mylife crossdefine=yes

```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE SERVER

| Befehl  | Beschreibung  |
|---|---|
| DEFINE DEVCLASS   | Definiert eine Einheitenklasse.   |
|   DEFINE PATH     |   Definiert einen Pfad, wenn das Ziel ein z/OS Media-Server ist.     |
| DELETE DEVCLASS   | Löscht eine Einheitenklasse.  |
| DELETE FILESPACE  | Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.                |
| DELETE SERVER   | Löscht die Definition eines Servers.  |
| QUERY NODE  | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.   |
| QUERY SERVER  | Zeigt Informationen über Server an.   |
| RECONCILE VOLUMES   | Stimmt Definitionen von virtuellen Datenträgern auf dem Quellenserver mit Archivierungsobjekten des Zielservers ab.   |
| REGISTER NODE   | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.   |
| REMOVE NODE   | Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.  |
| SET CROSSDEFINE   | Gibt an, ob Server überkreuz definiert werden sollen.   |
| SET SERVERNAME  | Gibt den Namen an, unter dem der Server registriert ist.  |
| SET SERVERHLADDRESS   | Gibt die Adresse der höheren Ebene eines Servers an.  |
| SET SERVERLLADDRESS   | Gibt die Adresse der unteren Ebene eines Servers an.  |
| SET SERVERPASSWORD  | Gibt das Serverkennwort an.   |
| SET REPLSERVER  | Gibt einen Zielreplikationsserver an.   |
| UPDATE DEVCLASS   | Ändert die Attribute einer Einheitenklasse.   |
| UPDATE NODE   | Ändert die Attribute, die einem Clientknoten zugeordnet sind.   |
|   UPDATE PATH |   Definiert einen Pfad, wenn das Ziel ein z/OS Media-Server ist. |
| UPDATE SERVER   | Aktualisiert Informationen über einen Server.   |

## DEFINE SERVERGROUP (Server-Gruppe definieren)

Mit diesem Befehl kann eine Server-Gruppe definiert werden. Mit einer Servergruppe können Befehle an mehrere Server weitergeleitet werden, indem nur der Gruppenname angegeben wird. Nach der Definition der Servergruppe können mit dem Befehl DEFINE GRPMEMBER Server zur Gruppe hinzugefügt werden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-DEFine SERVERGroup--Gruppenname----->
>--+-----+----->
  '-DESCRiption----Beschreibung-'
```

## Parameter

Gruppenname (Erforderlich)

Gibt den Namen der Server-Gruppe an. Die maximale Länge des Namens beträgt 64 Zeichen.

DESCRiption

Gibt eine Beschreibung der Server-Gruppe an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

## Beispiel: Eine Servergruppe definieren

Die Server-Gruppe WEST\_COMPLEX definieren.

```
define servergroup west_complex
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE SERVERGROUP

| Befehl             | Beschreibung  |
|--------------------|---|
| COPY SERVERGROUP   | Erstellt eine Kopie einer Servergruppe.             |
| DEFINE GRPMEMBER   | Definiert einen Server als Teil einer Servergruppe. |
| DELETE GRPMEMBER   | Löscht einen Server aus einer Servergruppe.         |
| DELETE SERVERGROUP | Löscht eine Servergruppe.                           |
| MOVE GRPMEMBER     | Versetzt einen Teil einer Servergruppe.             |
| QUERY SERVERGROUP  | Zeigt Informationen über Servergruppen an.          |
| RENAME SERVERGROUP | Benennt eine Servergruppe um.                       |
| UPDATE SERVERGROUP | Aktualisiert eine Servergruppe.                     |

## DEFINE SPACETRIGGER (Speicherbereichsauslöser definieren)

Mit diesem Befehl können Einstellungen für Auslöser definiert werden, die festlegen, wann und wie der Server zusätzlichen Speicherbereich vorbereitet, wenn vordefinierte Schwellen in Speicherpools, die die Einheitenklassen FILE und DISK verwenden, überschritten werden. Speicherbereichsauslöser werden für Speicherpools mit dem Parameter RECLAMATIONTYPE=SNAPLOCK nicht aktiviert.

Der IBM Spectrum Protect-Server ordnet weiteren Speicherbereich zu, wenn die Speicherauslastung einen angegebenen Wert erreicht. Nachdem weiterer Speicherbereich zugeordnet wurde, fügt der Server den Speicherbereich dem angegebenen Pool hinzu (Platte mit wahlfreiem Zugriff oder sequenziellem Zugriff).

Wichtig: Bei Speicherbereichsauslöserfunktionen und Berechnungen des Speicherbereichs im Speicherpool wird der Speicherbereich berücksichtigt, der in jedem Verzeichnis verbleibt. Eine ungenaue Berechnung kann zu einem Fehler bei der Erweiterung des Speicherbereichs führen, der in einem Speicherpool verfügbar ist. Ein Fehler bei der Erweiterung des Speicherbereichs in einem Speicherpool ist eine der Bedingungen, die zur Inaktivierung eines Auslösers führen kann.

Wenn Sie beispielsweise mehrere Verzeichnisse für eine Einheitenklasse angeben und sich die Verzeichnisse in demselben Dateisystem befinden, berechnet der Server den Speicherbereich durch Hinzufügen von Werten, die den Speicherbereich darstellen, der in jedem Verzeichnis verbleibt. Diese Speicherbereichsberechnungen sind ungenau. Anstatt einen Speicherpool mit ausreichend Speicherbereich für eine Operation auszuwählen, kann der Server das Verzeichnis auswählen, das für die Einheitenklasse angegeben ist, und frühzeitig über keinen Speicherbereich mehr verfügen.

Um mögliche Probleme zu vermeiden und eine genaue Berechnung sicherzustellen, sollten Sie jedem Verzeichnis ein separates Dateisystem zuordnen. Wird ein Auslöser inaktiviert, da der Speicherbereich in einem Speicherpool nicht erweitert werden konnte,

können Sie den Auslöser erneut aktivieren, indem Sie den folgenden Befehl angeben: `update spacetrigger stg`. Es sind keine weiteren Änderungen an dem Speicherbereichsauslöser erforderlich.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
                .-Fullpct----80-----.  
>>-DEFine SPACetrigger---STG-----+-----+----->  
                '-Fullpct----Prozent-'  
  
                .-SPACEexpansion----20-----.  
>>+-----+-----+----->  
                '-SPACEexpansion----Prozent-'  
  
>+-----+-----+----->  
                '-EXpansionprefix----Präfix-'  
  
>+-----+-----+----->  
                '-STGPOOL----Speicherpoolname-'
```

## Parameter

---

### STG

Gibt einen Speicherbereichsauslöser für den Speicherpool an.

### Fullpct

Dieser Parameter gibt den Auslastungsprozentsatz des Speicherpools an. Dieser Parameter ist wahlfrei. Geben Sie einen ganzzahligen Wert von 0 bis 99 an. Der Standardwert ist 80. Der Wert 0 inaktiviert den Speicherbereichsauslöser. Wird dieser Wert überschritten, erstellt der Speicherbereichsauslöser neue Datenträger. Bei Überschreiten der Schwelle werden neue Datenträger möglicherweise erst bei der nächsten Anforderung von Speicherbereich erstellt.


Sie können die Auslastung des Speicherpools bestimmen, indem Sie den Befehl `QUERY STGPOOL` mit `FORMAT=DETAILED` ausgeben. Der Prozentsatz der Speicherpoolauslastung wird im Feld "Ausl. für Speicherbereichsauslöser" angezeigt. Die Berechnung dieses Prozentsatzes schließt keine potenziellen Arbeitsdatenträger ein. Die Berechnung der prozentualen Auslastung, die für die Umlagerung und Wiederherstellung verwendet wird, schließt jedoch potenzielle Arbeitsdatenträger ein.

### SPACEexpansion

Für Speicherpools des Typs `FILE` mit sequenziellem Zugriff wird dieser Parameter bei der Bestimmung der Anzahl zusätzlicher Datenträger verwendet, die in dem Speicherpool erstellt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist 20. Datenträger werden unter Verwendung des Werts für `MAXCAPACITY` aus der Einheitenklasse des Speicherpools erstellt. Für `DISK`-Speicherpools mit wahlfreiem Zugriff erstellt der Speicherbereichsauslöser einen einzelnen Datenträger unter Verwendung von `EXPANSIONPREFIX`.

### EXpansionprefix



Für `DISK`-Speicherpools mit wahlfreiem Zugriff gibt dieser Parameter das Präfix an, das der Server zum Erstellen neuer Speicherpooldateien verwendet. Dieser Parameter ist wahlfrei und gilt nur für Einheitenklassen `DISK` mit wahlfreiem Zugriff. Das Standardpräfix ist der Serverinstallationspfad.


Das Präfix kann ein oder mehrere Verzeichnistrennzeichen enthalten. Beispiel:  

```
/opt/tivoli/tsm/server/bin/
```

```
 Windows-Betriebssysteme
```

```
c:\Programme\tivoli\tsm\
```

  Es können bis zu 250 Zeichen angegeben werden. Wird ein ungültiges Präfix angegeben, kann die automatische Erweiterung fehlschlagen.

 Sie können bis zu 200 Zeichen angeben. Wird ein ungültiges Präfix angegeben, kann die automatische Erweiterung fehlschlagen. Wird der Server als Windows-Dienst ausgeführt, ist das Standardpräfix das Verzeichnis `c:\wnnt\system32`.

Dieser Parameter ist für Speicherbereichsauslöser für `FILE`-Speicherpools mit sequenziellem Zugriff nicht gültig. Es werden Präfixe der Verzeichnisse verwendet, die mit der zugeordneten Einheitenklasse angegeben werden.

## STGPOOL

Gibt den Speicherpool an, der diesem Speicherbereichsauslöser zugeordnet ist. Dieser Parameter ist für Speicherbereichsauslöser für den Speicherpool wahlfrei. Wird der Parameter STG angegeben, aber der Parameter STGPOOL nicht angegeben, wird ein Speicherbereichsauslöser erstellt, der für alle DISK-Speicherpools mit wahlfreiem Zugriff und alle FILE-Speicherpools mit sequenziellem Zugriff gilt, die keinen spezifischen Speicherbereichsauslöser haben.

Dieser Parameter gilt nicht für Speicherpools mit dem Parameter RECLAMATIONTYPE=SNAPLOCK.

## Beispiel: Einen Speicherbereichsauslöser definieren, um den Speicherbereich im Speicherpool um 25 Prozent zu erhöhen

Einen Speicherbereichsauslöser für den Speicherpool definieren, um den Speicherbereich in einem Speicherpool um 25 Prozent zu vergrößern, wenn der Speicherpool zu 80 Prozent mit vorhandenen Datenträgern belegt ist. Speicherbereich wird in den Verzeichnissen erstellt, die der Einheitenklasse zugeordnet sind.

```
define spacetrigger stg spaceexpansion=25 stgpool=file
```

## Beispiel: Einen Speicherbereichsauslöser definieren, um den Speicherbereich im Speicherpool um 40 Prozent zu erhöhen

Einen Speicherbereichsauslöser für den Speicherpool WINPOOL1 definieren, um den Speicherbereich in dem Speicherpool um 40 Prozent zu vergrößern, wenn der Speicherpool zu 80 Prozent mit vorhandenen Datenträgern belegt ist.

```
define spacetrigger stg spaceexpansion=40 stgpool=winpool1
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE SPACETRIGGER

| Befehl              | Beschreibung   |
|---------------------|--|
| DEFINE VOLUME       | Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll. |
| DELETE SPACETRIGGER | Löscht den Speicherbereichsauslöser für den Speicherpool.  |
| QUERY SPACETRIGGER  | Zeigt Informationen zu einem Speicherbereichsauslöser für den Speicherpool an.                                 |
| UPDATE SPACETRIGGER | Ändert Attribute des Speicherbereichsauslösers für den Speicherpool.   |

## DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)

Mit diesem Befehl können Sie einen neuen Schwellenwert für die Statusüberwachung definieren.

Mit Statusüberwachungsschwellenwerten werden die definierten Bedingungen mit den Serverabfragen für die Statusüberwachung verglichen und die Ergebnisse in die Statusüberwachungstabelle eingefügt.

Es können mehrere Schwellenwerte für eine Aktivität definiert werden. Sie können beispielsweise einen Schwellenwert erstellen, der einen Warnstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 80 % ist. Sie können dann einen anderen Schwellenwert erstellen, der einen Fehlerstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 90 % ist.

Anmerkung: Wenn bereits ein Schwellenwert für eine Bedingung EXISTS definiert ist, können Sie keinen anderen Schwellenwert mit einem der anderen Bedingungstypen definieren.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-DEFine STATusthreshold--Schwellenwertname--Aktivität----->
.-Condition----EXists-----.
```

```

>----->
'-Condition--=-+-Exists-+-' '-Value-----Wert-'
      +-GT-----+
      +-GE-----+
      +-LT-----+
      +-LE-----+
      '-Equal--'

.-Status-----Normal-----.
>-----<
'-Status-----+Normal--+-'
      +-Warning-+
      '-Error---'

```

## Parameter

### Schwellenwertname (Erforderlich)

Gibt den Schwellenwertnamen an. Der Name darf 48 Zeichen nicht überschreiten.

### Aktivität (Erforderlich)

Gibt die Aktivität an, für die Statusanzeiger erstellt werden sollen. Geben Sie einen der folgenden Werte an:

#### PROCESSSUMMARY

Gibt die Anzahl Prozesse an, die gegenwärtig aktiv sind.

#### SESSIONSUMMARY

Gibt die Anzahl Sitzungen an, die gegenwärtig aktiv sind.

#### CLIENTSESSIONSUMMARY

Gibt die Anzahl Clientsitzungen an, die gegenwärtig aktiv sind.

#### SCHEDCLIENTSESSIONSUMMARY

Gibt die Anzahl geplanter Clientsitzungen an.

#### DBUTIL

Gibt die prozentuale Datenbankauslastung an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

#### DBFREESPACE

Gibt den freien Speicherbereich in Gigabyte an, der in der Datenbank verfügbar ist.

#### DBUSEDSPACE

Gibt den verwendeten Datenbankbereich in Gigabyte an.

#### ARCHIVELOGFREESPACE

Gibt den freien Speicherbereich in Gigabyte an, der im Archivprotokoll verfügbar ist.

#### STGPOOLUTIL

Gibt die prozentuale Auslastung des Speicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

#### STGPOOLCAPACITY

Gibt die Speicherpoolkapazität in Gigabyte an.

#### AVGSTGPOOLUTIL

Gibt die durchschnittliche prozentuale Speicherpoolauslastung für alle Speicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

#### TOTSTGPOOLCAPACITY

Gibt die Gesamtspeicherpoolkapazität in Gigabyte für alle verfügbaren Speicherpools an.

#### TOTSTGPOOLS

Gibt die Anzahl der definierten Speicherpools an.

#### TOTRWSTGPOOLS

Gibt die Anzahl der definierten Speicherpools an, die lesbar oder änderbar sind.

#### TOTNOTRWSTGPOOLS

Gibt die Anzahl der definierten Speicherpools an, die nicht lesbar oder änderbar sind.

#### STGPOOLINUSEANDEFINED

Gibt die Gesamtzahl der definierten Datenträger an, die im Gebrauch sind.

#### ACTIVELOGUTIL

Gibt die aktuelle prozentuale Auslastung der aktiven Protokolldatei an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

#### ARCHLOGUTIL

Gibt die aktuelle Auslastung des Archivprotokolls an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

#### CPYSTGPOOLUTIL

Gibt die prozentuale Auslastung eines Kopierspeicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

#### PMRYSTGPOOLUTIL

Gibt die prozentuale Auslastung eines primären Speicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

#### DEVCLASSPCTDRVOFFLINE

Gibt die prozentuale Auslastung von Laufwerken an (nach Einheitenklasse), die offline sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

#### DEVCLASSPCTDRVPOLLING

Gibt den Sendeaufruf für Laufwerke nach Einheitenklasse an. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

#### DEVCLASSPCTLIBPATHSOFFLINE

Gibt die Kassettenarchivpfade an (nach Einheitenklasse), die offline sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

#### DEVCLASSPCTPATHSOFFLINE

Gibt den Prozentsatz der Einheitenklassenpfade an (nach Einheitenklasse), die offline sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

#### DEVCLASSPCTDISKSNOTRW

Gibt den Prozentsatz der Platten an, die für die Einheitenklasse DISK nicht beschreibbar sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

#### DEVCLASSPCTDISKSUNAVAILABLE

Gibt den Prozentsatz der Plattendatenträger an (nach Einheitenklasse), die nicht verfügbar sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

#### FILEDEVCLASSPCTSCRUNALLOCATABLE

Gibt den Prozentsatz der Arbeitsdatenträger an, die der Server für eine bestimmte Einheitenklasse FILE, die nicht gemeinsam genutzt wird, nicht zuordnen kann. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

#### Condition

Gibt die Bedingung an, die verwendet wird, um die Aktivitätsausgabe mit dem angegebenen Wert zu vergleichen. Der Standardwert ist EXISTS. Geben Sie einen der folgenden Werte an:

##### EXists

Erstellt einen Statusüberwachungsanzeiger, wenn die Aktivität vorhanden ist.

##### GT

Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis größer als der angegebene Wert ist.

##### GE

Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis größer-gleich dem angegebenen Wert ist.

##### LT

Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis kleiner als der angegebene Wert ist.

##### LE

Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis kleiner-gleich dem angegebenen Wert ist.

##### EQual

Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis gleich dem angegebenen Wert ist.

#### Value (Erforderlich)

Gibt den Wert an, der mit der Aktivitätsausgabe für die angegebene Bedingung verglichen wird. Sie müssen diesen Parameter angeben, wenn CONDITION nicht auf EXISTS gesetzt ist. Sie können eine ganze Zahl im Bereich von 0 bis 9999999999999999 angeben.

#### Status

Gibt den Status des Anzeigers an, der bei der Statusüberwachung erstellt wird, wenn die Bedingung, die ausgewertet wird, erfüllt ist. Dieser optionale Parameter hat den Standardwert NORMAL. Geben Sie einen der folgenden Werte an:

##### Normal

Gibt an, dass der Statusanzeiger einen normalen Statuswert hat.

##### Warnung

Gibt an, dass der Statusanzeiger einen Warnstatuswert hat.

##### Fehler

Gibt an, dass der Statusanzeiger einen Fehlerstatuswert hat.

## Statusschwellenwert definieren

---

Mit dem folgenden Befehl einen Statusschwellenwert für die durchschnittliche prozentuale Speicherpoolauslastung definieren:

```
define statusthreshold avgstgpl "AVGSTGPOOLUTIL" value=85 condition=gt status=warning
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für DEFINE STATUSTHRESHOLD

---



| Befehl  | Beschreibung   |
|---|--|
| DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)  | Löscht einen Schwellenwert für die Statusüberwachung.  |
| QUERY MONITORSTATUS (Überwachungsstatus abfragen)   | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                             |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)                                      | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                             |
| QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)   | Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.   |
| SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)   | Gibt an, ob die Statusüberwachung aktiviert werden soll.   |
| SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)        | Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.         |
| SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)   | Gibt das Aktualisierungsintervall für die Statusüberwachung an.  |
| SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll) | Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll. |
| UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)  | Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.   |

## DEFINE STGPOOL (Speicherpool definieren)

Mit diesem Befehl kann ein primärer Speicherpool, ein Kopierspeicherpool, ein Pool für aktive Daten, ein Verzeichniscontainerspeicherpool, ein Containerkopierspeicherpool oder ein Containerspeicherpool in einer Cloudumgebung definiert werden.

Ein primärer Speicherpool stellt einen Zielort für Sicherungsdateien, Archivierungsdateien oder Dateien zur Verfügung, die von Clientknoten umgelagert werden. Ein Kopierspeicherpool stellt einen Zielort für Kopien von Dateien zur Verfügung, die sich in primären Speicherpools befinden. Ein Pool für aktive Daten stellt einen Zielort für aktive Versionen von Sicherungsdaten zur Verfügung, die sich in primären Speicherpools befinden. Ein Containerspeicherpool stellt ein Ziel für deduplizierte Dateien bereit. Ein Cloudspeicherpool stellt Speicher in einer Cloudumgebung bereit. Ein Containerkopierspeicherpool stellt eine Bandkopie eines Verzeichniscontainerspeicherpools bereit. Die maximale Anzahl der Speicherpools, die für einen Server definiert werden kann, beträgt 999.

Alle Datenträger in einem Speicherpool gehören zu derselben Einheitenklasse. Speicherpools mit wahlfreiem Zugriff verwenden den Einheitentyp DISK. Nach der Definition eines Speicherpools mit wahlfreiem Zugriff müssen Datenträger für den Pool definiert werden, um Speicherbereich zu erstellen.

Speicherpools mit sequenziellem Zugriff verwenden Einheitenklassen, die Sie für Bänder, Dateien auf Platte (Einheitentyp FILE) und Speicher auf einem anderen Server (Einheitentyp SERVER) definieren. Zum Erstellen von Speicherbereich in einem Speicherpool mit sequenziellem Zugriff müssen Arbeitsdatenträger für den Pool zugelassen werden, wenn dieser definiert oder aktualisiert wird, oder es müssen Datenträger für den Pool definiert werden, nachdem der Pool definiert wurde. Es können auch beide Vorgehensweisen verwendet werden.

Einschränkung: Wenn ein Client die Funktion für gleichzeitiges Schreiben und die Dateneduplizierung verwendet, wird das Feature für die Dateneduplizierung während der Ausführung von Sicherungen in einem Speicherpool inaktiviert.

Der Befehl DEFINE STGPOOL verwendet sieben Formen. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für DEFINE STGPOOL

| Befehl            | Beschreibung   |
|-------------------|--|
| BACKUP DB         | Sichert die IBM Spectrum Protect-Datenbank auf Datenträgern mit sequenziellem Zugriff. |
| BACKUP STGPOOL    | Sichert einen primären Speicherpool in einem Kopierspeicherpool.                       |
| COPY ACTIVATEDATA | Kopiert aktive Sicherungsdaten.  |

| Befehl                  | Beschreibung  |
|-------------------------|---|
| DEFINE COLLOGROUP       | Definiert eine Kollokationsgruppe.  |
| DEFINE COLLOCMEMBER     | Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.   |
| DEFINE DEVCLASS         | Definiert eine Einheitenklasse.   |
| DEFINE STGPOOLDIRECTORY | Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool.                             |
| DEFINE VOLUME           | Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.                      |
| DELETE COLLOGROUP       | Löscht eine Kollokationsgruppe.   |
| DELETE COLLOCMEMBER     | Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.   |
| DELETE STGPOOL          | Löscht einen Speicherpool aus dem Serverspeicher.   |
| MOVE DATA               | Versetzt Daten aus einem angegebenen Speicherpooldatenträger in einen anderen Speicherpooldatenträger.                              |
| MOVE MEDIA              | Versetzt Speicherpooldatenträger, die von einem automatisierten Kassettenarchive verwaltet werden.                                  |
| QUERY COLLOGROUP        | Zeigt Informationen zu Kollokationsgruppen an.  |
| QUERY DEVCLASS          | Zeigt Informationen zu Einheitenklassen an.   |
| QUERY NODEDATA          | Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.   |
| QUERY SHREDSTATUS       | Zeigt Informationen zu Daten an, die auf das Schreddern warten.   |
| QUERY STGPOOL           | Zeigt Informationen zu Speicherpools an.  |
| RENAME STGPOOL          | Benennt einen Speicherpool um.  |
| REPAIR STGPOOL          | Repariert einen Verzeichniscontainerspeicherpool.   |
| PROTECT STGPOOL         | Schützt einen Verzeichniscontainerspeicherpool.   |
| RESTORE STGPOOL         | Schreibt Dateien aus Kopierspeicherpools in einen primären Speicherpool zurück.   |
| RESTORE VOLUME          | Schreibt Dateien, die auf angegebenen Datenträgern in einem primären Speicherpool gespeichert sind, aus Kopierspeicherpools zurück. |
| SET DRMPRIMSTGPOOL      | Gibt an, dass primäre Speicherpools von DRM verwaltet werden.   |
| SHRED DATA              | Startet manuell den Prozess zum Schreddern gelöschter Daten.  |
| UPDATE COLLOGROUP       | Aktualisiert die Beschreibung einer Kollokationsgruppe.   |
| UPDATE STGPOOL          | Ändert die Attribute eines Speicherpools.   |

- **DEFINE STGPOOL (Cloud-Containerspeicherpool definieren)**  
Mit diesem Befehl können Sie einen Containerspeicherpool in einer Cloudumgebung definieren. Dieser Typ des Speicherpools wird für die Dateneduplizierung verwendet. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.
- **DEFINE STGPOOL (Verzeichniscontainerspeicherpool definieren)**  
Mit diesem Befehl kann ein Verzeichniscontainerspeicherpool definiert werden, der für die Dateneduplizierung verwendet wird.
- **DEFINE STGPOOL (Containerkopierspeicherpool definieren)**  
Mit diesem Befehl kann ein Containerkopierspeicherpool definiert werden, in dem eine Kopie der Daten aus einem Verzeichniscontainerspeicherpool gespeichert wird.
- **DEFINE STGPOOL (Primären Speicherpool definieren, der Einheiten mit wahlfreiem Zugriff zugeordnet wird)**  
Mit diesem Befehl kann ein primärer Speicherpool definiert werden, der Einheiten mit wahlfreiem Zugriff zugeordnet wird.
- **DEFINE STGPOOL (Primären Speicherpool definieren, der Einheiten mit sequenziellem Zugriff zugeordnet wird)**  
Mit diesem Befehl kann ein primärer Speicherpool definiert werden, der Einheiten mit sequenziellem Zugriff zugeordnet wird.
- **DEFINE STGPOOL (Kopierspeicherpool definieren, der Einheiten mit sequenziellem Zugriff zugeordnet wird)**  
Mit diesem Befehl kann ein Kopierspeicherpool definiert werden, der Einheiten mit sequenziellem Zugriff zugeordnet wird.
- **DEFINE STGPOOL (Pool für aktive Daten definieren, der Einheiten mit sequenziellem Zugriff zugeordnet wird)**  
Mit diesem Befehl kann ein Pool für aktive Daten definiert werden, der Einheiten mit sequenziellem Zugriff zugeordnet wird.



Standardwert No.

## Parameter

---

### Poolname (Erforderlich)

Gibt den Cloudspeicherpool an, der definiert werden soll. Dieser Parameter ist erforderlich. Die maximale Länge des Namens beträgt 30 Zeichen.

### STGType=Cloud (Erforderlich)

Gibt den Typ des Speichers an, der für einen Cloudspeicherpool definiert werden soll. Um sicherzustellen, dass der Speicherpool in einer Cloudumgebung verwendet werden kann, müssen Sie STGTYPE=CLOUD angeben.

Tipp: Um die Leistung zu optimieren, definieren Sie ein oder mehrere lokale Speicherzeichnisse zum temporären Speichern von Daten, die in die Cloud versetzt werden. Verwenden Sie nach der Definition eines Cloud-Containerspeicherpools den Befehl DEFINE STGPOOLDIRECTORY, um dem Cloud-Containerspeicherpool lokale Verzeichnisse zuzuordnen.

### Pooltype=Primary

Gibt an, dass ein primärer Speicherpool definiert werden soll. Dieser Parameter ist wahlfrei.

### DESCription

Gibt eine Beschreibung des Cloudspeicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält.

### CLOUDType

Gibt den Typ der Cloudumgebung an, in der der Speicherpool konfiguriert wird.

Sie können einen der folgenden Werte angeben:

#### Azure

Gibt an, dass der Speicherpool ein Cloud-Computing-System 'Microsoft Azure' verwendet.

#### S3

Gibt an, dass der Speicherpool ein Cloud-Computing-System mit dem Protokoll 'Simple Storage Service' (S3) verwendet, wie z. B. IBM® Cloud Object Storage oder Amazon Web Services (AWS) S3. Wenn Sie einen Speicherpool für die Verwendung von S3 mit diesem Parameter definieren, können Sie später den Speicherpooltyp mithilfe des Befehls UPDATE STGPOOL nicht ändern.

#### Softlayer

Gibt an, dass der Speicherpool ein Cloud-Computing-System 'IBM SoftLayer' (IBM Bluemix) mit einem Cloud-Computing-System 'OpenStack Swift' verwendet.

#### Swift

Gibt an, dass der Speicherpool ein Cloud-Computing-System 'OpenStack Swift' verwendet. Dieser Wert gibt auch an, dass der Speicherpool Version 2 des Protokolls für die Authentifizierung bei der Cloud verwendet. Die URL der Cloud enthält normalerweise die Versionsnummer des verwendeten Protokolls.

#### V1Swift

Gibt an, dass der Speicherpool ein Cloud-Computing-System 'OpenStack Swift' verwendet. Dieser Wert gibt auch an, dass der Speicherpool Version 1 des Protokolls für die Authentifizierung bei der Cloud verwendet. Die URL der Cloud enthält normalerweise die Versionsnummer des verwendeten Protokolls.

Dieser Parameter ist wahlfrei. Wird der Parameter nicht angegeben, wird der Standardwert SWIFT verwendet.

### CLOUDUrl

Gibt die URL der Cloudumgebung an, in der der Speicherpool konfiguriert wird. Auf der Basis Ihres Cloud-Providers können Sie einen BLOB-Dienstendpunkt, einen Regionendpunkt-URL, einen Accesser-IP-Adresse, einen Endpunkt für öffentliche Authentifizierung (Public Authentication Endpoint) oder einen ähnlichen Wert für diesen Parameter verwenden. Stellen Sie sicher, dass das Protokoll wie z. B. `https://` oder `http://` am Anfang der URL eingefügt wird. Die maximale Länge der Webadresse beträgt 870 Zeichen. Der Parameter CLOUDURL wird erst geprüft, wenn die erste Sicherung beginnt.

Weitere Informationen zum Ermitteln dieser Werte erhalten Sie, wenn Sie Ihren Cloud-Service-Provider in der Liste auf der Seite Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren auswählen.

Tipp: Um mehrere IBM Cloud Object Storage-Accesser zu verwenden, listen Sie die Accesser-IP-Adressen getrennt durch einen vertikalen Balken (|) ohne Leerzeichen auf. Beispiel:

```
CLOUDURL=<Accesser-URL1>|<Accesser-URL2>|<Accesser-URL3>
```

Falls Sie das Operations Center verwenden, geben Sie im Feld URL des Assistenten 'Speicherpool hinzufügen' eine Accesser-IP-Adresse ein und drücken Sie dann die Eingabetaste, um weitere IP-Adressen hinzuzufügen. Die Verwendung mehrerer Accesser verbessert die Leistung.

Dieser Parameter ist erforderlich, wenn Sie den Parameter CLOUDTYPE angeben.

- Azure
- S3 (Simple Storage Service)
- Softlayer
- Swift
- V1Swift

## Identity

Gibt die Benutzer-ID für die Cloud an, die im Parameter STGTYPE=CLOUD angegeben ist. Dieser Parameter ist für alle unterstützten Cloud-Computing-Systeme außer Azure erforderlich. Wenn Sie CLOUDTYPE=AZURE angegeben haben, geben Sie nicht den Parameter IDENTITY an. Auf der Basis Ihres Cloud-Providers können Sie eine Zugriffsschlüssel-ID, einen Benutzernamen, einen Tenantenamen und Benutzernamen oder einen ähnlichen Wert für diesen Parameter verwenden. Die maximale Länge der Benutzer-ID beträgt 255 Zeichen.

## PASSword (Erforderlich)

Gibt das Kennwort für die Cloud an, die im Parameter STGTYPE=CLOUD angegeben ist. Auf der Basis Ihres Cloud-Providers können Sie ein SAS-Token (SAS = Shared Access Signature), einen geheimen Zugriffsschlüssel, einen API-Schlüssel, ein Kennwort oder einen ähnlichen Wert für diesen Parameter verwenden. Dieser Parameter ist erforderlich. Die maximale Länge des Kennworts beträgt 255 Zeichen. Die Parameter IDENTITY und PASSWORD werden erst geprüft, wenn die erste Sicherung beginnt.

## CLOUDLocation

Gibt die physische Position der Cloud an, die im Parameter CLOUD angegeben ist. Dieser Parameter ist wahlfrei. Der Standardwert ist OFFPREMISE. Sie können einen der folgenden Werte angeben:

- Offpremise
- ONpremise

## BUCKETName

Gibt den Namen für ein AWS S3-Bucket oder eine IBM Cloud Object Storage-Vault an, das bzw. die anstelle des Standardbuckets oder der Standardvault mit diesem Speicherpool verwendet werden soll. Dieser Parameter ist optional und ist nur gültig, wenn Sie CLOUDTYPE=S3 angeben. Wenn der von Ihnen angegebene Name nicht vorhanden ist, erstellt der Server ein Bucket oder eine Vault mit dem angegebenen Namen, bevor das Bucket bzw. die Vault verwendet wird. Beachten Sie die Einschränkungen Ihres Cloud-Providers bei der Benennung, wenn Sie diesen Parameter angeben. Überprüfen Sie die Berechtigungen für das Bucket oder die Vault und stellen Sie sicher, dass die Berechtigungsnachweise für diesen Speicherpool über die Berechtigung zum Lesen, Schreiben, Auflisten und Löschen von Objekten in diesem Bucket oder dieser Vault haben. Wenn Sie die Berechtigungen nicht ändern oder anzeigen können und nicht bereits Daten in diesen Speicherpool geschrieben wurden, verwenden Sie den Befehl UPDATE STGPOOL mit dem Parameter BUCKETNAME, um ein anderes Bucket oder eine andere Vault zu verwenden.

## ACCess

Gibt an, wie Clientknoten und Serverprozesse auf den Cloudspeicherpool zugreifen. Dieser Parameter ist wahlfrei. Der Standardwert ist READWRITE. Sie können einen der folgenden Werte angeben:

### READWrite

Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff für den Cloudspeicherpool haben. Dieser Wert ist der Standardwert.

### READOnly

Gibt an, dass Clientknoten und Serverprozesse nur Lesezugriff für den Cloudspeicherpool haben.

### UNAVailable

Gibt an, dass Clientknoten und Serverprozesse nicht auf den Cloudspeicherpool zugreifen können.

## MAXWriters

Gibt die maximale Anzahl der Schreibsitzungen an, die gleichzeitig für den Cloudspeicherpool ausgeführt werden können. Geben Sie eine maximale Anzahl von Schreibsitzungen an, um zu steuern, dass die Leistung des Cloudspeicherpools keine negativen Auswirkungen auf andere Systemressourcen hat. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Sie können einen der folgenden Werte angeben:

### NOLimit

Gibt an, dass für die Anzahl der Writer, die Sie verwenden können, kein Grenzwert für die maximale Größe vorhanden ist. Dieser Wert ist der Standardwert.

### maximale\_Anzahl\_Writer

Begrenzt die maximale Anzahl der Writer, die Sie verwenden können. Geben Sie eine ganze Zahl im Bereich von 1 bis 99999 an.

## REUsedelay

Gibt die Anzahl Tage an, die verstreichen müssen, nachdem alle deduplizierte Speicherbereiche aus einem Cloudspeicherpool entfernt wurden. Dieser Parameter steuert die Dauer, die deduplizierte Speicherbereiche einem Cloudspeicherpool zugeordnet sind. Wenn der für den Parameter angegebene Wert abläuft, werden die deduplizierte Speicherbereiche aus dem Cloudspeicherpool gelöscht. Der Standardwert ist 1. Sie können einen der folgenden Werte angeben:

### 1

Gibt an, dass deduplizierte Speicherbereiche nach 1 Tag aus einem Cloudspeicherpool gelöscht werden. Dieser Wert ist der Standardwert.

### Tage

Sie können eine ganze Zahl im Bereich von 0 bis 9999 angeben.

Tipp: Setzen Sie diesen Parameter auf einen Wert, der größer als die für den Befehl SET DRMDBBACKUPEXPIREDDAYS angegebene Anzahl ist. Wird dieser Parameter auf einen höheren Wert gesetzt, können Sie sicherstellen, dass Verweise auf Dateien im

Cloudspeicherpool noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird.

#### ENCRypt

Gibt an, ob der Server Clientdaten verschlüsselt, bevor er sie in den Speicherpool schreibt. Sie können die folgenden Werte angeben:

Yes

Gibt an, dass Clientdaten vom Server verschlüsselt werden.

No

Gibt an, dass Clientdaten nicht vom Server verschlüsselt werden.

Dieser Parameter ist wahlfrei. Der Standardwert ist von der physischen Position der Cloud abhängig, die durch den Parameter CLOUDLOCATION angegeben wird. Wenn sich die Cloud außerhalb des Unternehmens (off premise) befindet, werden Daten standardmäßig vom Server verschlüsselt. Wenn sich die Cloud vor Ort (on premises) befindet, werden Daten standardmäßig nicht vom Server verschlüsselt.

#### COMPRession

Gibt an, ob Daten in dem Speicherpool komprimiert werden. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass Daten in dem Speicherpool nicht komprimiert werden.

Yes

Gibt an, dass Daten in dem Speicherpool komprimiert werden. Dies ist der Standardwert.

---

## Beispiel 1: Einen OpenStack Swift-Cloud-Containerspeicherpool definieren

Einen OpenStack Swift-Cloud-Containerspeicherpool mit dem Namen STGPOOL1 definieren.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=password description="OpenStack Swift cloud"
```

---

## Beispiel 2: Einen primären Cloud-Containerspeicherpool definieren

Einen primären Cloud-Containerspeicherpool mit dem Namen STGPOOL1 definieren.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 pooltype=primary
```

---

## Beispiel 3: Einen Cloud-Containerspeicherpool mit Lesezugriff definieren

Einen Cloud-Containerspeicherpool mit dem Namen STGPOOL1 mit Lesezugriff definieren.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 access=readonly
```

---

## Beispiel 4: Einen Cloud-Containerspeicherpool mit 99 Schreibsitzungen definieren

Einen Cloud-Containerspeicherpool mit dem Namen STGPOOL1 mit 99 Schreibsitzungen definieren.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 maxwr=99
```

---

## Beispiel 5: Einen Cloud-Containerspeicherpool definieren, in dem deduplizierte Speicherbereiche nach zwei Tagen gelöscht werden

Einen Cloud-Containerspeicherpool mit dem Namen STGPOOL1 definieren, in dem deduplizierte Speicherbereiche nach zwei Tagen gelöscht werden.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 reusedelay=2
```

#### Zugehörige Tasks:

Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren

#### Zugehörige Informationen:

## DEFINE STGPOOL (Verzeichniscontainerspeicherpool definieren)

Mit diesem Befehl kann ein Verzeichniscontainerspeicherpool definiert werden, der für die Dateneduplizierung verwendet wird.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DEFine STGpool--Poolname--STGType-----Directory----->
. -Pooltype-----Primary-.
>+-----+-----+-----+-----+-----+-----+-----+----->
' -Pooltype-----Primary-' ' -DESCription-----Beschreibung-'
. -ACCEss-----READWrite-----.
>+-----+-----+-----+-----+-----+-----+-----+----->
' -ACCEss-----+READWrite---+-'
      +READOnly-----+
      ' -UNAVailable-'
. -MAXSIze-----NOLimit-----.
>+-----+-----+-----+-----+-----+-----+-----+----->
' -MAXSIze-----+NOLimit-----+-'
      ' -maximale_Dateigröße-'
. -MAXWriters-----NOLimit-----.
>+-----+-----+-----+-----+-----+-----+-----+----->
' -MAXWriters-----+NOLimit-----+-'
      ' -maximale_Anzahl_Writer-'
>+-----+-----+-----+-----+-----+-----+-----+----->
' -NEXTstgpool-----Poolname-'
>+-----+-----+-----+-----+-----+-----+-----+----->
' -PROTECTstgpool-----Zielspeicherpool-'
>+-----+-----+-----+-----+-----+-----+-----+----->
|                                     .-,'-----'. |
|                                     V               | |
' -PROTECTLOCAlstgpools-----lokaler Zielspeicherpool+-'
. -REUsedelay-----1----- . -ENCRypt-----No----- .
>+-----+-----+-----+-----+-----+-----+-----+----->
' -REUsedelay-----Tage-' ' -ENCRypt-----+Yes+-'
      ' -No--'
. -COMPRession-----Yes----- .
>+-----+-----+-----+-----+-----+-----+-----+----->
' -COMPRession-----+Yes+-'
      ' -No--'
```

### Parameter

#### Poolname (Erforderlich)

Gibt den Speicherpool an, der definiert werden soll. Dieser Parameter ist erforderlich. Die maximale Länge des Namens beträgt 30 Zeichen.

#### STGType=Directory (Erforderlich)

Gibt den Typ des Speichers an, der für einen Speicherpool definiert werden soll. Dieser Parameter gibt an, dass dem Speicherpool ein Speicherpool des Typs Verzeichniscontainer zugeordnet wird. Sie müssen mit dem Befehl DEFINE STGPOOLDIRECTORY ein Speicherpoolverzeichnis für diesen Typ von Speicherpool definieren.

Voraussetzungen:

- Stellen Sie sicher, dass für den Verzeichniscontainerspeicherpool genügend Speicherbereich im Dateisystem verfügbar ist.

- Sie müssen den Verzeichniscontainerspeicherpool und die DB2-Datenbank auf separaten Mountpunkten im Dateisystem speichern. Der Verzeichniscontainerspeicherpool kann anwachsen und den gesamten Speicherbereich in dem Verzeichnis belegen, in dem er gespeichert ist.
- Sie müssen ein anderes Dateisystem als das Dateisystem verwenden, in dem sich der IBM Spectrum Protect-Server befindet.

**POoltype=PRimary**

Gibt an, dass der Speicherpool als primärer Speicherpool verwendet werden soll. Dieser Parameter ist wahlfrei.

**DEScRiption**

Gibt eine Beschreibung des Speicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält.

**ACCess**

Gibt an, wie Clientknoten und Serverprozesse auf den Speicherpool zugreifen können. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

**READWrite**

Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff für den Speicherpool haben.

**READOnly**

Gibt an, dass Clientknoten und Serverprozesse nur Lesezugriff für den Speicherpool haben.

**UNAVailable**

Gibt an, dass Clientknoten und Serverprozesse nicht auf den Speicherpool zugreifen können.

**MAXSIze**

Gibt die maximale Größe einer physischen Datei an, die der Server in dem Speicherpool speichern kann. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Sie können einen der folgenden Werte angeben:

**NOLimit**

Gibt an, dass für die im Speicherpool gespeicherten physischen Dateien keine Größenbeschränkung besteht.

**maximale\_Dateigröße**

Begrenzt die maximale Größe für physische Dateien. Geben Sie eine ganze Zahl im Bereich von 1 bis 999999 gefolgt von einem Maßstabsfaktor an. MAXSIZE=5G gibt z. B. an, dass die maximale Dateigröße für diesen Speicherpool 5 GB ist. Sie können einen der folgenden Maßstabsfaktoren verwenden:

**Tabelle 1. Maßstabsfaktor für die maximale Dateigröße**

| Maßstabsfaktor | Bedeutung |
|----------------|-----------|
| K              | Kilobyte  |
| M              | Megabyte  |
| G              | Gigabyte  |
| T              | Terabyte  |

Tipp: Wenn Sie keine Maßeinheit für die maximale Dateigröße angeben, wird der Wert in Byte angegeben.

Wenn die physische Größe des Speicherpools den Wert des Parameters MAXSIZE überschreitet, zeigt die folgende Tabelle an, wo Dateien normalerweise gespeichert werden.

**Tabelle 2. Position einer Datei gemäß der Dateigröße und dem angegebenen Pool**

| Angebener Pool  | Ergebnis   |
|---|--|
| Es ist kein Pool als nächster Speicherpool in der Hierarchie angegeben. | Die Datei wird vom Server nicht gespeichert.                                 |
| Ein Pool ist als nächster Speicherpool in der Hierarchie angegeben.     | Der Server speichert die Datei in dem Speicherpool, den Sie angegeben haben. |

Tipp: Wenn Sie auch den Parameter NEXTstgpool angeben, definieren Sie einen einzelnen Speicherpool in Ihrer Hierarchie so, dass er keine Begrenzung hinsichtlich der maximalen Dateigröße hat, indem Sie den Parameter MAXSIze=NOLimit angeben. Wenn mindestens ein Pool keine Größenbegrenzung hat, wird sichergestellt, dass der Server die Datei unabhängig von ihrer Größe speichern kann.

Werden während der Datendeduplizierungsverarbeitung mehrere Dateien gesendet, betrachtet der Server die Größe des Datendeduplizierungsprozesses als Dateigröße. Wenn die Gesamtgröße aller Dateien in dem Prozess die maximale Größe überschreitet, werden die Dateien vom Server nicht in dem Speicherpool gespeichert.

**MAXWriters**

Gibt die maximale Anzahl E/A-Threads für die folgenden Prozesse an:

- Die Anzahl E/A-Threads, die gleichzeitig für den Verzeichniscontainerspeicherpool ausgeführt werden können.



- Die Anzahl E/A-Threads, die gleichzeitig in den Verzeichniscontainerspeicherpool geschrieben werden.

Dieser Parameter ist wahlfrei. Verwenden Sie als Best Practice den Standardwert NOLIMIT. Sie können die folgenden Werte angeben:

NOLimit

Gibt an, dass keine maximale Anzahl E/A-Threads in den Speicherpool geschrieben wird.

maximale\_Anzahl\_Writer

Begrenzt die maximale Anzahl der E/A-Threads, die Sie verwenden können. Geben Sie eine ganze Zahl im Bereich von 1 bis 99999 an.

Tipp: Der IBM Spectrum Protect-Server steuert die Anzahl der E/A-Threads automatisch auf der Basis der verfügbaren Ressourcen und der Serverauslastung.

NEXTstgpool

Gibt den Namen eines Speicherpools mit wahlfreiem Zugriff oder eines primären sequenziellen Speicherpools an, in dem Dateien gespeichert werden, wenn der Verzeichniscontainerspeicherpool voll ist. Dieser Parameter ist wahlfrei.

Einschränkungen:

- Um sicherzustellen, dass keine Speicherpoolkette erstellt wird, die zu einer Endlosschleife führt, geben Sie mindestens einen Speicherpool in der Hierarchie ohne Wert an.
- Wenn Sie einen Pool mit sequenziellem Zugriff als nächsten Speicherpool angeben, muss der Pool entweder das Datenformat NATIVE oder NONBLOCK haben.
- Geben Sie keinen Verzeichniscontainer- oder Cloud-Containerspeicherpool an.
- Verwenden Sie diesen Parameter nicht, um einen Speicherpool für die Datenumlagerung anzugeben.

PROTECTstgpool

Gibt den Namen des Verzeichniscontainerspeicherpools auf dem Zielreplikationsserver an, in dem die Daten gesichert werden, wenn Sie den Befehl PROTECT STGPOOL für diesen Speicherpool verwenden. Dieser Parameter ist wahlfrei.

PROTECTLOCALstgpool

Gibt den Namen des Containerkopierspeicherpools auf einer lokalen Einheit an, in dem die Daten gesichert werden. Dieser Containerkopierspeicherpool ist ein lokaler Zielspeicherpool, wenn Sie den Befehl PROTECT STGPOOL verwenden. Sie können maximal zwei Containerkopierspeicherpoolnamen angeben. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Die maximale Länge jedes Namens beträgt 30 Zeichen. Dieser Parameter ist wahlfrei.

REUsedelay

Gibt die Anzahl Tage an, die verstreichen müssen, bevor alle deduplizierten Speicherbereiche aus einem Verzeichniscontainerspeicherpool entfernt werden. Dieser Parameter steuert die Dauer, die deduplizierte Speicherbereiche einem Verzeichniscontainerspeicherpool zugeordnet sind, nachdem sie nicht mehr referenziert werden. Wenn der für den Parameter angegebene Wert abläuft, werden die deduplizierten Speicherbereiche aus dem Verzeichniscontainerspeicherpool gelöscht. Geben Sie eine ganze Zahl im Bereich von 0 bis 9999 an. Der Standardwert für Verzeichniscontainerspeicherpools ist 1. Dies bedeutet, dass deduplizierte Speicherbereiche, die nicht mehr referenziert werden, nach 1 Tag aus einem Verzeichniscontainerspeicherpool gelöscht werden.

Setzen Sie diesen Parameter auf einen Wert, der größer als der Wert ist, der als Datenbanksicherungsperiode angegeben ist, um sicherzustellen, dass Datenbereiche noch gültig sind, wenn die Datenbank auf eine andere Stufe zurückgeschrieben wird.

ENCRypt

Gibt an, ob der Server Clientdaten verschlüsselt, bevor der Server die Daten in den Speicherpool schreibt. Sie können die folgenden Werte angeben:

Yes

Gibt an, dass Clientdaten vom Server verschlüsselt werden.

No

Gibt an, dass Clientdaten nicht vom Server verschlüsselt werden. Dies ist der Standardwert.

COMPRession

Gibt an, ob Daten in dem Speicherpool komprimiert werden. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass Daten in dem Speicherpool nicht komprimiert werden.

Yes

Gibt an, dass Daten in dem Speicherpool komprimiert werden. Dies ist der Standardwert.

**Beispiel: Einen Verzeichniscontainerspeicherpool definieren, der für Überlaufspeicher konfiguriert wird, wenn der Speicherpool voll ist**

---

Definieren Sie einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL1. Der Speicherpool wird für Überlaufspeicher in einem Bandspeicherpool konfiguriert, wenn der Speicherpool voll ist.

```
define stgpool stgpool1 stgtype=directory nextstgpool=overflow_tape_pool
```

## Beispiel: Einen Verzeichniscontainerspeicherpool definieren, der die maximale Dateigröße angibt

Definieren Sie einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL2. Der Speicherpool gibt als maximale Dateigröße 100 Megabyte an, die der Server im Speicherpool speichern kann.

```
define stgpool stgpool2 stgtype=directory maxsize=100M
```

## Beispiel: Einen Verzeichniscontainerspeicherpool auf dem Quellenreplikationsserver mit einem Verzeichniscontainerspeicherpool auf dem Zielreplikationsserver zum Sichern von Daten definieren

Definieren Sie einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL3. Die Daten für Speicherpool STGPOOL3 werden in dem Verzeichniscontainerspeicherpool TARGET\_STGPOOL3 auf dem Zielreplikationsserver gesichert.

```
define stgpool stgpool3 stgtype=directory protectstgpool=target_stgpool3
```

## Beispiel: Einen Verzeichniscontainerspeicherpool auf dem Quellenreplikationsserver mit einem Containerkopierspeicherpool definieren, um Daten lokal zu sichern

Definieren Sie einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL3. Die Daten für Speicherpool STGPOOL3 werden in dem lokalen Containerkopierspeicherpool TARGET\_LOCALSTGPOOL gesichert.

```
define stgpool stgpool3 stgtype=directory protectlocalstgpools=target_localstgpool
```

## Beispiel: Einen Verzeichniscontainerspeicherpool definieren und die Komprimierung inaktivieren

Definieren Sie einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL1 und inaktivieren Sie die Komprimierung.

```
define stgpool stgpool1 stgtype=directory compression=no
```

Tabelle 3. Zugehörige Befehle für DEFINE STGPOOL (Verzeichniscontainerspeicherpool definieren)

| Befehl                                | Beschreibung  |
|---------------------------------------|---|
| DEFINE STGPOOLDIRECTORY               | Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool. |
| PROTECT STGPOOL                       | Schützt einen Verzeichniscontainerspeicherpool.   |
| QUERY CONTAINER                       | Zeigt Informationen zu einem Container an.  |
| QUERY STGPOOL                         | Zeigt Informationen zu Speicherpools an.  |
| REPAIR STGPOOL                        | Repariert einen Verzeichniscontainerspeicherpool.   |
| UPDATE STGPOOL (Verzeichniscontainer) | Aktualisiert einen Verzeichniscontainerspeicherpool.  |

## DEFINE STGPOOL (Containerkopierspeicherpool definieren)

Mit diesem Befehl kann ein Containerkopierspeicherpool definiert werden, in dem eine Kopie der Daten aus einem Verzeichniscontainerspeicherpool gespeichert wird.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DEFine STGpool--Poolname--Einheitenklassename----->
>--POOLtype-----COPYCONTainer--MAXSCRatch-----Anzahl----->
>--+-----+----->
```



Gibt an, dass der Server nicht auf Daten zugreifen kann, die auf Datenträgern im Speicherpool gespeichert sind.

#### PROTECTProcess

Gibt die maximale Anzahl paralleler Prozesse an, die verwendet werden, wenn Sie den Befehl PROTECT STGPOOL ausgeben, um Daten aus einem Verzeichniscontainerspeicherpool in diesen Pool zu kopieren. Dieser Parameter ist wahlfrei. Geben Sie einen Wert im Bereich von 1 bis 20 ein. Der Standardwert ist 2.

Die Zeit, die für die Ausführung der Kopieroperation erforderlich ist, kann durch die Verwendung mehrerer Prozesse verringert werden. Sind mehrere Prozesse aktiv, müssen jedoch in einigen Fällen ein oder mehrere Prozesse auf die Verwendung eines Datenträgers warten, der bereits von einem anderen Prozess verwendet wird.

Berücksichtigen Sie bei der Angabe dieses Werts die Anzahl der logischen und physischen Laufwerke, die der Kopieroperation zugeordnet werden können. Für den Zugriff auf einen Banddatenträger verwendet der Server einen Mountpunkt und ein Laufwerk. Die Anzahl verfügbarer Mountpunkte und Laufwerke ist von dem Mountlimit der Einheitenklasse für den Speicherpool und von anderen Server- und Systemaktivitäten abhängig.

Dieser Parameter wird ignoriert, wenn Sie die Option PREVIEW=YES im Befehl PROTECT STGPOOL verwenden. In diesem Fall wird nur ein Prozess verwendet und es werden keine Mountpunkte oder Laufwerke benötigt.

#### REClaim

Gibt an, wann ein Datenträger für die Konsolidierung und Wiederverwendung auswählbar ist. Geben Sie die Auswählbarkeit als Prozentsatz des Speicherbereichs eines Datenträgers an, der von Bereichen belegt ist, die nicht mehr im zugeordneten Verzeichniscontainerspeicherpool gespeichert werden. Bei der Konsolidierung werden alle Bereiche, die noch im zugeordneten Verzeichniscontainerspeicherpool gespeichert werden, von auswählbaren Datenträgern auf andere Datenträger versetzt. Die Konsolidierung erfolgt nur, wenn mit einem Befehl PROTECT STGPOOL Daten in diesem Speicherpool gespeichert werden.

Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl im Bereich von 1 bis 100 angeben. Der Standardwert 100 bedeutet, dass keine Datenträger in diesem Speicherpool konsolidiert werden.

Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

Wird der Wert für 'Reclaim' auf 50 Prozent oder höher gesetzt, belegen Daten, die von zwei konsolidierten Datenträgern versetzt werden, maximal das Äquivalent eines neuen Datenträgers.

Gehen Sie mit Vorsicht vor, wenn Sie die Konsolidierung mit Containerkopierspeicherpools verwenden, die über ausgelagerte Datenträger verfügen. Wenn ein ausgelagerter Datenträger für die Konsolidierung auswählbar wird, werden die Bereiche auf dem Datenträger vom Server an den Standort vor Ort zurückversetzt. Wenn vor Ort ein Katastrophenfall eintritt, kann der Server Bereiche vom ausgelagerten Datenträger anfordern, wenn die zurückgeschriebene Datenbank auf Bereiche auf dem ausgelagerten Datenträger verweist. Stellen Sie daher zu Zwecken der Wiederherstellung nach einem Katastrophenfall sicher, dass Sie die Ausführung von Datenbanksicherungen planen, nachdem Speicherpoolschutzzeitpläne und DRM-Versetzungszeitpläne ausgeführt wurden, und stellen Sie sicher, dass alle Datenbanksicherungsdatenträger zusammen mit den DRM-Datenträgern ausgelagert werden.

Tipp: Definieren Sie verschiedene Konsolidierungswerte für Containerkopierspeicherpools an einem anderen Standort und Containerkopierspeicherpools vor Ort. Da Containerkopierspeicherpools deduplizierte Daten speichern, sind die Datenbereiche auf mehrere Banddatenträger verteilt. Wenn Sie einen Schwellenwert für die Konsolidierung für eine Kopie an einem anderen Standort auswählen, beachten Sie sorgfältig die Anzahl verfügbarer Mountpunkte und die Anzahl Banddatenträger, die abgerufen werden müssen, wenn ein Katastrophenfall eintritt. Wird ein höherer Schwellenwert definiert, bedeutet dies, dass Sie mehr Datenträger abrufen müssen als bei einem niedrigeren Konsolidierungswert. Bei Verwendung eines niedrigeren Schwellenwerts wird die Anzahl der Mountpunkte reduziert, die in einem Katastrophenfall erforderlich sind. Die bevorzugte Methode ist die Angabe des Konsolidierungswerts 60 für Kopien an einem anderen Standort. Für Kopien vor Ort liegt er im Bereich von 90 bis 100.

#### RECLAIMLimit

Gibt die maximale Anzahl von Datenträgern an, die der Server konsolidiert, wenn Sie den Befehl PROTECT STGPOOL ausgeben und die Option RECLAIM=YESLIMITED oder RECLAIM=ONLYLIMITED angeben. Dieser Parameter ist nur für Containerkopierspeicherpools gültig. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Sie können einen der folgenden Werte angeben:

#### NOLimit

Gibt an, dass alle Datenträger im Containerkopierspeicherpool für die Konsolidierung verarbeitet werden.

#### Datenträgergrenzwert

Gibt die maximale Anzahl der Datenträger im Containerkopierspeicherpool an, die konsolidiert werden. Der von Ihnen angegebene Wert bestimmt, wie viele neue Arbeitsbänder nach Abschluss der Konsolidierungsverarbeitung verfügbar sind. Sie können eine Zahl im Bereich von 1 bis 100000 angeben.

#### REUsedelay

Gibt die Anzahl Tage an, die nach dem Löschen aller Bereiche von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerstatus versetzt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl im Bereich von 0 bis 9999 angeben. Der Standardwert ist 0, was bedeutet, dass ein Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerstatus versetzt werden kann, sobald alle Bereiche auf dem Datenträger gelöscht wurden. Tipp: Mit diesem Parameter kann sichergestellt werden, dass Datenbankverweise auf Bereiche im Speicherpool noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird. Dieser Parameter muss auf einen Wert gesetzt werden, der größer als die Anzahl der Tage ist, die die älteste Datenbanksicherung aufbewahrt werden soll. Wenn Sie Disaster Recovery Manager verwenden, muss die für diesen Parameter angegebene Anzahl Tage mit der für den Befehl SET DRMDBBACKUPEXPIREDDAYS angegebenen Anzahl übereinstimmen.

## Beispiel: Einen Containerkopierspeicherpool mit einer Einheitenklasse LTO7A definieren

Den Containerkopierspeicherpool CONTAINER1\_COPY2 für die Einheitenklasse LTO7A definieren. Maximal 50 Arbeitsdatenträger für diesen Pool zulassen. Die Wiederverwendung der Datenträger um 45 Tage verzögern.

```
define stgpool container1_copy2 lto7a pooltype=copycontainer
maxscratch=50 reusedelay=45
```

Tabelle 1. Zugehörige Befehle für DEFINE STGPOOL (Containerkopierspeicherpool definieren)

| Befehl                                | Beschreibung   |
|---------------------------------------|--|
| DEFINE STGPOOL (Verzeichniscontainer) | Definiert einen Verzeichniscontainerspeicherpool.  |
| PROTECT STGPOOL                       | Schützt einen Verzeichniscontainerspeicherpool.  |
| QUERY STGPOOL                         | Zeigt Informationen zu Speicherpools an.   |
| REPAIR STGPOOL                        | Repariert einen Verzeichniscontainerspeicherpool.  |
| UPDATE STGPOOL (Containerkopie)       | Aktualisiert einen Containerkopierspeicherpool, in dem Kopien von Daten aus einem Verzeichniscontainerspeicherpool gespeichert werden. |
| UPDATE STGPOOL (Verzeichniscontainer) | Aktualisiert einen Verzeichniscontainerspeicherpool.   |

## DEFINE STGPOOL (Primären Speicherpool definieren, der Einheiten mit wahlfreiem Zugriff zugeordnet wird)

Mit diesem Befehl kann ein primärer Speicherpool definiert werden, der Einheiten mit wahlfreiem Zugriff zugeordnet wird.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```

                                .-Pooltype-----Primary-.
>>-DEFine STGpool--Poolname--DISK--+-----+-----+----->
                                '-Pooltype-----Primary-'

    .-STGType-----Devclass-.
>--+-----+-----+-----+-----+-----+----->
    '-STGType-----Devclass-' '-DESCription-----Beschreibung-'

    .-ACCess-----READWrite------.
>--+-----+-----+-----+-----+-----+----->
    '-ACCess-----+READWrite---+'
                                +-READOnly-----+
                                '-UNAVailable-'

    .-MAXSIze-----NOLimit------.
>--+-----+-----+-----+-----+-----+----->
    '-MAXSIze-----maximale_Dateigröße-'

    .-CRCData-----No------.
>--+-----+-----+-----+-----+-----+----->
    '-CRCData-----+Yes--+-' '-NEXTstgpool-----Poolname-'
                                '-No--'
```



Gibt an, dass Clientknoten Dateien auf den Datenträgern im Speicherpool nur lesen können.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Für die Datenträger in dem Speicherpool sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig.

Wenn dieser Speicherpool als untergeordneter Speicherpool angegeben (mit dem Parameter NEXTSTGPOOL) und als *readonly (schreibgeschützt)* definiert wurde, wird der Speicherpool übersprungen, wenn Serverprozesse versuchen, Dateien in den Speicherpool zu schreiben.

#### UNAVailable

Gibt an, dass Clientknoten nicht auf Dateien, die auf Datenträgern im Speicherpool gespeichert sind, zugreifen können.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Außerdem können sie Dateien aus diesem Speicherpool in einen anderen Speicherpool versetzen oder kopieren. Für die Datenträger in dem Speicherpool sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig.

Wenn dieser Speicherpool als untergeordneter Speicherpool angegeben (mit dem Parameter NEXTSTGPOOL) und als *unavailable (nicht verfügbar)* definiert wurde, wird der Speicherpool übersprungen, wenn Serverprozesse versuchen, Dateien in den Speicherpool zu schreiben.

#### MAXSize

Gibt die maximale Größe einer physischen Datei an, die der Server in dem Speicherpool speichern kann. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Sie können die folgenden Werte angeben:

#### NOLimit

Gibt an, dass für die im Speicherpool gespeicherten physischen Dateien keine Größenbeschränkung besteht.

#### maximale\_Dateigröße

Begrenzt die maximale Größe für physische Dateien. Geben Sie eine ganze Zahl zwischen 1 und 999999 Terabyte gefolgt von einem Maßstabsfaktor an. MAXSIZE=5G gibt z. B. an, dass die maximale Dateigröße für diesen Speicherpool 5 GB ist. Sie können einen der folgenden Maßstabsfaktoren verwenden:

| Maßstabsfaktor | Bedeutung |
|----------------|-----------|
| K              | Kilobyte  |
| M              | Megabyte  |
| G              | Gigabyte  |
| T              | Terabyte  |

Der Client schätzt die Größe der Dateien, die an den Server gesendet werden. Die Schätzung des Clients wird verwendet und nicht das tatsächliche Datenvolumen, das an den Server gesendet wird. Clientoptionen, wie z. B. Deduplizierung, Komprimierung und Verschlüsselung, können zur Folge haben, dass das tatsächliche Datenvolumen, das an den Server gesendet wird, größer oder kleiner als die Größenschätzung ist. Beispielsweise kann eine komprimierte Datei kleiner als die Schätzung sein, sodass weniger Daten als der Schätzwert gesendet werden. Des Weiteren kann eine Binärdatei nach der Komprimierungsverarbeitung größer sein, sodass mehr Daten als der Schätzwert gesendet werden.

Wenn die physische Größe des Speicherpools den Wert des Parameters MAXSIZE überschreitet, zeigt die folgende Tabelle an, wo Dateien normalerweise gespeichert werden.

Tabelle 1. Position einer Datei gemäß der Dateigröße und dem angegebenen Pool

| Dateigröße                       | Angegebener Pool   | Ergebnis   |
|----------------------------------|--|--|
| Überschreitet die maximale Größe | Es ist kein Pool als nächster Speicherpool in der Hierarchie angegeben | Die Datei wird vom Server nicht gespeichert  |
|                                  | Ein Pool ist als nächster Speicherpool in der Hierarchie angegeben     | Der Server speichert die Datei im nächsten Speicherpool, der die Dateigröße akzeptiert |

Tipp: Wenn Sie auch den Parameter NEXTstgpool angeben, definieren Sie einen einzelnen Speicherpool in Ihrer Hierarchie so, dass er keine Begrenzung hinsichtlich der maximalen Dateigröße hat, indem Sie den Parameter MAXSize=NOLimit angeben. Wenn mindestens ein Pool keine Größenbegrenzung hat, wird sichergestellt, dass der Server die Datei unabhängig von ihrer Größe speichern kann.

Bei mehreren Dateien, die in einer einzelnen Transaktion gesendet werden, betrachtet der Server die Größe der Transaktion als Dateigröße. Wenn die Gesamtgröße aller Dateien in der Transaktion die maximale Größe überschreitet, werden die Dateien vom Server nicht in dem Speicherpool gespeichert.

#### CRCData

Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCData

auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

Yes

Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da mehr Aufwand erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

No

Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

#### NEXTStgpool

Gibt einen primären Speicherpool an, in den Dateien umgelagert werden. Dieser Parameter ist wahlfrei.

Wird kein nächster Speicherpool angegeben, gilt Folgendes:

- Der Server kann keine Dateien aus diesem Speicherpool umlagern
- Der Server kann keine Dateien, die die maximale Größe für diesen Speicherpool überschreiten, in einem anderen Speicherpool speichern

Einschränkungen:

- Um sicherzustellen, dass keine Speicherpoolkette erstellt wird, die zu einer Endlosschleife führt, geben Sie mindestens einen Speicherpool in der Hierarchie ohne Wert an.
- Wenn Sie einen Pool mit sequenziellem Zugriff als nächsten Speicherpool angeben, muss der Pool entweder das Datenformat NATIVE oder NONBLOCK haben.
- Geben Sie keinen Verzeichniscontainer- oder Cloud-Containerspeicherpool an.
- Verwenden Sie diesen Parameter nicht, um einen Speicherpool für die Datenumlagerung anzugeben.

#### Highmig

Gibt an, dass der Server die Umlagerung für diesen Speicherpool startet, wenn der Datenumfang in dem Pool diesen Prozentsatz der geschätzten Kapazität des Pools erreicht. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 100 angeben. Der Standardwert ist 90.

Wenn der Speicherpool die obere Umlagerungsschwelle überschreitet, kann der Server die Umlagerung von Dateien in den nächsten Speicherpool nach Knoten starten. Der Parameter NEXTSTGPOOL definiert diese Einstellung. Sie können HIGHMIG=100 angeben, um die Umlagerung für diesen Speicherpool zu verhindern.

#### Lowmig

Gibt an, dass der Server die Umlagerung für diesen Speicherpool stoppt, wenn der Datenumfang in dem Pool diesen Prozentsatz der geschätzten Kapazität des Pools erreicht. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 99 angeben. Der Standardwert ist 70.

Wenn die Umlagerung nach Knoten oder Dateibereich erfolgt (abhängig von der Kollokation), kann der Wert für den Speicherpool unter den für diesen Parameter angegebenen Wert fallen. Um den Speicherpool zu leeren, definieren Sie LOWMIG=0.

#### CACHe

Gibt an, ob der Umlagerungsprozess eine Cachekopie einer Datei in diesem Speicherpool zurücklässt, nachdem die Datei in den nächsten Speicherpool umgelagert wurde. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können die folgenden Werte angeben:

Yes

Caching ist aktiviert.

No

Caching ist inaktiviert.

Die Verwendung von Cache kann die Abrufbarkeit von Dateien verbessern, kann jedoch die Leistung anderer Prozesse negativ beeinflussen.

#### MIGPRocess

Gibt die Anzahl der Prozesse an, die der Server zum Umlagern von Dateien aus diesem Speicherpool verwendet. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 999 angeben. Der Standardwert ist 1.

Während der Umlagerung werden diese Prozesse parallel ausgeführt, um die Umlagerungsgeschwindigkeit zu verbessern.

Tipps:

- Die Anzahl der Umlagerungsprozesse ist von den folgenden Einstellungen abhängig:
  - Einstellung des Parameters MIGPROCESS
  - Kollokationseinstellung des nächsten Pools
  - Anzahl der Knoten oder Anzahl der Kollokationsgruppen mit Daten in dem Speicherpool, der umgelagert wird



Beispiel: Angenommen, dass `MIGPROCESS =6` angegeben und der Parameter `COLLOCATE` für den nächsten Pool auf `NODE` gesetzt ist, aber nur zwei Knoten mit Daten in dem Speicherpool vorhanden sind. Die Umlagerungsverarbeitung besteht nur aus zwei, nicht sechs Prozessen. Wird der Parameter `COLLOCATE` auf `GROUP` gesetzt und befinden sich beide Knoten in derselben Gruppe, besteht die Umlagerungsverarbeitung nur aus einem Prozess. Wird der Parameter `COLLOCATE` auf `NO` oder `FILESPEC` gesetzt und hat jeder Knoten zwei Dateibereiche mit Sicherungsdaten, besteht die Umlagerungsverarbeitung aus vier Prozessen.

- Beachten Sie bei der Angabe dieses Parameters, ob die Funktion für simultanes Schreiben für die Serverdatenumlagerung aktiviert ist. Jeder Umlagerungsprozess erfordert einen Mountpunkt und ein Laufwerk für jeden Kopienspeicherpool und Pool für aktive Daten, der für den Zielspeicherpool definiert ist.

#### MIGDelay

Gibt die Mindestanzahl Tage an, die eine Datei in einem Speicherpool verbleiben muss, bevor sie für die Umlagerung ausgewählt werden kann. Um einen Wert zu berechnen, der mit dem angegebenen Wert für `MIGDELAY` verglichen wird, zählt der Server:

- Die Anzahl der Tage, die die Datei im Speicherpool war
- Die Anzahl der Tage (falls zutreffend), seit die Datei von einem Client abgerufen wurde

Der kleinere der beiden Werte wird mit dem angegebenen Wert für `MIGDELAY` verglichen. Beispiel: Sind alle folgenden Bedingungen wahr, wird eine Datei nicht umgelagert:

- Eine Datei war fünf Tage in einem Speicherpool.
- Auf die Datei wurde innerhalb der letzten drei Tage von einem Client zugegriffen.
- Der für den Parameter `MIGDELAY` angegebene Wert beträgt vier Tage.

Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Standardwert 0 gibt an, dass die Umlagerung nicht verzögert werden soll.

Soll der Server die Anzahl der Tage ab dem Tag zählen, an dem eine Datei gespeichert wurde, und nicht ab dem Tag, an dem sie abgerufen wurde, die Serveroption `NORETRIEVEDATE` verwenden.

#### MIGContinue

Gibt an, ob der Server Dateien umlagern darf, die der Verzögerungszeit für die Umlagerung nicht entsprechen. Dieser Parameter ist wahlfrei. Der Standardwert ist `YES`.

Da angegeben werden kann, dass Dateien eine Mindestanzahl Tage in dem Speicherpool verbleiben müssen, kann der Server alle auswählbaren Dateien in den nächsten Speicherpool umlagern, obwohl sie dem Wert für die untere Umlagerungsschwelle nicht entsprechen. Mit diesem Parameter kann angegeben werden, ob der Server den Umlagerungsprozess fortsetzen darf, indem Dateien umgelagert werden, die der Verzögerungszeit für die Umlagerung nicht entsprechen.

Sie können einen der folgenden Werte angeben:

##### Yes

Muss die untere Umlagerungsschwelle eingehalten werden, gibt dieser Wert an, dass der Server mit der Umlagerung von Dateien fortfährt, die der Verzögerungszeit für die Umlagerung nicht entsprechen.

Sind mehrere Umlagerungsprozesse für den Speicherpool zulässig, werden einige Dateien, die der Verzögerungszeit für die Umlagerung nicht entsprechen, unter Umständen unnötigerweise umgelagert. Während ein Prozess Dateien umlagert, die der Verzögerungszeit für die Umlagerung entsprechen, könnte ein zweiter Prozess mit der Umlagerung von Dateien beginnen, die der Verzögerungszeit für die Umlagerung nicht entsprechen, um die untere Umlagerungsschwelle einzuhalten. Der erste Prozess, der noch Dateien umlagert, die der Verzögerungszeit für die Umlagerung entsprechen, könnte selbst die Einhaltung der unteren Umlagerungsschwelle bewirkt haben.

##### No

Gibt an, dass der Server die Umlagerung stoppt, wenn keine auswählbaren Dateien mehr für die Umlagerung verfügbar sind; dies gilt auch vor Erreichen der unteren Umlagerungsschwelle. Der Server lagert nur Dateien um, die der Verzögerungszeit für die Umlagerung entsprechen.

#### AUTOCopy

Gibt an, wann IBM Spectrum Protect Operationen mit simultanem Schreiben ausführt. Der Standardwert ist `CLIENT`. Dieser Parameter ist wahlfrei und betrifft die folgenden Operationen:

- Clientspeichersitzungen
- Serverimportprozesse
- Serverdatenumlagerungsprozesse

Tritt ein Fehler auf, wenn Daten während eines Umlagerungsprozesses gleichzeitig in einen Kopienspeicherpool oder einen Pool für aktive Daten geschrieben werden, stoppt der Server das Schreiben in die fehlerhaften Speicherpools für den Rest des Prozesses. Der Server speichert jedoch weiterhin Dateien in dem primären Speicherpool und in allen verbleibenden Kopienspeicherpools oder Pools für aktive Daten. Diese Pools bleiben für die Dauer des Umlagerungsprozesses aktiv.

Kopienspeicherpools werden mit dem Parameter COPYSTGPOOLS angegeben. Pools für aktive Daten werden mit dem Parameter ACTIVEPOOLSDATA angegeben.

Sie können einen der folgenden Werte angeben:

None

Gibt an, dass die Funktion für simultanes Schreiben inaktiviert ist.

Client

Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen oder Serverimportprozessen gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverimportprozessen werden Daten nur gleichzeitig in Kopienspeicherpools geschrieben. Daten werden während der Ausführung von Serverimportprozessen nicht in Pools für aktive Daten geschrieben.

MIGRATION

Gibt an, dass Daten nur während der Umlagerung in diesen Speicherpool gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverdatenumlagerungsprozessen werden Daten in Kopienspeicherpools und Pools für aktive Daten nur dann gleichzeitig geschrieben, wenn die Daten in diesen Pools nicht vorhanden sind. Knoten, deren Daten umgelagert werden, müssen sich in einer Domäne befinden, die einem Pool für aktive Daten zugeordnet ist. Befinden sich die Knoten nicht in einer Domäne, die einem Pool für aktive Daten zugeordnet ist, können die Daten nicht in den Pool geschrieben werden.

All

Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen, Serverimportprozessen oder Serverdatenumlagerungsprozessen gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Mit diesem Wert wird sichergestellt, dass Daten immer dann gleichzeitig geschrieben werden, wenn dieser Pool ein Ziel für eine der auswählbaren Operationen ist.

COPYSTGpools

Gibt die Namen von Kopienspeicherpools an, in die der Server gleichzeitig Daten schreibt. Der Parameter COPYSTGPOOLS ist optional. Sie können maximal drei Kopienpoolnamen angeben, die durch Kommas voneinander getrennt werden müssen. Leerzeichen zwischen den Namen der Kopienpools sind nicht zulässig. Wenn Sie einen Wert für den Parameter COPYSTGPOOLS angeben, können Sie auch einen Wert für den Parameter COPYCONTINUE angeben.

Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSTGPOOLS und ACTIVEPOOLSDATA angegeben sind, darf drei nicht überschreiten.

Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Kopienspeicherpools und den Wert für COPYCONTINUE aus dem primären Speicherpool. Der primäre Speicherpool wird durch die Kopiergruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

Der Server kann während der Ausführung der folgenden Operationen Daten gleichzeitig in Kopienspeicherpools schreiben:

- Sicherungs- und Archivierungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder Anwendungsclients, die die IBM Spectrum Protect-API verwenden
- Umlagerungsoperationen durch IBM Spectrum Protect for Space Management-Clients
- Importoperationen, die das Kopieren von exportierten Dateidaten von externen Datenträgern in einen primären Speicherpool einbeziehen, der einer Kopienspeicherpoolliste zugeordnet ist

Einschränkung: Die Funktion für simultanes Schreiben wird für die folgenden Speicheroperationen nicht unterstützt:

- Wenn die Operation die LAN-unabhängige Datenversetzung verwendet. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch berücksichtigt.
- NAS-Sicherungsoperationen. Sind für den primären Speicherpool, der in DESTINATION oder TOCDESTINATION in der Kopiergruppe der Verwaltungsklasse angegeben ist, Kopienspeicherpools definiert, werden
  - die Kopienspeicherpools ignoriert.
  - die Daten nur im primären Speicherpool gespeichert.

Achtung: Die mit dem Parameter COPYSTGPOOLS zur Verfügung gestellte Funktion soll nicht den Befehl BACKUP STGPOOL ersetzen. Wird der Parameter COPYSTGPOOLS verwendet, verwenden Sie weiterhin den Befehl BACKUP STGPOOL, um sicherzustellen, dass die Kopienspeicherpools vollständige Kopien des primären Speicherpools sind. Es gibt Fälle, in denen eine Kopie möglicherweise nicht erstellt wird. Weitere Informationen enthält die Beschreibung des Parameters COPYCONTINUE.

COPYContinue

Gibt an, wie der Server normalerweise auf einen Fehler beim Schreiben in einen der Kopienspeicherpools reagiert, die im Parameter COPYSTGPOOLS aufgelistet sind. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Wenn Sie den Parameter COPYCONTINUE angeben, müssen Sie auch den Parameter COPYSTGPOOLS angeben.

Sie können die folgenden Werte angeben:

Yes

Ist der Parameter COPYCONTINUE auf YES gesetzt, stoppt der Server das Schreiben in die fehlerhaften Kopienpools für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Kopienpools fort. Die Liste der Kopienspeicherpools ist nur für die Dauer der Clientsitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.

No

Ist der Parameter COPYCONTINUE auf NO gesetzt, wird die aktuelle Transaktion vom Server nicht ausgeführt und die Speicheroperation nicht fortgesetzt.

Einschränkungen:

- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf Pools für aktive Daten. Tritt für einen der Pools für aktive Daten ein Schreibfehler auf, stoppt der Server das Schreiben in den fehlerhaften Pool für aktive Daten für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Pools für aktive Daten und Kopienspeicherpools fort. Die Liste der Pools für aktive Daten ist nur für die Dauer der Sitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.
- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Ausführung eines Serverimportprozesses. Werden Daten gleichzeitig geschrieben und tritt für den primären Speicherpool oder einen Kopienspeicherpool ein Schreibfehler auf, schlägt der Serverimportprozess fehl.
- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Serverdatenumlagerung. Werden Daten gleichzeitig geschrieben und tritt für einen Kopienspeicherpool oder Pool für aktive Daten ein Schreibfehler auf, wird der fehlerhafte Speicherpool entfernt und der Datenumlagerungsprozess wird fortgesetzt. Bei Schreibfehlern für den primären Speicherpool schlägt der Umlagerungsprozess fehl.

#### ACTIVEDATApools

Gibt die Namen der Pools für aktive Daten an, in die der Server während einer Clientsicherungsoperation gleichzeitig Daten schreibt. Der Parameter ACTIVEDATAPOOLS ist optional. Leerzeichen zwischen den Namen der Pools für aktive Daten sind nicht zulässig.

Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSGTPOOLS und ACTIVEDATAPOOLS angegeben sind, darf drei nicht überschreiten.

Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Pools für aktive Daten aus dem Zielspeicherpool, der in der Kopiengruppe angegeben ist. Der primäre Speicherpool wird durch die Kopiengruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

Der Server kann nur während Sicherungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder durch Anwendungsclients, die die IBM Spectrum Protect-API verwenden, Daten gleichzeitig in Pools für aktive Daten schreiben.

Einschränkungen:

1. Dieser Parameter ist nur für primäre Speicherpools verfügbar, die das Datenformat "NATIVE" oder "NONBLOCK" verwenden. Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP
2. Das simultane Schreiben in Pools für aktive Daten wird nicht unterstützt, wenn die LAN-unabhängige Datenversetzung verwendet wird. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch berücksichtigt.
3. Die Funktion für simultanes Schreiben wird nicht unterstützt, wenn eine NAS-Sicherungsoperation eine Inhaltsverzeichnisdatei schreibt. Sind für den primären Speicherpool, der in TOCDESTINATION in der Kopiengruppe der Verwaltungsklasse angegeben ist, Pools für aktive Daten definiert, werden
  - die Pools für aktive Daten ignoriert.
  - die Daten nur im primären Speicherpool gespeichert.
4. Die Funktion für simultanes Schreiben kann mit CENTERA-Speichereinheiten nicht verwendet werden.
5. Daten, die importiert werden, werden nicht in Pools für aktive Daten gespeichert. Verwenden Sie nach einer Importoperation den Befehl COPY ACTIVEDATA, um die importierten Daten in einem Pool für aktive Daten zu speichern.

Achtung: Die mit dem Parameter ACTIVEDATAPOOLS zur Verfügung gestellte Funktion soll nicht den Befehl COPY ACTIVEDATA ersetzen. Wird der Parameter ACTIVEDATAPOOLS verwendet, verwenden Sie den Befehl COPY ACTIVEDATA, um sicherzustellen, dass die Pools für aktive Daten alle aktiven Daten des primären Speicherpools enthalten.

#### SHRED

Gibt an, ob Daten beim Löschen physisch überschrieben werden. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 10 angeben. Der Standardwert ist 0.

Wird der Wert Null angegeben, löscht der Server die Daten aus der Datenbank. Der Speicher, in dem die Daten gespeichert waren, wird jedoch nicht überschrieben, und die Daten sind weiterhin im Speicher vorhanden, bis dieser Speicher für andere Daten wiederverwendet wird. Möglicherweise können die Daten nach dem Löschen erkannt und wiederhergestellt werden.

Wenn Sie einen Wert größer als Null angeben, löscht der Server die Daten sowohl logisch als auch physisch. Der Server überschreibt den Speicher, in dem die Daten gespeichert waren, so oft wie angegeben wurde. Durch das Überschreiben wird es schwieriger, die Daten zu erkennen und wiederherzustellen, nachdem sie gelöscht wurden.

Um sicherzustellen, dass alle Kopien der Daten geschreddert werden, geben Sie einen SHRED-Wert größer als Null für den im Parameter NEXTSTGPOOL angegebenen Speicherpool an. Geben Sie nicht COPYSTGPOOLS oder ACTIVEDATAPOOLS an. Durch die Angabe relativ hoher Werte für die Anzahl Überschreibungen wird im Allgemeinen die Sicherheitsstufe erhöht, aber sie kann umgekehrt die Leistung beeinflussen.

Das Überschreiben gelöschter Daten wird asynchron ausgeführt, nachdem die Löschoption abgeschlossen ist. Daher bleibt der durch die gelöschten Daten belegte Speicherbereich für einige Zeit belegt. Der Speicherbereich ist nicht als freier Speicherbereich für neue Daten verfügbar.

Ein SHRED-Wert größer als null kann nicht verwendet werden, wenn der Parameter CACHE den Wert YES hat.

Wichtig: Nachdem eine Exportoperation die Identifizierung von Dateien für den Export beendet hat, werden alle Änderungen des Werts SHRED für den Speicherpool ignoriert. Eine Exportoperation, die ausgesetzt ist, behält während der gesamten Operation den ursprünglichen SHRED-Wert. Möglicherweise möchten Sie Ihre Exportoperation abbrechen, wenn Änderungen des Werts SHRED für den Speicherpool die Operation gefährden. Sie können den Exportbefehl nach einer erforderlichen Bereinigung erneut ausgeben.

## Beispiel: Einen primären Speicherpool für eine Einheitenklasse DISK definieren

Den primären Speicherpool POOL1 für die Verwendung der Einheitenklasse DISK mit aktiviertem Caching definieren. Die maximale Dateigröße auf 5 MB begrenzen. Alle Dateien, die größer sind als 5 MB, in untergeordneten Speicherpools speichern (beginnend bei Speicherpool PROG2). Die obere Umlagerungsschwelle auf 70 Prozent und die untere Umlagerungsschwelle auf 30 Prozent setzen.

```
define stgpool pool1 disk
description="main disk storage pool" maxsize=5m
highmig=70 lowmig=30 cache=yes
nextstgpool=prog2
```

## DEFINE STGPOOL (Primären Speicherpool definieren, der Einheiten mit sequenziellem Zugriff zugeordnet wird)

Mit diesem Befehl kann ein primärer Speicherpool definiert werden, der Einheiten mit sequenziellem Zugriff zugeordnet wird.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DEFine STGpool--Poolname--Einheitenklassenname----->
. -Pooltype----Primary-. . -STGType----Devclass-.
>--+-----+----->
' -Pooltype----Primary-' ' -STGType----Devclass-'

>--+-----+----->
' -DESCription----Beschreibung-'

. -ACCess----READWrite-----.
>--+-----+----->
' -ACCess----+READWrite---+
                +-READOnly----+
                ' -UNAVailable-'

. -MAXSIze----NOLimit----- .
>--+-----+----->
|                                     (1) (2) |
' -MAXSIze----maximale_Dateigröße-----'

. -CRCData----No----- .
>--+-----+----->
' -CRCData----+Yes---+
                | (1) |
                ' -No-----'
```

```

>----->
|                (1) (2) |
'-NEXTstgpool----Poolname-----'

.-Highmig----90-----
>----->
|                (1) (2) |
'-Highmig----Prozent-----'

.-Lowmig----70-----
>----->
|                (1) (2) |
'-Lowmig----Prozent-----'

.-REclaim----60-----
>----->
|                (1) (2) |
'-REclaim----Prozent-----'

.-RECLAIMProcess---1-----
>----->
|                (1) (2) |
'-RECLAIMProcess---Anzahl-----'

>----->
|                (1) (2) |
'-RECLAIMSTGpool---Poolname-----'

.-RECLAMATIONType---THRESHold-----
>----->
|                (1) (2) (3) |
'-RECLAMATIONType---+THRESHold+-----'
|                '-SNAPlock--'

.-COLlocate---Group-----
>----->
|                (2) |
'-COLlocate---+No-----'
|                +-Group-----+
|                +-NODE-----+
|                '-Filespace-'

(2) .-REUsedelay---0-----
>--MAXSCRatch---Anzahl----->
|                (2) |
|                '-REUsedelay---Tage-----'

>----->
|                (1) (2) |
'-OVFLocation---Standort-----'

.-MIGDelay---0-----
>----->
|                (1) (2) |
'-MIGDelay---Tage-----'

.-MIGContinue---Yes-----
>----->
|                (1) (2) |
'-MIGContinue---+No-----'
|                '-Yes-'

.-MIGProcess---1-----
>----->
|                (1) (2) |
'-MIGProcess---Anzahl-----'

.-DATAFormat---NATive-----
>----->
|                (2) (4) |
'-DATAFormat---+NATive-----'
|                +-NONblock---+
|                +-NETAPPDump--+
|                +-CELERRADump--+
|                '-NDMPDump----'

.-AUTOCopy---Client-----

```



#### READWrite

Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff auf Dateien haben, die auf Datenträgern in dem Speicherpool gespeichert sind.

#### READOnly

Gibt an, dass Clientknoten Dateien auf den Datenträgern im Speicherpool nur lesen können.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Für die Datenträger in dem Speicherpool sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig.

Wenn dieser Speicherpool als untergeordneter Speicherpool angegeben (mit dem Parameter NEXTSTGPOOL) und als *readonly (schreibgeschützt)* definiert wurde, wird der Speicherpool übersprungen, wenn Serverprozesse versuchen, Dateien in den Speicherpool zu schreiben.

#### UNAVailable

Gibt an, dass Clientknoten nicht auf Dateien, die auf Datenträgern im Speicherpool gespeichert sind, zugreifen können.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Außerdem können sie Dateien aus diesem Speicherpool in einen anderen Speicherpool versetzen oder kopieren. Für die Datenträger in dem Speicherpool sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig.

Wenn dieser Speicherpool als untergeordneter Speicherpool angegeben (mit dem Parameter NEXTSTGPOOL) und als *unavailable (nicht verfügbar)* definiert wurde, wird der Speicherpool übersprungen, wenn Serverprozesse versuchen, Dateien in den Speicherpool zu schreiben.

#### MAXSIze

Gibt die maximale Größe einer physischen Datei an, die der Server in dem Speicherpool speichern kann. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Sie können einen der folgenden Werte angeben:

#### NOLimit

Gibt an, dass für die im Speicherpool gespeicherten physischen Dateien keine Größenbeschränkung besteht.

#### maximale\_Dateigröße

Begrenzt die maximale Größe für physische Dateien. Geben Sie eine ganze Zahl zwischen 1 und 999999 Terabyte gefolgt von einem Maßstabsfaktor an. MAXSIZE=5G gibt z. B. an, dass die maximale Dateigröße für diesen Speicherpool 5 Gigabyte ist. Maßstabsfaktoren sind:

| Maßstabsfaktor | Bedeutung |
|----------------|-----------|
| K              | Kilobyte  |
| M              | Megabyte  |
| G              | Gigabyte  |
| T              | Terabyte  |

Der Client schätzt die Größe der Dateien, die an den Server gesendet werden. Die Schätzung des Clients wird verwendet und nicht das tatsächliche Datenvolumen, das an den Server gesendet wird. Clientoptionen, wie z. B. Deduplizierung, Komprimierung und Verschlüsselung, können zur Folge haben, dass das tatsächliche Datenvolumen, das an den Server gesendet wird, größer oder kleiner als die Größenschätzung ist. Beispielsweise kann eine komprimierte Datei kleiner als die Schätzung sein, sodass weniger Daten als der Schätzwert gesendet werden. Des Weiteren kann eine Binärdatei nach der Komprimierungsverarbeitung größer sein, sodass mehr Daten als der Schätzwert gesendet werden.

Wenn die physische Größe des Speicherpools den Wert des Parameters MAXSIZE überschreitet, zeigt die folgende Tabelle an, wo Dateien normalerweise gespeichert werden.

Tabelle 1. Position einer Datei gemäß der Dateigröße und dem angegebenen Pool

| Dateigröße                       | Angegebener Pool   | Ergebnis   |
|----------------------------------|--|--|
| Überschreitet die maximale Größe | Es ist kein Pool als nächster Speicherpool in der Hierarchie angegeben | Die Datei wird vom Server nicht gespeichert  |
|                                  | Ein Pool ist als nächster Speicherpool in der Hierarchie angegeben     | Der Server speichert die Datei im nächsten Speicherpool, der die Dateigröße akzeptiert |

Tipp: Wenn Sie auch den Parameter NEXTstgpool angeben, definieren Sie einen einzelnen Speicherpool in Ihrer Hierarchie so, dass er keine Begrenzung hinsichtlich der maximalen Dateigröße hat, indem Sie den Parameter MAXSIZE=NOLimit angeben. Wenn mindestens ein Pool keine Größenbegrenzung hat, wird sichergestellt, dass der Server die Datei unabhängig von ihrer Größe speichern kann.

Bei mehreren Dateien, die in einer einzelnen Transaktion gesendet werden, betrachtet der Server die Größe der Transaktion als Dateigröße. Wenn die Gesamtgröße aller Dateien in der Transaktion die maximale Größe überschreitet, werden die Dateien vom Server nicht in dem Speicherpool gespeichert.

Einschränkung:

Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### CRCData

Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist nur für Speicherpools mit dem Datenformat NATIVE gültig. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCDATA auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

Yes

Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da eine zusätzliche Verarbeitung erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

No

Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

Tipp:

Für Speicherpools, die dem Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet sind, bietet der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust als die CRC-Überprüfung für einen Speicherpool. Wenn Sie die CRC-Überprüfung für einen Speicherpool angeben, werden Daten nur während der Ausführung von Datenträgerprüfungsoperationen überprüft. Fehler werden identifiziert, nachdem Daten auf Band geschrieben wurden.

Um den Schutz logischer Blöcke zu aktivieren, geben Sie den Wert READWRITE für den Parameter LBPROTECT in den Befehlen DEFINE DEVCLASS und UPDATE DEVCLASS für den Einheitentyp 3592, LTO oder ECARTRIDGE an. Der Schutz logischer Blöcke wird nur für die folgenden Typen von Laufwerken und Datenträgern unterstützt:

- IBM® LTO5 und höher
- IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
- Oracle StorageTek T10000C- und T10000D-Laufwerke

#### NEXTstgpool

Gibt einen primären Speicherpool an, in den Dateien umgelagert werden. Sie können keine Daten aus einem Speicherpool mit sequenziellem Zugriff in einen Speicherpool mit wahlfreiem Zugriff umlagern. Dieser Parameter ist wahlfrei.

Verfügt dieser Speicherpool nicht über einen nächsten Speicherpool, kann der Server nicht Dateien aus diesem Speicherpool umlagern und Dateien, die die maximale Größe für diesen Speicherpool überschreiten, nicht in einem anderen Speicherpool speichern.

Ist in dem aktuellen Speicherpool nicht genügend Speicherbereich verfügbar, erlaubt der Parameter NEXTSTGPOOL für Speicherpools mit sequenziellem Zugriff nicht das Speichern von Daten im nächsten Pool. In diesem Fall gibt der Server eine Nachricht aus, und die Transaktion schlägt fehl.

Für nächste Speicherpools mit dem Einheitentyp FILE führt der Server eine vorläufige Überprüfung durch, um zu bestimmen, ob genügend Speicherbereich verfügbar ist. Ist kein Speicherbereich verfügbar, springt der Server zum nächsten Speicherpool in der Hierarchie. Ist Speicherbereich verfügbar, versucht der Server, Daten in diesem Pool zu speichern. Die Speicheroperation kann jedoch fehlschlagen, wenn zum Zeitpunkt der tatsächlichen Speicheroperation der Speicherbereich nicht mehr verfügbar ist.

Einschränkungen:

- Um sicherzustellen, dass keine Speicherpoolkette erstellt wird, die zu einer Endlosschleife führt, geben Sie mindestens einen Speicherpool in der Hierarchie ohne Wert an.
- Wenn Sie einen Pool mit sequenziellem Zugriff als nächsten Speicherpool angeben, muss der Pool entweder das Datenformat NATIVE oder NONBLOCK haben.
- Geben Sie keinen Verzeichniscontainer- oder Cloud-Containerspeicherpool an.
- Verwenden Sie diesen Parameter nicht, um einen Speicherpool für die Datenumlagerung anzugeben.
- Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:



- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### Highmig

Gibt an, dass der Server die Umlagerung startet, wenn die Speicherpoolauslastung diesen Prozentsatz erreicht. Für Plattenspeicherpools mit sequenziellem Zugriff (FILE) ist die Auslastung das Verhältnis der Daten in einem Speicherpool zur Summe der geschätzten Datenkapazität des Pools, einschließlich der Kapazität aller für den Pool angegebenen Arbeitsdatenträger. Für Speicherpools, die Banddatenträger verwenden, ist die Auslastung das Verhältnis der Datenträger, die Daten enthalten, zur Gesamtzahl der Datenträger in dem Speicherpool. Die Gesamtzahl der Datenträger schließt die maximale Anzahl Arbeitsdatenträger ein. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 100 angeben. Der Standardwert ist 90.

Wenn der Speicherpool die obere Umlagerungsschwelle überschreitet, kann der Server die Umlagerung von Dateien in den nächsten definierten Speicherpool nach Datenträger starten. Die obere Umlagerungsschwelle kann auf 100 gesetzt werden, um die Umlagerung für den Speicherpool zu verhindern.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### Lowmig

Gibt an, dass der Server die Umlagerung stoppt, wenn die Speicherpoolauslastung diesen Prozentsatz erreicht oder unter diesem Prozentsatz liegt. Für Plattenspeicherpools mit sequenziellem Zugriff (FILE) ist die Auslastung das Verhältnis der Daten in einem Speicherpool zur Summe der geschätzten Datenkapazität des Pools, einschließlich der Kapazität aller für den Pool angegebenen Arbeitsdatenträger. Für Speicherpools, die Banddatenträger verwenden, ist die Auslastung das Verhältnis der Datenträger, die Daten enthalten, zur Gesamtzahl der Datenträger in dem Speicherpool. Die Gesamtzahl der Datenträger schließt die maximale Anzahl Arbeitsdatenträger ein. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 99 angeben. Der Standardwert ist 70.

Wenn der Speicherpool die untere Umlagerungsschwelle erreicht, wird die Umlagerung von Dateien von einem anderen Datenträger von dem Server nicht gestartet. Die Angabe von 0 für die untere Umlagerungsschwelle erlaubt eine Umlagerung, um den Speicherpool zu leeren.


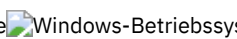
Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### REClaim

Gibt an, wann der Server einen Datenträger auf der Basis des Prozentsatzes wiederherstellbaren Speicherbereichs auf einem Datenträger zurückfordert. Der wiederherstellbare Speicherbereich ist der Speicherbereich, der durch Dateien belegt ist, die verfallen sind oder aus der Datenbank gelöscht wurden.

Bei der Wiederherstellung wird der zerstückelte Speicherbereich auf Datenträgern durch Versetzen der restlichen nicht verfallenen Dateien von einem Datenträger auf einen anderen wieder verwendbar, wodurch der ursprüngliche Datenträger wiederverwendet werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 100 angeben. Der Standardwert ist 60, außer für Speicherpools, die WORM-Einheiten verwenden.

  Für Speicherpools, die eine Einheitenklasse WORM verwenden, kann der Standardwert 100 verringert werden. Damit wird es dem Server ermöglicht, Daten bei Bedarf auf weniger Datenträger zusammenzulegen. Datenträger, die durch die Wiederherstellung geleert werden, können aus dem Kassettenarchiv entnommen werden, wodurch Schächte für neue Datenträger freigegeben werden. Da die Datenträger nur einmal beschrieben werden können, ist eine Wiederverwendung der Datenträger nicht möglich.

Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

Einen Wert von 50 Prozent oder höher für diesen Parameter angeben, so dass Dateien, die auf zwei Datenträgern gespeichert sind, auf einem einzigen Ausgabedatenträger gespeichert werden können.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP

- NDMPDUMP

#### RECLAIMProcess

Gibt die Anzahl paralleler Prozesse für das Wiederherstellen der Datenträger in diesem Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein. Der Standardwert ist 1. Sie können einen oder mehrere Wiederherstellungsprozesse für jeden primären Speicherpool mit sequenziellem Zugriff angeben. Berücksichtigen Sie bei der Berechnung des Werts für diesen Parameter die folgenden Ressourcen, die für die Wiederherstellungsverarbeitung erforderlich sind:

- Die Anzahl sequenzieller Speicherpools
- Die Anzahl logischer und physischer Laufwerke, die der Operation zugeordnet werden kann

Für den Zugriff auf Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk.

Beispiel: Angenommen, Sie möchten die Datenträger aus zwei Speicherpools mit sequenziellem Zugriff gleichzeitig wiederherstellen und Sie möchten vier Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Wenn der Parameter RECLAIMSTGPOOL nicht angegeben ist oder der Wiederherstellungsspeicherpool dieselbe Einheitenklasse wie der Speicherpool hat, der wiederhergestellt wird, benötigt jeder Prozess zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um acht Wiederherstellungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 16 Mountpunkte und 16 Laufwerke. Die Einheitenklasse für die Speicherpools muss einen Grenzwert für Ladeanforderungen von mindestens 16 haben.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### RECLAIMSTGpool

Gibt einen anderen primären Speicherpool als Ziel für wiederhergestellte Daten aus diesem Speicherpool an. Dieser Parameter ist wahlfrei. Wenn der Server Datenträger für den Speicherpool zurückfordert, versetzt der Server nicht verfallene Daten von den Datenträgern, die zurückgefordert werden, in den Speicherpool, der in diesem Parameter angegeben ist.

Ein Wiederherstellungsspeicherpool ist besonders nützlich für einen Speicherpool, der nur ein Laufwerk in seinem Kassettenarchiv hat. Wird dieser Parameter angegeben, versetzt der Server alle Daten von den zurückgeforderten Datenträgern in den Wiederherstellungsspeicherpool, unabhängig von der Anzahl der Laufwerke in dem Kassettenarchiv.

Um die Daten aus dem Wiederherstellungsspeicherpool wieder in den ursprünglichen Speicherpool zu versetzen, ist die Speicherpoolhierarchie zu verwenden. Den ursprünglichen Speicherpool als nächsten Speicherpool für den Wiederherstellungsspeicherpool angeben.

Einschränkung:

- Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### RECLAMATIONType

Gibt die Methode an, mit der Datenträger wiederhergestellt und verwaltet werden. Dieser Parameter ist wahlfrei. Der Standardwert ist THRESHOLD. Gültige Werte:

##### THRESHold

Gibt an, dass Datenträger, die zu diesem Speicherpool gehören, gemäß dem Schwellenwert im Attribut RECLAIM für diesen Speicherpool wiederhergestellt werden.

##### SNAPlock

Gibt an, dass FILE-Datenträger, die zu diesem Speicherpool gehören, mit NetApp Data ONTAP-Software und NetApp SnapLock-Datenträgern für die Aufbewahrung verwaltet werden. Dieser Parameter ist nur für Speicherpools gültig, die für einen Server definiert sind, auf dem der Aufbewahrungsschutz für Daten aktiviert ist und der einer Einheitenklasse FILE zugeordnet ist. Datenträger in diesem Speicherpool werden nicht anhand des Schwellenwerts wiederhergestellt. Der RECLAIM-Wert für den Speicherpool wird ignoriert.

Alle Datenträger in diesem Speicherpool werden als FILE-Datenträger erstellt. Ein Aufbewahrungsdatum, das von den Aufbewahrungsattributen in der Archivierungskopiengruppe für den Speicherpool abgeleitet wird, wird in den Metadaten für den FILE-Datenträger mit der SnapLock-Funktion des Betriebssystems NetApp Data ONTAP definiert. Bis zum Ablauf

des Aufbewahrungsdatums können der FILE-Datenträger und alle darauf befindlichen Daten nicht von dem physischen SnapLock-Datenträger gelöscht werden, auf dem sie gespeichert sind.

Der Parameter RECLAMATIONTYPE muss für alle Speicherpools, die definiert werden, identisch sein, wenn er für denselben Einheitenklassennamen definiert wird. Der Befehl DEFINE kann fehlschlagen, wenn der angegebene Parameter RECLAMATIONTYPE von der Angabe abweicht, die für Speicherpools definiert ist, die bereits für den Einheitenklassennamen definiert wurden.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### COLlocate

Gibt an, ob der Server versucht, Daten, die zu den folgenden Kandidaten gehören, auf möglichst wenig Datenträgern zu speichern:

- Ein einzelner Clientknoten
- Eine Gruppe von Dateibereichen
- Eine Gruppe von Clientknoten
- Ein Clientdateibereich

Dieser Parameter ist wahlfrei. Der Standardwert ist GROUP.

Die Kollokation reduziert die Anzahl der Ladevorgänge für Datenträger mit sequenziellem Zugriff für Zurückschreibungs-, Abruf- und Rückrufoperationen. Die Kollokation erfordert jedoch mehr Serverzeit, um Dateien zum Speichern zusammenzufassen, sowie eine größere Anzahl Datenträger. Die Kollokation kann sich auch auf die Anzahl Prozesse zum Umlagern von Platten in den sequenziellen Pool auswirken.

Sie können eine der folgenden Optionen angeben:

#### No

Gibt an, dass die Kollokation inaktiviert ist. Während der Umlagerung von Platte werden Prozesse auf einer Dateibereichsebene erstellt.

#### GRoup

Gibt an, dass die Kollokation auf Gruppenebene für Clientknoten oder Dateibereiche aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten für Knoten oder Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf so wenig Datenträgern wie möglich zu speichern.

Wenn Sie COLLOCATE=GROUP angeben, aber keine Kollokationsgruppen definieren, oder wenn Sie keine Knoten oder Dateibereiche zu einer Kollokationsgruppe hinzufügen, werden Daten nach Knoten durch Kollokation zusammengefasst. Ziehen Sie die Verwendung von Bändern in Betracht, wenn Sie Clientknoten oder Dateibereiche in Kollokationsgruppen zusammenfassen.

Besteht beispielsweise ein bandbasierter Speicherpool aus Daten von Knoten, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst die Daten für gruppierte Knoten nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Knoten gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten für nicht gruppierte Knoten nach Knoten zusammen. Wenn möglich, speichert der Server die Daten für einen einzelnen Knoten auf einem einzelnen Band. Alle verfügbaren Bänder, die bereits Daten für den Knoten enthalten, werden verwendet, bevor verfügbarer Speicherbereich auf einem anderen Band verwendet wird.
- Während der Umlagerung von Platte erstellt der Server Umlagerungsprozesse auf der Kollokationsgruppenebene für gruppierte Knoten und auf der Knotenebene für nicht gruppierte Knoten.

Besteht ein bandbasierter Speicherpool aus Daten aus gruppierten Dateibereichen, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst nur die Daten für gruppierte Dateibereiche nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Dateibereichen gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Dateibereich können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten nach Knoten zusammen (für Dateibereiche, die nicht explizit für eine Dateibereichskollokationsgruppe definiert sind). Beispiel: Knoten1 hat die Dateibereiche A, B, C, D und E. Die Dateibereiche A und B gehören zu einer Dateibereichskollokationsgruppe, die Dateibereiche C, D und E dagegen nicht. Die Dateibereiche A und B werden nach Dateibereichskollokationsgruppe zusammengefasst, während die Dateibereiche C, D und E nach Knoten zusammengefasst werden.

- Während der Umlagerung von Platte erstellt der Server Umlagerungsprozesse auf der Kollokationsgruppenebene für gruppierte Dateibereiche.

Daten werden auf so wenig Datenträger mit sequenziellm Zugriff wie möglich zusammengefasst.

#### NODE

Gibt an, dass die Kollokation auf Clientknotenebene aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten eines Knotens auf so wenig Datenträgern wie möglich zu speichern. Verfügt der Knoten über mehrere Dateibereiche, versucht der Server nicht, diese Dateibereiche durch Kollokation zusammenzufassen. Für die Kompatibilität mit früheren Versionen wird COLLOCATE=YES noch vom Server akzeptiert, um die Kollokation auf der Clientknotenebene anzugeben.

Enthält ein Speicherpool Daten für einen Knoten, der Teil einer Kollokationsgruppe ist, und geben Sie COLLOCATE=NODE an, werden die Daten nach Knoten durch Kollokation zusammengefasst.

Bei COLLOCATE=NODE erstellt der Server Prozesse auf der Knotenebene, wenn Daten von Platte umgelagert werden.

#### Filespace

Gibt an, dass die Kollokation auf der Dateibereichsebene für Clientknoten aktiviert ist. Der Server versucht, Daten eines Knotens und eines Dateibereichs auf so wenig Datenträgern wie möglich zu speichern. Verfügt ein Knoten über mehrere Dateibereiche, versucht der Server, Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern zu speichern.

Bei COLLOCATE=FILESPACE erstellt der Server Prozesse auf der Dateibereichsebene, wenn Daten von Platte umgelagert werden.

#### MAXSCRatch (Erforderlich)

Gibt die maximale Anzahl der Arbeitsdatenträger an, die der Server für diesen Speicherpool anfordern kann. Sie können eine ganze Zahl von 0 bis 100000000 angeben. Wird dem Server das Anfordern von Arbeitsdatenträgern erlaubt, muss der Benutzer nicht jeden zu verwendenden Datenträger definieren.

Mit dem für diesen Parameter angegebenen Wert wird die Gesamtzahl der im Speicherpool verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Speicherpools geschätzt.

Arbeitsdatenträger werden automatisch aus dem Speicherpool gelöscht, sobald sie leer sind. Wenn Arbeitsdatenträger mit dem Einheitentyp FILE gelöscht werden, wird der von den Datenträgern belegte Speicherbereich von dem Server freigegeben und an das Dateisystem zurückgegeben.

Tipp: Für serverübergreifende Operationen, die virtuelle Datenträger verwenden und ein kleines Datenvolumen speichern, sollte ein Wert für den Parameter MAXSCRATCH angegeben werden, der höher als der Wert ist, der normalerweise für Schreiboperationen für andere Datenträgertypen angegeben wird. Nach einer Schreiboperation auf einem virtuellen Datenträger markiert IBM Spectrum Protect den Datenträger als FULL, auch wenn der Wert des Parameters MAXCAPACITY in der Einheitenklassendefinition noch nicht erreicht wurde. Der Server behält virtuelle Datenträger nicht im Status FILLING und hängt keine Daten an. Ist der Wert des Parameters MAXSCRATCH zu niedrig, können serverübergreifende Operationen fehlschlagen.

#### REUsedelay

Gibt die Anzahl Tage an, die nach dem Löschen aller Dateien von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerpool zurückgestellt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Standardwert ist 0, was bedeutet, dass ein Datenträger neu beschrieben oder in den Arbeitsdatenträgerpool zurückgestellt werden kann, sobald alle Dateien von dem Datenträger gelöscht wurden.

Tipp: Mit diesem Parameter kann sichergestellt werden, dass Datenbankverweise auf Dateien im Speicherpool noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird. Dieser Parameter muss auf einen Wert gesetzt werden, der größer als die Anzahl der Tage ist, die die älteste Datenbanksicherung aufbewahrt werden soll. Die für diesen Parameter angegebene Anzahl Tage muss der im Befehl SET DRMDBBACKUPEXPIREDAYS angegebenen Anzahl entsprechen.

#### OVFLocation

Gibt den Überlaufstandort für den Speicherpool an. Der Server ordnet diesen Standortnamen einem Datenträger zu, der durch den Befehl aus dem Kassettenarchiv ausgegeben wird. Dieser Parameter ist wahlfrei. Der Standortname darf maximal 255 Zeichen lang sein. Den Standortnamen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### MIGDelay

Gibt die Mindestanzahl Tage an, die eine Datei in einem Speicherpool verbleiben muss, bevor sie für die Umlagerung ausgewählt werden kann. Alle Dateien auf einem Datenträger müssen für die Umlagerung auswählbar sein, bevor der Server den Datenträger für die Umlagerung auswählt. Um einen Wert zu berechnen, der mit dem angegebenen Wert für MIGDELAY verglichen wird, zählt der Server die Anzahl der Tage, die die Datei im Speicherpool war.

Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Standardwert 0 gibt an, dass die Umlagerung nicht verzögert werden soll. Soll der Server die Anzahl der Tage nur ab dem Tag zählen, an dem eine Datei gespeichert wurde, und nicht ab dem Tag, an dem sie abgerufen wurde, die Serveroption NORETRIEVEDATE verwenden.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### MIGContinue

Gibt an, ob der Server Dateien umlagern darf, die der Verzögerungszeit für die Umlagerung nicht entsprechen. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Da angegeben werden kann, dass Dateien eine Mindestanzahl Tage in dem Speicherpool verbleiben müssen, kann der Server alle auswählbaren Dateien in den nächsten Speicherpool umlagern, obwohl sie dem Wert für die untere Umlagerungsschwelle nicht entsprechen. Mit diesem Parameter kann angegeben werden, ob der Server den Umlagerungsprozess fortsetzen darf, indem Dateien umgelagert werden, die der Verzögerungszeit für die Umlagerung nicht entsprechen.

Sie können einen der folgenden Werte angeben:

#### Yes

Muss die untere Umlagerungsschwelle eingehalten werden, gibt dieser Wert an, dass der Server mit der Umlagerung von Dateien fortfährt, die der Verzögerungszeit für die Umlagerung nicht entsprechen.

Sind mehrere Umlagerungsprozesse für den Speicherpool zulässig, werden einige Dateien, die der Verzögerungszeit für die Umlagerung nicht entsprechen, unter Umständen unnötigerweise umgelagert. Während ein Prozess Dateien umlagert, die der Verzögerungszeit für die Umlagerung entsprechen, könnte ein zweiter Prozess mit der Umlagerung von Dateien beginnen, die der Verzögerungszeit für die Umlagerung nicht entsprechen, um die untere Umlagerungsschwelle einzuhalten. Der erste Prozess, der noch Dateien umlagert, die der Verzögerungszeit für die Umlagerung entsprechen, könnte selbst die Einhaltung der unteren Umlagerungsschwelle bewirkt haben.

#### No

Gibt an, dass der Server die Umlagerung stoppt, wenn keine auswählbaren Dateien mehr für die Umlagerung verfügbar sind; dies gilt auch vor Erreichen der unteren Umlagerungsschwelle. Der Server lagert nur Dateien um, die der Verzögerungszeit für die Umlagerung entsprechen.

#### MIGProcess

Gibt die Anzahl paralleler Prozesse für das Umlagern der Dateien von den Datenträgern in diesen Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein. Der Standardwert ist 1.

Bei der Berechnung des Werts für diesen Parameter ist die Anzahl der sequenziellen Speicherpools, die von der Umlagerung betroffen sind, und die Anzahl der logischen und physischen Laufwerke zu berücksichtigen, die der Operation zugeordnet werden können. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl der verfügbaren Mountpunkte und Laufwerke ist von anderen IBM Spectrum Protect- und Systemaktivitäten sowie von den Grenzwerten für Ladeanforderungen der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die von der Umlagerung betroffen sind.

Beispiel: Angenommen, Sie möchten gleichzeitig die Dateien von Datenträgern in zwei primären sequenziellen Speicherpools umlagern und Sie möchten drei Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Hat der Speicherpool, in den Dateien umgelagert werden, dieselbe Einheitenklasse wie der Speicherpool, aus dem Dateien umgelagert werden, benötigt jeder Prozess zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um sechs Umlagerungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 12 Mountpunkte und 12 Laufwerke. Die Einheitenklasse für die Speicherpools muss einen Grenzwert für Ladeanforderungen von mindestens 12 haben.

Überschreitet die angegebene Anzahl der Umlagerungsprozesse die Anzahl der verfügbaren Mountpunkte oder Laufwerke, warten die Prozesse, die keine Mountpunkte oder Laufwerke anfordern können, bis Mountpunkte oder Laufwerke verfügbar werden. Werden Mountpunkte oder Laufwerke innerhalb der MOUNTWAIT-Zeit nicht verfügbar, werden die Umlagerungsprozesse beendet. Informationen zur Angabe der MOUNTWAIT-Zeit befinden sich in DEFINE DEVCLASS (Einheitenklasse definieren).

Der IBM Spectrum Protect-Server startet die angegebene Anzahl der Umlagerungsprozesse, unabhängig von der Anzahl der Datenträger, die für die Umlagerung ausgewählt werden können. Geben Sie beispielsweise zehn Umlagerungsprozesse an und können nur sechs Datenträger für die Umlagerung ausgewählt werden, startet der Server zehn Prozesse, von denen vier beendet werden, ohne dass ein Datenträger verarbeitet wird.

Tipp: Beachten Sie bei der Angabe dieses Parameters, ob die Funktion für simultanes Schreiben für die Serverdatenumlagerung aktiviert ist. Jeder Umlagerungsprozess erfordert einen Mountpunkt und ein Laufwerk für jeden Kopierspeicherpool und Pool für

aktive Daten, der für den Zielspeicherpool definiert ist.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### DATAFormat

Gibt das Datenformat an, das zum Sichern von Dateien in diesem Speicherpool und zum Zurückschreiben von Dateien aus diesem Speicherpool verwendet werden soll. Das Standardformat ist das NATIVE-Serverformat. Sie können die folgenden Werte angeben:

##### NATive

Gibt an, dass das Datenformat das native IBM Spectrum Protect-Serverformat ist und Block-Header einschließt.

##### NONblock

Gibt an, dass das Datenformat das native IBM Spectrum Protect-Serverformat ist und keine Block-Header einschließt. Die standardmäßige Mindestblockgröße auf einem Datenträger, der der Einheitenklasse FILE zugeordnet ist, beträgt 256 KB, unabhängig davon, wie viele Daten auf den Datenträger geschrieben werden. Für bestimmte Tasks können Sie die ineffiziente Speichernutzung auf Speicherdatenträgern minimieren, indem Sie das Datenformat NONBLOCK angeben. Sie können beispielsweise das Datenformat NONBLOCK für die folgenden Tasks angeben:

- Verwendung von Content-Management-Produkten
- Verwendung der Clientoption DIRMC zum Speichern von Verzeichnisinformationen
- Umlagerung sehr kleiner Dateien mit IBM Spectrum Protect for Space Management oder IBM Spectrum Protect HSM for Windows

In den meisten Situationen wird jedoch das native Format bevorzugt.

##### NETAPPDump

Gibt an, dass die Daten das NetApp-Speicherauszugsformat haben. Dieses Datenformat muss für Dateisystemimages angegeben werden, die ein Speicherauszugsformat haben und die von einem NetApp-Dateiserver oder einem IBM System Storage N Series-Dateiserver unter Verwendung von NDMP gesichert wurden. Der Server führt keine Umlagerung, Wiederherstellung oder AUDIT VOLUME für einen Speicherpool mit DATAFORMAT=NETAPPDUMP aus. Mit dem Befehl MOVE DATA können Sie Daten aus einem primären Speicherpool in einen anderen primären Speicherpool oder von einem Datenträger versetzen, wenn der Datenträger wiederverwendet werden muss.

##### CELERRADump

Gibt an, dass die Daten das EMC Celerra-Speicherauszugsformat haben. Dieses Datenformat muss für Dateisystemimages angegeben werden, die ein Speicherauszugsformat haben und die von einem EMC Celerra-Dateiserver unter Verwendung von NDMP gesichert wurden. Der Server führt keine Umlagerung, Wiederherstellung oder AUDIT VOLUME für einen Speicherpool mit DATAFORMAT=CELERRADUMP aus. Mit dem Befehl MOVE DATA können Sie Daten aus einem primären Speicherpool in einen anderen primären Speicherpool oder von einem Datenträger versetzen, wenn der Datenträger wiederverwendet werden muss.

##### NDMPDump

Gibt an, dass die Daten ein lieferantenspezifisches NAS-Sicherungsformat haben. Verwenden Sie dieses Datenformat für Dateisystemimages, die von einem NAS-Dateiserver gesichert wurden, der kein NetApp-Dateiserver oder EMC Celerra-Dateiserver ist. Der Server führt keine Umlagerung, Wiederherstellung oder AUDIT VOLUME für einen Speicherpool mit DATAFORMAT=NDMPDUMP aus. Mit dem Befehl MOVE DATA können Sie Daten aus einem primären Speicherpool in einen anderen primären Speicherpool oder von einem Datenträger versetzen, wenn der Datenträger wiederverwendet werden muss.

#### AUTOCopy

Gibt an, wann IBM Spectrum Protect Operationen mit simultanem Schreiben ausführt. Der Standardwert ist CLIENT. Dieser Parameter ist wahlfrei und betrifft die folgenden Operationen:

- Clientspeichersitzungen
- Serverimportprozesse
- Serverdatenumlagerungsprozesse

Wenn die Option AUTOCOPY auf ALL oder CLIENT gesetzt wird und mindestens ein Speicherpool vorhanden ist, der in der Option COPYSTGPOOLS oder ACTIVEDATAPOOLS aufgelistet ist, wird die clientseitige Deduplizierung inaktiviert.

Tritt ein Fehler auf, wenn Daten während eines Umlagerungsprozesses gleichzeitig in einen Kopienspeicherpool oder einen Pool für aktive Daten geschrieben werden, stoppt der Server das Schreiben in die fehlerhaften Speicherpools für den Rest des Prozesses. Der Server speichert jedoch weiterhin Dateien in dem primären Speicherpool und in allen verbleibenden Kopienspeicherpools oder Pools für aktive Daten. Diese Pools bleiben für die Dauer des Umlagerungsprozesses aktiv. Kopienspeicherpools werden mit dem Parameter COPYSTGPOOLS angegeben. Pools für aktive Daten werden mit dem Parameter ACTIVEDATAPOOLS angegeben.

Sie können einen der folgenden Werte angeben:

None

Gibt an, dass die Funktion für simultanes Schreiben inaktiviert ist.

Client

Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen oder Serverimportprozessen gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverimportprozessen werden Daten nur gleichzeitig in Kopienspeicherpools geschrieben. Daten werden während der Ausführung von Serverimportprozessen nicht in Pools für aktive Daten geschrieben.

MIGRation

Gibt an, dass Daten nur während der Umlagerung in diesen Speicherpool gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverdatenumlagerungsprozessen werden Daten in Kopienspeicherpools und Pools für aktive Daten nur dann gleichzeitig geschrieben, wenn die Daten in diesen Pools nicht vorhanden sind. Knoten, deren Daten umgelagert werden, müssen sich in einer Domäne befinden, die einem Pool für aktive Daten zugeordnet ist. Befinden sich die Knoten nicht in einer Domäne, die einem Pool für aktive Daten zugeordnet ist, können die Daten nicht in den Pool geschrieben werden.

All

Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen, Serverimportprozessen oder Serverdatenumlagerungsprozessen gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Mit diesem Wert wird sichergestellt, dass Daten immer dann gleichzeitig geschrieben werden, wenn dieser Pool ein Ziel für eine der auswählbaren Operationen ist.

COPYSTGpools

Gibt die Namen von Kopienspeicherpools an, in die der Server gleichzeitig Daten schreibt. Der Parameter COPYSTGPOOLS ist optional. Sie können maximal drei Kopienpoolnamen angeben, die durch Kommas voneinander getrennt werden müssen. Leerzeichen zwischen den Namen der Kopienpools sind nicht zulässig. Wenn Sie einen Wert für den Parameter COPYSTGPOOLS angeben, können Sie auch einen Wert für den Parameter COPYCONTINUE angeben.

Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSTGPOOLS und ACTIVEDATAPOOLS angegeben sind, darf drei nicht überschreiten.

Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Kopienspeicherpools und den Wert für COPYCONTINUE aus dem primären Speicherpool. Der primäre Speicherpool wird durch die Kopiergruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

Der Server kann während der Ausführung der folgenden Operationen Daten gleichzeitig in Kopienspeicherpools schreiben:

- Sicherungs- und Archivierungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder Anwendungsclients, die die IBM Spectrum Protect-API verwenden
- Umlagerungsoperationen durch IBM Spectrum Protect for Space Management-Clients
- Importoperationen, die das Kopieren von exportierten Dateidaten von externen Datenträgern in einen Speicherpool einbeziehen, der mit einer Kopienspeicherpoolliste definiert ist

Einschränkungen:

1. Dieser Parameter ist nur für primäre Speicherpools verfügbar, die das Datenformat NATIVE oder NONBLOCK verwenden. Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP
2. Das simultane Schreiben in Kopienspeicherpools wird nicht unterstützt, wenn die LAN-unabhängige Datenversetzung verwendet wird. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch akzeptiert.
3. Die Funktion für simultanes Schreiben wird für NAS-Sicherungsoperationen nicht unterstützt. Sind für den primären Speicherpool, der in DESTINATION oder TOCDESTINATION in der Kopiergruppe der Verwaltungsklasse angegeben ist, Kopienspeicherpools definiert, werden die Kopienspeicherpools ignoriert und die Daten werden nur im primären Speicherpool gespeichert.
4. Die Funktion für simultanes Schreiben kann mit CENTERA-Speichereinheiten nicht verwendet werden.

Achtung: Die mit dem Parameter COPYSTGPOOLS zur Verfügung gestellte Funktion soll nicht den Befehl BACKUP STGPOOL ersetzen. Wird der Parameter COPYSTGPOOLS verwendet, verwenden Sie weiterhin den Befehl BACKUP STGPOOL, um sicherzustellen, dass die Kopienspeicherpools vollständige Kopien des primären Speicherpools sind. Es gibt Fälle, in denen eine Kopie möglicherweise nicht erstellt wird. Weitere Informationen enthält die Beschreibung des Parameters COPYCONTINUE.

COPYContinue

Gibt an, wie der Server auf einen Fehler beim Schreiben in einen der Kopienspeicherpools reagiert, die im Parameter COPYSTGPOOLS aufgelistet sind. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Wenn Sie den Parameter COPYCONTINUE angeben, müssen Sie auch den Parameter COPYSTGPOOLS angeben.

Der Parameter COPYCONTINUE hat keine Auswirkung auf die Funktion für simultanes Schreiben während der Umlagerung.

Sie können die folgenden Werte angeben:

Yes

Ist der Parameter COPYCONTINUE auf YES gesetzt, stoppt der Server das Schreiben in die fehlerhaften Kopienpools für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Kopienpools fort. Die Liste der Kopienspeicherpools ist nur für die Dauer der Clientsitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.

No

Ist der Parameter COPYCONTINUE auf NO gesetzt, wird die aktuelle Transaktion vom Server nicht ausgeführt und die Speicheroperation nicht fortgesetzt.

Einschränkungen:

- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf Pools für aktive Daten. Tritt für einen der Pools für aktive Daten ein Schreibfehler auf, stoppt der Server das Schreiben in den fehlerhaften Pool für aktive Daten für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Pools für aktive Daten und Kopienspeicherpools fort. Die Liste der Pools für aktive Daten ist nur für die Dauer der Sitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.
- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Ausführung eines Serverimportprozesses. Werden Daten gleichzeitig geschrieben und tritt für den primären Speicherpool oder einen Kopienspeicherpool ein Schreibfehler auf, schlägt der Serverimportprozess fehl.
- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Serverdatenumlagerung. Werden Daten gleichzeitig geschrieben und tritt für einen Kopienspeicherpool oder Pool für aktive Daten ein Schreibfehler auf, wird der fehlerhafte Speicherpool entfernt und der Datenumlagerungsprozess wird fortgesetzt. Bei Schreibfehlern für den primären Speicherpool schlägt der Umlagerungsprozess fehl.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### ACTIVEDATApools

Gibt die Namen der Pools für aktive Daten an, in die der Server während einer Clientsicherungsoperation gleichzeitig Daten schreibt. Der Parameter ACTIVEDATAPOOLS ist optional. Leerzeichen zwischen den Namen der Pools für aktive Daten sind nicht zulässig.

Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSGTPOOLS und ACTIVEDATAPOOLS angegeben sind, darf drei nicht überschreiten.

Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Pools für aktive Daten aus dem Zielspeicherpool, der in der Kopiengruppe angegeben ist. Der primäre Speicherpool wird durch die Kopiengruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

Der Server kann nur während Sicherungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder durch Anwendungsclients, die die IBM Spectrum Protect-API verwenden, Daten gleichzeitig in Pools für aktive Daten schreiben.

Einschränkungen:

1. Dieser Parameter ist nur für primäre Speicherpools verfügbar, die das Datenformat NATIVE oder NONBLOCK verwenden. Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP
2. Das simultane Schreiben in Pools für aktive Daten wird nicht unterstützt, wenn die LAN-unabhängige Datenversetzung verwendet wird. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch akzeptiert.
3. Die Funktion für simultanes Schreiben wird nicht unterstützt, wenn eine NAS-Sicherungsoperation eine Inhaltsverzeichnisdatei schreibt. Sind für den primären Speicherpool, der in TOCDESTINATION in der Kopiengruppe der Verwaltungsklasse angegeben ist, Pools für aktive Daten definiert, werden die Pools für aktive Daten ignoriert und die Daten werden nur im primären Speicherpool gespeichert.
4. Die Funktion für simultanes Schreiben kann mit CENTERA-Speichereinheiten nicht verwendet werden.
5. Daten, die importiert werden, werden nicht in Pools für aktive Daten gespeichert. Verwenden Sie nach einer Importoperation den Befehl COPY ACTIVEDATA, um die importierten Daten in einem Pool für aktive Daten zu speichern.



Achtung: Die mit dem Parameter ACTIVEPOOL zur Verfügung gestellte Funktion soll nicht den Befehl COPY ACTIVEPOOL ersetzen. Wird der Parameter ACTIVEPOOL verwendet, verwenden Sie den Befehl COPY ACTIVEPOOL, um sicherzustellen, dass die Pools für aktive Daten alle aktiven Daten des primären Speicherpools enthalten.

#### DEDuplicate

Gibt an, ob die in diesem Speicherpool gespeicherten Daten dedupliziert werden. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Der Standardwert ist NO.

#### IDENTIFYProcess

Gibt die Anzahl paralleler Prozesse an, die für die serverseitige Datendeduplizierung verwendet werden sollen. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Geben Sie einen Wert von 0 bis 50 ein. Der Standardwert ist 1. Hat der Parameter DEDuplicate den Wert NO, hat die Standardeinstellung für IDENTIFYPROCESS keine Auswirkung.

Hinweis: Datendeduplizierungsprozesse können entweder aktiv oder inaktiv sein. Prozesse, die gegenwärtig Dateien bearbeiten, sind aktiv. Prozesse, die auf Dateien warten, die bearbeitet werden sollen, sind inaktiv. Prozesse bleiben inaktiv, bis Datenträger mit Daten, die dedupliziert werden sollen, verfügbar werden. Die Ausgabe des Befehls QUERY PROCESS für einen Datendeduplizierungsprozess umfasst die Gesamtzahl Byte und Dateien, die seit dem ersten Start des Prozesses verarbeitet wurden. Wenn beispielsweise ein Datendeduplizierungsprozess vier Dateien verarbeitet, dann inaktiv wird und anschließend fünf weitere Dateien verarbeitet, beträgt die Gesamtzahl der verarbeiteten Dateien neun. Prozesse werden nur beendet, wenn sie abgebrochen werden oder wenn die Anzahl Datendeduplizierungsprozesse für den Speicherpool in einen Wert geändert wird, der kleiner als die gegenwärtig angegebene Anzahl ist.

## Beispiel: Einen primären Speicherpool mit einer Einheitenklasse 8MMTAPE definieren

Den primären Speicherpool 8MMPool für die Einheitenklasse 8MMTAPE (mit Einheitentyp 8MM) mit einer maximalen Dateigröße von 5 MB definieren. Alle Dateien, die größer sind als 5 MB, in untergeordneten Pools speichern (beginnend bei Pool POOL1). Die Kollokation von Dateien für Clientknoten aktivieren. Maximal 5 Arbeitsdatenträger für diesen Speicherpool zulassen.

```
define stgpool 8mmpool 8mmtape maxsize=5m
nextstgpool=pool1 collocate=node
maxscratch=5
```

#### Zugehörige Verweise:

SET DRMDBBACKUPEXPIREDDAYS (Verfall für DB-Sicherungsserie angeben)

## DEFINE STGPOOL (Kopierspeicherpool definieren, der Einheiten mit sequenziellem Zugriff zugeordnet wird)

Mit diesem Befehl kann ein Kopierspeicherpool definiert werden, der Einheiten mit sequenziellem Zugriff zugeordnet wird.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DEFine STGpool--Poolname--Einheitenklassenname----->
>--POOLtype-----COPY--+-+-----+----->
      '-DESCRiption-----Beschreibung-'
      .-ACCess-----READWrite-----
>+-----+----->
      '-ACCess-----+READWrite----+'
          +-READOnly----+
          '-UNAVailable-'
      .-COLlocate-----No----- .-REClaim-----100-----
>+-----+-----+-----+----->
      '-COLlocate-----+No-----+'   '-REClaim-----Prozent-'
          +-GRoup-----+
          +-NODE-----+
          '-Filespace-'
      .-RECLAIMProcess-----1-----
>+-----+----->
      '-RECLAIMProcess-----Anzahl-'
      .-RECLAMATIOnType-----THRESHold-----
```

```

>-----+----->
|                                     (1) |
|'-RECLAMATIONType-----+THRESHold+-----'|
|                                     '-SNAPlock--'|

.-OFFSITERECLAIMLimit---NOLimit-.
>-----+-----+-----+-----+-----+----->
|'-OFFSITERECLAIMLimit---Anzahl---'|

.-REUsedelay---0---.
>-----+-----+-----+-----+----->
|'-REUsedelay---Tage-' '-OVFLocation---Standort-'|

.-DATAFormat---NATive-----|.
>-----+-----+-----+-----+----->
|                                     (2) |
|'-DATAFormat---+NATive-----+-----'|
|                                     +-NONblock----+|
|                                     +-NETAPPDump--+|
|                                     +-CELERRADump+  |
|                                     '-NDMPDump----'|

.-CRCDATA---No-----|. -DEDuplicate---No-----|.
>-----+-----+-----+-----+-----+----->
|'-CRCDATA---+Yes--+ '| '-DEDuplicate---+No-----+ '|
|                                     '-No-- '|          | (3) |
|                                     '|-Yes----- '|

.-IDENTIFYProcess---0-----|.
>-----+-----+-----+-----+-----><
|                                     (4) |
|'-IDENTIFYProcess---Anzahl-----'|

```

#### Anmerkungen:

1. Die Einstellung RECLAMATIONTYPE=SNAPLOCK ist nur für Speicherpools gültig, die für Server definiert sind, die für IBM Spectrum Protect for Data Retention aktiviert sind. Der Speicherpool muss einer Einheitenklasse FILE zugeordnet sein, und die in der Einheitenklasse angegebenen Verzeichnisse müssen NetApp SnapLock-Datenträger sein.
2. Die Werte NETAPPDUMP, CELERRADUMP und NDMPDUMP sind nicht für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.
3. Dieser Parameter ist nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.
4. Dieser Parameter ist nur verfügbar, wenn der Parameter DEDUPLICATE den Wert YES hat.

## Parameter

#### Poolname (Erforderlich)

Gibt den Namen des Speicherpools an, der definiert werden soll. Der Name muss eindeutig sein, und die maximale Länge beträgt 30 Zeichen.

#### Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse für den sequenziellen Zugriff an, der dieser Kopienspeicherpool zugeordnet ist. Mit Ausnahme von DISK kann jede Einheitenklasse angegeben werden.

#### POoltype=COpy (Erforderlich)

Gibt an, dass ein Kopienspeicherpool definiert werden soll.

#### DESCRiption

Gibt eine Beschreibung des Kopienspeicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

#### ACCess

Gibt an, wie Clientknoten und Serverprozesse (wie Wiederherstellung) auf Dateien im Kopienspeicherpool zugreifen können. Dieser Parameter ist wahlfrei. Der Standardwert ist READWRITE. Sie können die folgenden Werte angeben:

#### READWrite

Gibt an, dass Dateien auf die Datenträger im Kopienspeicherpool geschrieben und daraus gelesen werden können.

#### READOnly

Gibt an, dass Clientknoten Dateien, die auf den Datenträgern im Kopienspeicherpool gespeichert sind, nur lesen können.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Kopienspeicherpool verwenden, um Dateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Kopienspeicherpool sind jedoch keine neuen Schreiboperationen durch Datenträger außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht im Kopienspeicherpool gesichert werden.

#### UNAVailable

Gibt an, dass Clientknoten nicht auf Dateien zugreifen können, die auf Datenträgern im Kopienspeicherpool gespeichert sind.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Kopienspeicherpool verwenden, um Dateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Kopienspeicherpool sind jedoch keine neuen Schreiboperationen durch Datenträger außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht im Kopienspeicherpool gesichert werden.

#### COLlocate

Gibt an, ob der Server versucht, Daten, die zu den folgenden Kandidaten gehören, auf möglichst wenig Datenträgern zu speichern:

- Ein einzelner Clientknoten
- Eine Gruppe von Dateibereichen
- Eine Gruppe von Clientknoten
- Ein Clientdateibereich

Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

Die Kollokation reduziert die Anzahl der Ladevorgänge für Datenträger mit sequenziellem Zugriff für Zurückschreibungs-, Abruf- und Rückrufoperationen. Die Kollokation erfordert jedoch mehr Serverzeit, um Dateien zum Speichern zusammenzufassen, sowie eine größere Anzahl Datenträger.

Sie können eine der folgenden Optionen angeben:

#### No

Gibt an, dass die Kollokation inaktiviert ist.

#### GRoup

Gibt an, dass die Kollokation auf Gruppenebene für Clientknoten oder Dateibereiche aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten für Knoten oder Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf so wenig Datenträgern wie möglich zu speichern.

Wenn Sie COLLOCATE=GROUP angeben, aber keine Kollokationsgruppen definieren, oder wenn Sie keine Knoten oder Dateibereiche zu einer Kollokationsgruppe hinzufügen, werden Daten nach Knoten durch Kollokation zusammengefasst. Ziehen Sie die Verwendung von Bändern in Betracht, wenn Sie Clientknoten oder Dateibereiche in Kollokationsgruppen zusammenfassen.

Besteht beispielsweise ein bandbasierter Speicherpool aus Daten von Knoten, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst die Daten für gruppierte Knoten nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Knoten gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten für nicht gruppierte Knoten nach Knoten zusammen. Wenn möglich, speichert der Server die Daten für einen einzelnen Knoten auf einem einzelnen Band. Alle verfügbaren Bänder, die bereits Daten für den Knoten enthalten, werden verwendet, bevor verfügbarer Speicherbereich auf einem anderen Band verwendet wird.

Besteht ein bandbasierter Speicherpool aus Daten aus gruppierten Dateibereichen, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst nur die Daten für gruppierte Dateibereiche nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Dateibereichen gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Dateibereich können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten nach Knoten zusammen (für Dateibereiche, die nicht explizit für eine Dateibereichskollokationsgruppe definiert sind). Beispiel: Knoten1 hat die Dateibereiche A, B, C, D und E. Die Dateibereiche A und B gehören zu einer Dateibereichskollokationsgruppe, die Dateibereiche C, D und E dagegen nicht. Die Dateibereiche A und B werden nach Dateibereichskollokationsgruppe zusammengefasst, während die Dateibereiche C, D und E nach Knoten zusammengefasst werden.

Daten werden auf so wenig Datenträger mit sequenziellem Zugriff wie möglich zusammengefasst.

#### NODe

Gibt an, dass die Kollokation auf Clientknotenebene aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten eines Knotens auf so wenig Datenträgern wie möglich zu speichern. Verfügt der Knoten über mehrere Dateibereiche, versucht der Server nicht, diese Dateibereiche durch Kollokation zusammenzufassen. Für die Kompatibilität mit früheren Versionen wird COLLOCATE=YES noch vom Server akzeptiert, um die Kollokation auf der Clientknotenebene anzugeben.

Enthält ein Speicherpool Daten für einen Knoten, der Teil einer Kollokationsgruppe ist, und geben Sie COLLOCATE=NODE an, werden die Daten nach Knoten durch Kollokation zusammengefasst.

#### Filespace

Gibt an, dass die Kollokation auf der Dateibereichsebene für Clientknoten aktiviert ist. Der Server versucht, Daten eines Knotens und eines Dateibereichs auf so wenig Datenträgern wie möglich zu speichern. Verfügt ein Knoten über mehrere Dateibereiche, versucht der Server, Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern zu speichern.

#### REclaim

Gibt an, wann der Server einen Datenträger auf der Basis des Prozentsatzes wiederherstellbaren Speicherbereichs auf einem Datenträger zurückfordert. Der wiederherstellbare Speicherbereich ist der Speicherbereich, der durch Dateien belegt ist, die verfallen sind oder aus der IBM Spectrum Protect-Datenbank gelöscht wurden.

Bei der Wiederherstellung wird der zerstückelte Speicherbereich auf Datenträgern durch Versetzen der restlichen nicht verfallenen Dateien von einem Datenträger auf einen anderen wieder verwendbar, wodurch der ursprüngliche Datenträger wiederverwendet werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 100 angeben. Der Standardwert 100 bedeutet, dass keine Wiederherstellung erfolgt.

Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

Wird der Standardwert geändert, einen Wert von 50 Prozent oder höher angeben, so dass Dateien, die auf zwei Datenträgern gespeichert sind, auf einem einzigen Ausgabedatenträger gespeichert werden können.

Wenn ein ausgelagerter Kopierspeicherpoolatenträger für die Wiederherstellung ausgewählt werden kann, versucht der Wiederherstellungsprozess, die nicht verfallenen Dateien auf einem zurückforderbaren Datenträger aus einem primären Speicherpool oder einem Kopierspeicherpool vor Ort abzurufen. Der Prozess schreibt dann diese Dateien auf einen verfügbaren Datenträger in dem ursprünglichen Kopierspeicherpool. Tatsächlich werden diese Dateien wieder an den Standort vor Ort versetzt. Die Dateien können jedoch nach einem Katastrophenfall auch vom ausgelagerten Datenträger abgerufen werden, wenn eine Datenbanksicherung verwendet wird, die auf die Dateien auf dem ausgelagerten Datenträger verweist. Wegen der Art, mit der ausgelagerte Datenträger bei der Wiederherstellung bearbeitet werden, sollte die Wiederherstellung bei Kopierspeicherpools mit Vorsicht verwendet werden.

#### RECLAIMProcess

Gibt die Anzahl paralleler Prozesse für das Wiederherstellen der Datenträger in diesem Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein. Der Standardwert ist 1.

Berücksichtigen Sie bei der Berechnung des Werts für diesen Parameter die folgenden Ressourcen, die für die Wiederherstellungsverarbeitung erforderlich sind:

- Die Anzahl sequenzieller Speicherpools
- Die Anzahl logischer und physischer Laufwerke, die der Operation zugeordnet werden kann

Für den Zugriff auf Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk.

Beispiel: Angenommen, Sie möchten die Datenträger aus zwei Speicherpools mit sequenziellem Zugriff gleichzeitig wiederherstellen und Sie möchten vier Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Jeder Prozess benötigt zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um acht Wiederherstellungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 16 Mountpunkte und 16 Laufwerke. Die Einheitenklasse für die Speicherpools muss einen Grenzwert für Ladeanforderungen von mindestens 16 haben.

Sie können einen oder mehrere Wiederherstellungsprozesse für jeden Kopierspeicherpool angeben. Sie können mehrere gleichzeitig ablaufende Wiederherstellungsprozesse für einen einzelnen Kopierspeicherpool angeben. Damit wird eine bessere Nutzung Ihrer verfügbaren Bandlaufwerke oder FILE-Datenträger erreicht. Wenn die gleichzeitig ablaufende Verarbeitung mehrerer Prozesse nicht erforderlich ist, geben Sie den Wert 1 für den Parameter RECLAIMPROCESS an.

#### RECLAMATIONType

Gibt die Methode an, mit der Datenträger wiederhergestellt und verwaltet werden. Dieser Parameter ist wahlfrei. Der Standardwert ist THRESHOLD. Gültige Werte:

##### THRESHold

Gibt an, dass Datenträger, die zu diesem Speicherpool gehören, gemäß dem Schwellenwert im Attribut RECLAIM für diesen Speicherpool wiederhergestellt werden.

##### SNAPlock

Gibt an, dass FILE-Datenträger, die zu diesem Speicherpool gehören, mit NetApp Data ONTAP-Software und NetApp SnapLock-Datenträgern für die Aufbewahrung verwaltet werden. Dieser Parameter ist nur für Speicherpools gültig, die für

einen Server definiert sind, auf dem der Aufbewahrungsschutz für Daten aktiviert ist und der einer Einheitenklasse FILE zugeordnet ist. Datenträger in diesem Speicherpool werden nicht anhand des Schwellenwerts wiederhergestellt. Der RECLAIM-Wert für den Speicherpool wird ignoriert.

Alle Datenträger in diesem Speicherpool werden als FILE-Datenträger erstellt. Ein Aufbewahrungsdatum, das von den Aufbewahrungsattributen in der Archivierungskopiengruppe für den Speicherpool abgeleitet wird, wird in den Metadaten für den FILE-Datenträger mit der SnapLock-Funktion des Betriebssystems NetApp Data ONTAP definiert. Bis zum Ablauf des Aufbewahrungsdatums können der FILE-Datenträger und alle darauf befindlichen Daten nicht von dem physischen SnapLock-Datenträger gelöscht werden, auf dem sie gespeichert sind.

Der Parameter RECLAMATIONTYPE muss für alle Speicherpools, die definiert werden, identisch sein, wenn er für denselben Einheitenklassenamen definiert wird. Der Befehl DEFINE schlägt fehl, wenn der angegebene Parameter RECLAMATIONTYPE von der Angabe abweicht, die für Speicherpools definiert ist, die bereits für den Einheitenklassenamen definiert wurden.

#### OFFSITERECLAIMLimit

Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich während der Wiederherstellung für diesen Speicherpool zurückgefordert wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Sie können die folgenden Werte angeben:

##### NOLimit

Gibt an, dass der Speicherbereich auf allen ausgelagerten Datenträgern wiederhergestellt werden soll.

##### Anzahl

Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich wiederhergestellt werden soll. Sie können eine ganze Zahl von 0 bis 99999 angeben. Der Wert 0 bedeutet, dass für keine ausgelagerten Datenträger der Speicherbereich wiederhergestellt wird.

##### Tipp:

Um den Wert für OFFSITERECLAIMLIMIT zu bestimmen, verwenden Sie die statistischen Informationen in der Nachricht, die am Ende der Wiederherstellungsoperation für den ausgelagerten Datenträger ausgegeben wird. Die statistischen Informationen umfassen die folgenden Elemente:

- Die Anzahl der ausgelagerten Datenträger, die verarbeitet wurden
- Die Anzahl der parallelen Prozesse, die verwendet wurden
- Die Gesamtzeit, die für die Verarbeitung benötigt wurde

Die Reihenfolge, in der ausgelagerte Datenträger wiederhergestellt werden, basiert auf dem Umfang des freien Speicherplatzes auf einem Datenträger. (Freier Speicherplatz umfasst den Speicherbereich, der auf dem Datenträger nie verwendet wurde, und den Speicherbereich, der aufgrund des Löschs von Dateien frei geworden ist.) Datenträger mit dem größten freien Speicherplatz werden zuerst wiederhergestellt.

Beispiel: Angenommen, ein Kopierspeicherpool enthält drei Datenträger: VOL1, VOL2 und VOL3. VOL1 hat den größten freien Speicherplatz, und VOL3 hat den kleinsten freien Speicherplatz. Weiter wird angenommen, dass der Prozentsatz des freien Speicherplatzes auf jedem der drei Datenträger größer als der Wert des Parameters RECLAIM ist. Wird kein Wert für den Parameter OFFSITERECLAIMLIMIT angegeben, werden alle drei Datenträger wiederhergestellt, wenn die Wiederherstellung ausgeführt wird. Wird der Wert 2 angegeben, werden nur VOL1 und VOL2 bei der Wiederherstellung wiederhergestellt. Wird der Wert 1 angegeben, wird nur VOL1 wiederhergestellt.

#### MAXSCRatch (Erforderlich)

Gibt die maximale Anzahl der Arbeitsdatenträger an, die der Server für diesen Speicherpool anfordern kann. Sie können eine ganze Zahl von 0 bis 100000000 angeben. Wird dem Server das Anfordern von Arbeitsdatenträgern nach Bedarf erlaubt, muss der Benutzer nicht jeden zu verwendenden Datenträger definieren.

Mit dem für diesen Parameter angegebenen Wert wird die Gesamtzahl der im Kopierspeicherpool verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Kopierspeicherpools geschätzt.

Arbeitsdatenträger werden automatisch aus dem Speicherpool gelöscht, sobald sie leer sind. Lautet jedoch der Zugriffsmodus für einen Arbeitsdatenträger OFFSITE, wird der Datenträger erst dann aus dem Kopierspeicherpool gelöscht, wenn der Zugriffsmodus geändert wird. Ein Administrator kann dann den Server nach leeren ausgelagerten Arbeitsdatenträgern abfragen und diese an den Standort vor Ort zurückgeben.

Wenn Arbeitsdatenträger mit dem Einheitentyp FILE leer werden und gelöscht werden, wird der von den Datenträgern belegte Speicherbereich von dem Server freigegeben und an das Dateisystem zurückgegeben.

Tipp: Für serverübergreifende Operationen, die virtuelle Datenträger verwenden und ein kleines Datenvolumen speichern, sollte ein Wert für den Parameter MAXSCRATCH angegeben werden, der höher als der Wert ist, der normalerweise für Schreiboperationen für andere Datenträgertypen angegeben wird. Nach einer Schreiboperation auf einem virtuellen Datenträger markiert IBM Spectrum Protect den Datenträger als FULL, auch wenn der Wert des Parameters MAXCAPACITY in der

Einheitenklassendefinition noch nicht erreicht wurde. Der Server behält virtuelle Datenträger nicht im Status FILLING und hängt keine Daten an. Ist der Wert des Parameters MAXSCRATCH zu niedrig, können serverübergreifende Operationen fehlschlagen.

#### REUsedelay

Gibt die Anzahl Tage an, die nach dem Löschen aller Dateien von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerpool zurückgestellt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Standardwert ist 0, was bedeutet, dass ein Datenträger neu beschrieben oder in den Arbeitsdatenträgerpool zurückgestellt werden kann, sobald alle Dateien von dem Datenträger gelöscht wurden. Tipp: Mit diesem Parameter kann sichergestellt werden, dass Datenbankverweise auf Dateien im Kopierspeicherpool noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird. Dieser Parameter muss auf einen Wert gesetzt werden, der größer als die Anzahl der Tage ist, die die älteste Datenbanksicherung aufbewahrt werden soll. Die für diesen Parameter angegebene Anzahl Tage muss der im Befehl SET DRMDBBACKUPEXPIREDAYS angegebenen Anzahl entsprechen.

#### OVFLocation

Gibt den Überlaufstandort für den Speicherpool an. Der Server ordnet diesen Standortnamen einem Datenträger zu, der durch den Befehl aus dem Kassettenarchiv ausgegeben wird. Dieser Parameter ist wahlfrei. Der Standortname darf maximal 255 Zeichen lang sein. Den Standortnamen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

#### DATAFormat

Gibt das Datenformat an, das zum Sichern von Dateien in diesem Speicherpool und zum Zurückschreiben von Dateien aus diesem Speicherpool verwendet werden soll. Das Standardformat ist das NATIVE-Serverformat. Sie können die folgenden Werte angeben:

##### NATIVE

Gibt an, dass das Datenformat das native IBM Spectrum Protect-Serverformat ist und Block-Header einschließt.

##### NONblock

Gibt an, dass das Datenformat das native IBM Spectrum Protect-Serverformat ist und keine Block-Header einschließt. Die standardmäßige Mindestblockgröße auf einem Datenträger, der der Einheitenklasse FILE zugeordnet ist, beträgt 256 KB, unabhängig davon, wie viele Daten auf den Datenträger geschrieben werden. Für bestimmte Tasks können Sie die ineffiziente Speichernutzung auf Speicherdatenträgern minimieren, indem Sie das Datenformat NONBLOCK angeben. Sie können beispielsweise das Datenformat NONBLOCK für die folgenden Tasks angeben:

- Verwendung von Content-Management-Produkten
- Verwendung der Clientoption DIRMC zum Speichern von Verzeichnisinformationen
- Umlagerung sehr kleiner Dateien mit IBM Spectrum Protect for Space Management oder IBM Spectrum Protect HSM for Windows

In den meisten Situationen wird jedoch das native Format bevorzugt.

#### NETAPPDump

Gibt an, dass die Daten das NetApp-Speicherauszugsformat haben. Geben Sie dieses Datenformat nicht für Dateisystemimages an, die ein Speicherauszugsformat haben und die von einem NetApp-Dateiserver unter Verwendung von NDMP gesichert wurden. Der Server führt keine Speicherpoolwiederherstellung oder AUDIT VOLUME für einen Speicherpool mit DATAFORMAT=NETAPPDUMP aus. Sie können den Befehl MOVE DATA verwenden, um NDMP-generierte Daten von einem Datenträger zu versetzen, wenn der Datenträger wiederverwendet werden muss.

#### CELERRADump

Gibt an, dass die Daten das EMC Celerra-Speicherauszugsformat haben. Geben Sie dieses Datenformat nicht für Dateisystemimages an, die ein Speicherauszugsformat haben und die von einem EMC Celerra-Dateiserver unter Verwendung von NDMP gesichert wurden. Der Server führt keine Speicherpoolwiederherstellung oder AUDIT VOLUME für einen Speicherpool mit DATAFORMAT=CELERRADUMP aus. Sie können den Befehl MOVE DATA verwenden, um NDMP-generierte Daten von einem Datenträger zu versetzen, wenn der Datenträger wiederverwendet werden muss.

#### NDMPDump

Gibt an, dass die Daten ein lieferantenspezifisches NAS-Sicherungsformat haben. Geben Sie dieses Datenformat nicht für Dateisystemimages an, die ein Sicherungsformat haben und die von einem anderen NAS-Dateiserver als von einem NetApp- oder EMC Celerra-Dateiserver gesichert wurden. Der Server führt keine Speicherpoolwiederherstellung oder AUDIT VOLUME für einen Speicherpool mit DATAFORMAT=NDMPDUMP aus. Sie können den Befehl MOVE DATA verwenden, um NDMP-generierte Daten von einem Datenträger zu versetzen, wenn der Datenträger wiederverwendet werden muss.

#### CRCData

Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist nur für Speicherpools mit dem Datenformat NATIVE gültig. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCData auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

##### Yes

Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da eine zusätzliche Verarbeitung erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

##### No

Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

Tipp:

Für Speicherpools, die dem Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet sind, bietet der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust als die CRC-Überprüfung für einen Speicherpool. Wenn Sie die CRC-Überprüfung für einen Speicherpool angeben, werden Daten nur während der Ausführung von Datenträgerprüfungsoperationen überprüft. Fehler werden identifiziert, nachdem Daten auf Band geschrieben wurden.

Um den Schutz logischer Blöcke zu aktivieren, geben Sie den Wert READWRITE für den Parameter LBPROTECT in den Befehlen DEFINE DEVCLASS und UPDATE DEVCLASS für den Einheitentyp 3592, LTO oder ECARTRIDGE an. Der Schutz logischer Blöcke wird nur für die folgenden Typen von Laufwerken und Datenträgern unterstützt:

- IBM® LTO5 und höher
- IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
- Oracle StorageTek T10000C- und T10000D-Laufwerke

#### DEDuplicate

Gibt an, ob die in diesem Speicherpool gespeicherten Daten dedupliziert werden. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Der Standardwert ist NO.

#### IDENTIFYProcess

Gibt die Anzahl paralleler Prozesse an, die für die serverseitige Dateneduplizierung verwendet werden sollen. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Geben Sie einen Wert von 0 bis 50 ein.

Der Standardwert für diesen Parameter ist 0. Dateneduplizierungsprozesse für einen Kopierspeicherpool sind nicht erforderlich, wenn Sie Dateneduplizierungsprozesse für den primären Speicherpool angeben. Wenn IBM Spectrum Protect eine Datei in einem Speicherpool analysiert, analysiert IBM Spectrum Protect die Datei auch in allen anderen Speicherpools.

Hinweis: Dateneduplizierungsprozesse können entweder aktiv oder inaktiv sein. Prozesse, die gegenwärtig Dateien bearbeiten, sind aktiv. Prozesse, die auf Dateien warten, die bearbeitet werden sollen, sind inaktiv. Prozesse bleiben inaktiv, bis Datenträger mit Daten, die dedupliziert werden sollen, verfügbar werden. Die Ausgabe des Befehls QUERY PROCESS für einen Dateneduplizierungsprozess umfasst die Gesamtzahl Byte und Dateien, die seit dem ersten Start des Prozesses verarbeitet wurden. Wenn beispielsweise ein Dateneduplizierungsprozess vier Dateien verarbeitet, dann inaktiv wird und anschließend fünf weitere Dateien verarbeitet, beträgt die Gesamtzahl der verarbeiteten Dateien neun. Prozesse werden nur beendet, wenn sie abgebrochen werden oder wenn die Anzahl Dateneduplizierungsprozesse für den Speicherpool in einen Wert geändert wird, der kleiner als die gegenwärtig angegebene Anzahl ist.

## Beispiel: Einen Kopierspeicherpool mit einer Einheitenklasse DC480 definieren

Den Kopierspeicherpool TAPEPOOL2 für die Einheitenklasse DC480 definieren. Maximal 50 Arbeitsdatenträger für diesen Pool zulassen. Die Wiederverwendung der Datenträger um 45 Tage verzögern.

```
define stgpool tapepool2 dc480 pooltype=copy
maxscratch=50 reusedelay=45
```

#### Zugehörige Verweise:

SET DRMDBBACKUPEXPIREDAYS (Verfall für DB-Sicherungsserie angeben)

## DEFINE STGPOOL (Pool für aktive Daten definieren, der Einheiten mit sequenziellem Zugriff zugeordnet wird)

Mit diesem Befehl kann ein Pool für aktive Daten definiert werden, der Einheiten mit sequenziellem Zugriff zugeordnet wird.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DEFine STGpool--Poolname--Einheitenklassenname----->
>--POOLtype-----ACTIVEdata--+-+-----+----->
      '-DESCription-----Beschreibung-'
      .-ACCess-----READWrite----->
>+-----+-----+-----+----->
      '-ACCess-----+READWrite-----+'
```

```

+-READOnly----+
'-UNAVailable-'

.-COLlocate---No-----, .-REClaim---60-----.
>-----+-----+-----+-----+-----+-----+----->
'-COLlocate---+No-----+' '-REClaim---Prozent-'
      +-GRoup-----+
      +-NODE-----+
      '-Filespace-'

.-RECLAIMProcess---1-----.
>-----+-----+-----+-----+-----+-----+----->
'-RECLAIMProcess---Anzahl-'

.-RECLAMATIONType---THRESHold-----.
>-----+-----+-----+-----+-----+-----+----->
|                                     (1) |
'-RECLAMATIONType---+THRESHold+-----+'
      '-SNAPlock--'

.-OFFSITERECLAIMLimit---NOLimit-.
>-----+-----+-----+-----+-----+-----+----->
'-OFFSITERECLAIMLimit---Anzahl--'

.-REUsedelay---0----.
>-----+-----+-----+-----+-----+-----+----->
'-REUsedelay---Tage-' '-OVFLocation---Standort-'

.-DATAFormat---NATive-----, .-CRCDATA---No-----.
>-----+-----+-----+-----+-----+-----+----->
'-DATAFormat---+NATive---+' '-CRCDATA---+Yes-+'
      '-NONblock-'           '-No--'

.-DEDuplicate---No-----.
>-----+-----+-----+-----+-----+-----+----->
'-DEDuplicate---+No-----+'
      |               (2) |
      '-Yes-----'

.-IDENTIFYProcess---0-----.
>-----+-----+-----+-----+-----+-----+----->
|                                     (3) |
'-IDENTIFYProcess---Anzahl-----'

```

Anmerkungen:

1. Die Einstellung RECLAMATIONTYPE=SNAPLOCK ist nur für Speicherpools gültig, die für Server definiert sind, die für IBM Spectrum Protect for Data Retention aktiviert sind. Der Speicherpool muss einer Einheitenklasse FILE zugeordnet sein, und die in der Einheitenklasse angegebenen Verzeichnisse müssen NetApp SnapLock-Datenträger sein.
2. Dieser Parameter ist nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.
3. Dieser Parameter ist nur verfügbar, wenn der Parameter DEDUPLICATE den Wert YES hat.

## Parameter

### Poolname (Erforderlich)

Gibt den Namen des Speicherpools an, der definiert werden soll. Der Name muss eindeutig sein, und die maximale Länge beträgt 30 Zeichen.

### Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse für den sequenziellen Zugriff an, der dieser Pool für aktive Daten zugeordnet ist. Mit Ausnahme von DISK kann jede Einheitenklasse angegeben werden.

### POOLtype=ACTIVEdata (Erforderlich)

Gibt an, dass ein Pool für aktive Daten definiert werden soll.

### DESCRiption

Gibt eine Beschreibung des Pools für aktive Daten an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

### ACCess

Gibt an, wie Clientknoten und Serverprozesse (wie Wiederherstellung) auf Dateien im Pool für aktive Daten zugreifen können. Dieser Parameter ist wahlfrei. Der Standardwert ist READWRITE. Sie können die folgenden Werte angeben:

#### READWrite

Gibt an, dass Dateien auf die Datenträger im Pool für aktive Daten geschrieben und daraus gelesen werden können.

#### READOnly



Gibt an, dass Clientknoten Dateien, die auf den Datenträgern im Pool für aktive Daten gespeichert sind, nur lesen können.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Pool für aktive Daten verwenden, um Dateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Pool für aktive Daten sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht in den Pool für aktive Daten kopiert werden.

#### UNAVailable

Gibt an, dass Clientknoten nicht auf Dateien zugreifen können, die auf Datenträgern im Pool für aktive Daten gespeichert sind.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Pool für aktive Daten verwenden, um Dateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Pool für aktive Daten sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht in den Pool für aktive Daten kopiert werden.

#### COLlocate

Gibt an, ob der Server versucht, Daten, die zu den folgenden Kandidaten gehören, auf möglichst wenig Datenträgern zu speichern:

- Ein einzelner Clientknoten
- Eine Gruppe von Dateibereichen
- Eine Gruppe von Clientknoten
- Ein Clientdateibereich

Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

Die Kollokation reduziert die Anzahl der Ladevorgänge für Datenträger mit sequenziellem Zugriff für Zurückschreibungs-, Abruf- und Rückrufoperationen. Die Kollokation erfordert jedoch mehr Serverzeit, um Dateien zum Speichern zusammenzufassen, sowie eine größere Anzahl Datenträger.

Sie können eine der folgenden Optionen angeben:

#### No

Gibt an, dass die Kollokation inaktiviert ist.

#### GRoup

Gibt an, dass die Kollokation auf Gruppenebene für Clientknoten oder Dateibereiche aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten für Knoten oder Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf so wenig Datenträgern wie möglich zu speichern.

Wenn Sie COLLOCATE=GROUP angeben, aber keine Kollokationsgruppen definieren, oder wenn Sie keine Knoten oder Dateibereiche zu einer Kollokationsgruppe hinzufügen, werden Daten nach Knoten durch Kollokation zusammengefasst. Ziehen Sie die Verwendung von Bändern in Betracht, wenn Sie Clientknoten oder Dateibereiche in Kollokationsgruppen zusammenfassen.

Besteht beispielsweise ein bandbasierter Speicherpool aus Daten von Knoten, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst die Daten für gruppierte Knoten nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Knoten gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten für nicht gruppierte Knoten nach Knoten zusammen. Wenn möglich, speichert der Server die Daten für einen einzelnen Knoten auf einem einzelnen Band. Alle verfügbaren Bänder, die bereits Daten für den Knoten enthalten, werden verwendet, bevor verfügbarer Speicherbereich auf einem anderen Band verwendet wird.

Besteht ein bandbasierter Speicherpool aus Daten aus gruppierten Dateibereichen, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst nur die Daten für gruppierte Dateibereiche nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Dateibereichen gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Dateibereich können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten nach Knoten zusammen (für Dateibereiche, die nicht explizit für eine Dateibereichskollokationsgruppe definiert sind). Beispiel: Knoten1 hat die Dateibereiche A, B, C, D und E. Die Dateibereiche A und B gehören zu einer Dateibereichskollokationsgruppe, die Dateibereiche C, D und E dagegen nicht. Die Dateibereiche A und B werden nach Dateibereichskollokationsgruppe zusammengefasst, während die Dateibereiche C, D und E nach Knoten zusammengefasst werden.

Daten werden auf so wenig Datenträger mit sequenziellem Zugriff wie möglich zusammengefasst.

## NODE

Gibt an, dass die Kollokation auf Clientknotenebene aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten eines Knotens auf so wenig Datenträgern wie möglich zu speichern. Verfügt der Knoten über mehrere Dateibereiche, versucht der Server nicht, diese Dateibereiche durch Kollokation zusammenzufassen. Für die Kompatibilität mit früheren Versionen wird COLLOCATE=YES noch vom Server akzeptiert, um die Kollokation auf der Clientknotenebene anzugeben.

Enthält ein Speicherpool Daten für einen Knoten, der Teil einer Kollokationsgruppe ist, und geben Sie COLLOCATE=NODE an, werden die Daten nach Knoten durch Kollokation zusammengefasst.

## FILESpace

Gibt an, dass die Kollokation auf der Dateibereichsebene für Clientknoten aktiviert ist. Der Server versucht, Daten eines Knotens und eines Dateibereichs auf so wenig Datenträgern wie möglich zu speichern. Verfügt ein Knoten über mehrere Dateibereiche, versucht der Server, Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern zu speichern.

## RECLAIM

Gibt an, wann der Server einen Datenträger auf der Basis des Prozentsatzes wiederherstellbaren Speicherbereichs auf einem Datenträger zurückfordert. Der wiederherstellbare Speicherbereich ist der Speicherbereich, der durch Dateien belegt ist, die verfallen sind oder aus der IBM Spectrum Protect-Datenbank gelöscht wurden.

Bei der Wiederherstellung werden der fragmentierte Speicherbereich und der durch inaktive Sicherungsdateien belegte Speicherbereich auf Datenträgern durch Versetzen der restlichen nicht verfallenen Dateien und der aktiven Sicherungsdateien von einem Datenträger auf einen anderen Datenträger wieder verwendbar. Mit dieser Aktion kann der ursprüngliche Datenträger wiederverwendet werden. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 100 angeben. Der Standardwert ist 60.

Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

Wird der Standardwert geändert, einen Wert von 50 Prozent oder höher angeben, so dass Dateien, die auf zwei Datenträgern gespeichert sind, auf einem einzigen Ausgabedatenträger gespeichert werden können.

Wenn ein ausgelagerter Datenträger des Pools für aktive Daten für die Wiederherstellung ausgewählt werden kann, versucht der Wiederherstellungsprozess, die nicht verfallenen Dateien auf einem zurückforderbaren Datenträger aus einem primären Speicherpool oder einem Pool für aktive Daten vor Ort abzurufen. Der Prozess schreibt dann diese Dateien auf einen verfügbaren Datenträger in dem ursprünglichen Pool für aktive Daten. Tatsächlich werden diese Dateien wieder an den Standort vor Ort versetzt. Die Dateien können jedoch nach einem Katastrophenfall auch vom ausgelagerten Datenträger abgerufen werden, wenn eine Datenbanksicherung verwendet wird, die auf die Dateien auf dem ausgelagerten Datenträger verweist. Wegen der Art, mit der ausgelagerte Datenträger bei der Wiederherstellung bearbeitet werden, sollte die Wiederherstellung bei Pools mit aktiven Daten mit Vorsicht verwendet werden.

## RECLAIMPROCESS

Gibt die Anzahl paralleler Prozesse für das Wiederherstellen der Datenträger in diesem Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein. Der Standardwert ist 1.

Berücksichtigen Sie bei der Berechnung des Werts für diesen Parameter die folgenden Ressourcen, die für die Wiederherstellungsverarbeitung erforderlich sind:

- Die Anzahl sequenzieller Speicherpools
- Die Anzahl logischer und physischer Laufwerke, die der Operation zugeordnet werden kann

Für den Zugriff auf Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk.

Beispiel: Angenommen, Sie möchten die Datenträger aus zwei Speicherpools mit sequenziellem Zugriff gleichzeitig wiederherstellen und Sie möchten vier Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Jeder Prozess benötigt zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um acht Wiederherstellungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 16 Mountpunkte und 16 Laufwerke. Die Einheitenklasse für die Speicherpools muss einen Grenzwert für Ladeanforderungen von mindestens 16 haben.

Sie können einen oder mehrere Wiederherstellungsprozesse für jeden Pool für aktive Daten angeben. Sie können mehrere gleichzeitig ablaufende Wiederherstellungsprozesse für einen einzelnen Pool für aktive Daten angeben. Damit wird eine bessere Nutzung Ihrer verfügbaren Bandlaufwerke oder FILE-Datenträger erreicht. Wenn die gleichzeitig ablaufende Verarbeitung mehrerer Prozesse nicht erforderlich ist, geben Sie den Wert 1 für den Parameter RECLAIMPROCESS an.

## RECLAMATIONType

Gibt die Methode an, mit der Datenträger wiederhergestellt und verwaltet werden. Dieser Parameter ist wahlfrei. Der Standardwert ist THRESHOLD. Gültige Werte:

## THRESHold

Gibt an, dass Datenträger, die zu diesem Speicherpool gehören, gemäß dem Schwellenwert im Attribut RECLAIM für diesen Speicherpool wiederhergestellt werden.

## SNAPlock

Gibt an, dass FILE-Datenträger, die zu diesem Speicherpool gehören, mit NetApp Data ONTAP-Software und NetApp SnapLock-Datenträgern für die Aufbewahrung verwaltet werden. Dieser Parameter ist nur für Speicherpools gültig, die für einen Server definiert werden, auf dem der Aufbewahrungsschutz für Daten aktiviert ist und der einer Einheitenklasse FILE zugeordnet ist. Datenträger in diesem Speicherpool werden nicht anhand des Schwellenwerts wiederhergestellt. Der RECLAIM-Wert für den Speicherpool wird ignoriert.

Alle Datenträger in diesem Speicherpool werden als FILE-Datenträger erstellt. Ein Aufbewahrungsdatum, das von den Aufbewahrungsattributen in der Archivierungskopiengruppe für den Speicherpool abgeleitet wird, wird in den Metadaten für den FILE-Datenträger mit der SnapLock-Funktion des Betriebssystems NetApp Data ONTAP definiert. Bis zum Ablauf des Aufbewahrungsdatums können der FILE-Datenträger und alle darauf befindlichen Daten nicht von dem physischen SnapLock-Datenträger gelöscht werden, auf dem sie gespeichert sind.

Der Parameter RECLAMATIONTYPE muss für alle Speicherpools, die definiert werden, identisch sein, wenn er für denselben Einheitenklassennamen definiert wird. Der Befehl DEFINE schlägt fehl, wenn der angegebene Parameter RECLAMATIONTYPE von der Angabe abweicht, die für Speicherpools definiert ist, die bereits für den Einheitenklassennamen definiert wurden.

## OFFSITERECLAIMLimit

Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich während der Wiederherstellung für diesen Speicherpool zurückgefordert wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Sie können die folgenden Werte angeben:

### NOLimit

Gibt an, dass der Speicherbereich auf allen ausgelagerten Datenträgern wiederhergestellt werden soll.

### Anzahl

Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich wiederhergestellt werden soll. Sie können eine ganze Zahl von 0 bis 99999 angeben. Der Wert 0 bedeutet, dass für keine ausgelagerten Datenträger der Speicherbereich wiederhergestellt wird.

### Tipp:

Um den Wert für OFFSITERECLAIMLIMIT zu bestimmen, verwenden Sie die statistischen Informationen in der Nachricht, die am Ende der Wiederherstellungsoperation für den ausgelagerten Datenträger ausgegeben wird. Die statistischen Informationen umfassen die folgenden Elemente:

- Die Anzahl der ausgelagerten Datenträger, die verarbeitet wurden
- Die Anzahl der parallelen Prozesse, die verwendet wurden
- Die Gesamtzeit, die für die Verarbeitung benötigt wurde

Die Reihenfolge, in der ausgelagerte Datenträger wiederhergestellt werden, basiert auf dem Umfang des freien Speicherplatzes auf einem Datenträger. (Freier Speicherplatz umfasst den Speicherbereich, der auf dem Datenträger nie verwendet wurde, und den Speicherbereich, der aufgrund des Löschs von Dateien frei geworden ist.) Datenträger mit dem größten freien Speicherplatz werden zuerst wiederhergestellt.

Beispiel: Angenommen, ein Pool für aktive Daten enthält drei Datenträger: VOL1, VOL2 und VOL3. VOL1 hat den größten freien Speicherplatz, und VOL3 hat den kleinsten freien Speicherplatz. Weiter wird angenommen, dass der Prozentsatz des freien Speicherplatzes auf jedem der drei Datenträger größer als der Wert des Parameters RECLAIM ist. Wird kein Wert für den Parameter OFFSITERECLAIMLIMIT angegeben, werden alle drei Datenträger wiederhergestellt, wenn die Wiederherstellung ausgeführt wird. Wird der Wert 2 angegeben, werden nur VOL1 und VOL2 bei der Wiederherstellung wiederhergestellt. Wird der Wert 1 angegeben, wird nur VOL1 wiederhergestellt.

## MAXSCRatch (Erforderlich)

Gibt die maximale Anzahl der Arbeitsdatenträger an, die der Server für diesen Speicherpool anfordern kann. Sie können eine ganze Zahl von 0 bis 100000000 angeben. Wird dem Server das Anfordern von Arbeitsdatenträgern nach Bedarf erlaubt, muss der Benutzer nicht jeden zu verwendenden Datenträger definieren.

Mit dem für diesen Parameter angegebenen Wert wird die Gesamtzahl der im Pool für aktive Daten verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Pools für aktive Daten geschätzt.

Arbeitsdatenträger werden automatisch aus dem Speicherpool gelöscht, sobald sie leer sind. Lautet jedoch der Zugriffsmodus für einen Arbeitsdatenträger OFFSITE, wird der Datenträger erst dann aus dem Pool für aktive Daten gelöscht, wenn der Zugriffsmodus geändert wird. Ein Administrator kann dann den Server nach leeren ausgelagerten Arbeitsdatenträgern abfragen und diese an den Standort vor Ort zurückgeben.

Wenn Arbeitsdatenträger mit dem Einheitentyp FILE leer werden und gelöscht werden, wird der von den Datenträgern belegte Speicherbereich von dem Server freigegeben und an das Dateisystem zurückgegeben.

Tipp: Für serverübergreifende Operationen, die virtuelle Datenträger verwenden und ein kleines Datenvolumen speichern, sollte ein Wert für den Parameter MAXSCRATCH angegeben werden, der höher als der Wert ist, der normalerweise für Schreiboperationen für andere Datenträgertypen angegeben wird. Nach einer Schreiboperation auf einem virtuellen Datenträger markiert IBM Spectrum Protect den Datenträger als FULL, auch wenn der Wert des Parameters MAXCAPACITY in der Einheitenklassendefinition noch nicht erreicht wurde. Der Server behält virtuelle Datenträger nicht im Status FILLING und hängt keine Daten an. Ist der Wert des Parameters MAXSCRATCH zu niedrig, können serverübergreifende Operationen fehlschlagen.

#### REUsedelay

Gibt die Anzahl Tage an, die nach dem Löschen aller Dateien von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerpool zurückgestellt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Standardwert ist 0, was bedeutet, dass ein Datenträger neu beschrieben oder in den Arbeitsdatenträgerpool zurückgestellt werden kann, sobald alle Dateien von dem Datenträger gelöscht wurden. Tipp: Mit diesem Parameter kann sichergestellt werden, dass Datenbankverweise auf Dateien im Pool für aktive Daten noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird. Dieser Parameter muss auf einen Wert gesetzt werden, der größer als die Anzahl der Tage ist, die die älteste Datenbanksicherung aufbewahrt werden soll. Die für diesen Parameter angegebene Anzahl Tage muss der im Befehl SET DRMDBBACKUPEXPIREDAYS angegebenen Anzahl entsprechen.

#### OVFLocation

Gibt den Überlaufstandort für den Speicherpool an. Der Server ordnet diesen Standortnamen einem Datenträger zu, der durch den Befehl aus dem Kassettenarchiv ausgegeben wird. Dieser Parameter ist wahlfrei. Der Standortname darf maximal 255 Zeichen lang sein. Den Standortnamen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

#### DATAFormat

Gibt das Datenformat an, das zum Kopieren von Dateien in diesen Speicherpool und zum Zurückschreiben von Dateien aus diesem Speicherpool verwendet werden soll. Das Standardformat ist das NATIVE-Serverformat. Sie können die folgenden Werte angeben:

##### NATIVE

Gibt an, dass das Datenformat das native IBM Spectrum Protect-Serverformat ist und Block-Header einschließt.

##### NONblock

Gibt an, dass das Datenformat das native IBM Spectrum Protect-Serverformat ist und keine Block-Header einschließt. Die standardmäßige Mindestblockgröße auf einem Datenträger, der der Einheitenklasse FILE zugeordnet ist, beträgt 256 KB, unabhängig davon, wie viele Daten auf den Datenträger geschrieben werden. Für bestimmte Tasks können Sie die ineffiziente Speichernutzung auf Speicherdatenträgern minimieren, indem Sie das Datenformat NONBLOCK angeben. Sie können beispielsweise das Datenformat NONBLOCK für die folgenden Tasks angeben:

- Verwendung von Content-Management-Produkten
- Verwendung der Clientoption DIRMC zum Speichern von Verzeichnisinformationen
- Umlagerung sehr kleiner Dateien mit IBM Spectrum Protect for Space Management oder IBM Spectrum Protect HSM for Windows

In den meisten Situationen wird jedoch das native Format bevorzugt.

#### CRCDATA

Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist nur für Speicherpools mit dem Datenformat NATIVE gültig. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCDATA auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

##### Yes

Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da eine zusätzliche Verarbeitung erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

##### No

Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

#### Tipp:

Für Speicherpools, die dem Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet sind, bietet der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust als die CRC-Überprüfung für einen Speicherpool. Wenn Sie die CRC-Überprüfung für einen Speicherpool angeben, werden Daten nur während der Ausführung von Datenträgerprüfungsoperationen überprüft. Fehler werden identifiziert, nachdem Daten auf Band geschrieben wurden.

Um den Schutz logischer Blöcke zu aktivieren, geben Sie den Wert READWRITE für den Parameter LBPROTECT in den Befehlen DEFINE DEVCLASS und UPDATE DEVCLASS für den Einheitentyp 3592, LTO oder ECARTRIDGE an. Der Schutz logischer Blöcke wird nur für die folgenden Typen von Laufwerken und Datenträgern unterstützt:

- IBM® LTO5 und höher
- IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
- Oracle StorageTek T10000C- und T10000D-Laufwerke

## DEDuplicate

Gibt an, ob die in diesem Speicherpool gespeicherten Daten dedupliziert werden. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Der Standardwert ist NO.

## IDENTIFYProcess

Gibt die Anzahl paralleler Prozesse an, die für die serverseitige Dateneduplizierung verwendet werden sollen. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Geben Sie einen Wert von 0 bis 50 ein.

Der Standardwert für diesen Parameter ist 0. Dateneduplizierungsprozesse für einen Kopierspeicherpool sind nicht erforderlich, wenn Sie Dateneduplizierungsprozesse für den primären Speicherpool angeben. Wenn IBM Spectrum Protect eine Datei in einem Speicherpool analysiert, analysiert IBM Spectrum Protect die Datei auch in allen anderen Speicherpools.

Hinweis: Dateneduplizierungsprozesse können entweder aktiv oder inaktiv sein. Prozesse, die gegenwärtig Dateien bearbeiten, sind aktiv. Prozesse, die auf Dateien warten, die bearbeitet werden sollen, sind inaktiv. Prozesse bleiben inaktiv, bis Datenträger mit Daten, die dedupliziert werden sollen, verfügbar werden. Die Ausgabe des Befehls QUERY PROCESS für einen Dateneduplizierungsprozess umfasst die Gesamtzahl Byte und Dateien, die seit dem ersten Start des Prozesses verarbeitet wurden. Wenn beispielsweise ein Dateneduplizierungsprozess vier Dateien verarbeitet, dann inaktiv wird und anschließend fünf weitere Dateien verarbeitet, beträgt die Gesamtzahl der verarbeiteten Dateien neun. Prozesse werden nur beendet, wenn sie abgebrochen werden oder wenn die Anzahl Dateneduplizierungsprozesse für den Speicherpool in einen Wert geändert wird, der kleiner als die gegenwärtig angegebene Anzahl ist.

## Beispiel: Einen Pool für aktive Daten mit einer Einheitenklasse DC500 definieren.

---

Den Pool für aktive Daten TAPEPOOL2 für die Einheitenklasse DC500 definieren. Maximal 50 Arbeitsdatenträger für diesen Pool zulassen. Die Wiederverwendung der Datenträger um 45 Tage verzögern.

```
define stgpool tapepool3 dc500 pooltype=activedata
maxscratch=50 reusedelay=45
```

### Zugehörige Verweise:

SET DRMDBBACKUPEXPIREDDAYS (Verfall für DB-Sicherungsserie angeben)

## DEFINE STGPOOLDIRECTORY (Speicherpoolverzeichnis definieren)

---

Mit diesem Befehl können Sie ein oder mehrere Verzeichnisse in einem Verzeichniscontainer- oder Cloud-Containerspeicherpool definieren.

Tipp: Erstellen Sie nach der Definition eines Cloud-Containerspeicherpools ein oder mehrere Verzeichnisse, die für lokalen Speicher verwendet werden. Sie können während der Datenaufnahme Daten temporär im lokalen Speicher speichern, bevor die Daten in die Cloud versetzt werden. Auf diese Weise können Sie die Sicherungs- und Archivierungsleistung verbessern. Weitere Informationen finden Sie in Leistung für Cloudobjektspeicher optimieren.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```

      .-,-----
      v          |
>>-DEfIne STGPOOLDIRectory--Poolname-----Verzeichnisname-+-----<<
```

## Parameter

---

### Poolname (Erforderlich)

Gibt den Namen eines Verzeichniscontainer- oder Cloud-Containerspeicherpools an. Dieser Parameter ist erforderlich.

### Verzeichnisname (Erforderlich)

Gibt das Verzeichnis an, das in dem Speicherpool definiert werden soll. Dieser Parameter ist erforderlich. Sie können mehrere Verzeichnisnamen angeben, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden.

Wenn Sie den Verwaltungsclient verwenden und der Verzeichnisname ein Komma oder einen Backslash ("\") enthält, schließen Sie den Namen in Anführungszeichen ein.

## Beispiel: Ein Speicherpoolverzeichnis definieren

---

Definieren Sie ein Speicherpoolverzeichnis mit dem Namen DIR1 unter Verwendung eines Verzeichniscontainerspeicherpools mit dem Namen POOL1.

```
define stgpooldirectory pool1 /storage/dir1
```

```
define stgpooldirectory pool1 c:\storage\dir1
```

## Beispiel: Mehrere Speicherpoolverzeichnisse definieren

Definieren Sie Speicherpoolverzeichnisse mit dem Namen DIR1 und DIR2 unter Verwendung eines Verzeichniscontainerspeicherpools mit dem Namen POOL1.

```
define stgpooldirectory pool1 /storage/dir1,/storage/dir2
```

```
define stgpooldirectory pool1 e:\storage\dir1,f:\storage\dir2
```

## Beispiel: Lokalen Speicher für einen Cloud-Containerspeicherpool definieren

Erstellen Sie ein Speicherpoolverzeichnis mit dem Namen DIR3 in einem Cloud-Containerspeicherpool mit dem Namen CLOUDLOCALDISK1.

```
define stgpooldirectory cloudlocaldisk1 /storage/dir3
```

```
define stgpooldirectory cloudlocaldisk1 c:\storage\dir3
```

Tabelle 1. Zugehörige Befehle für DEFINE STGPOOLDIRECTORY

| Befehl                  | Beschreibung   |
|-------------------------|--|
| DEFINE STGPOOL          | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.                   |
| DELETE STGPOOLDIRECTORY | Löscht ein Speicherpoolverzeichnis aus einem Verzeichniscontainer- oder Cloud-Containerspeicherpool. |
| QUERY STGPOOLDIRECTORY  | Zeigt Informationen zu Speicherpoolverzeichnissen an.  |
| UPDATE STGPOOLDIRECTORY | Ändert die Attribute eines Speicherpoolverzeichnisses.   |

## DEFINE STGRULE (Speicherregel für Speicherpools definieren)

Verwenden Sie diesen Befehl, um eine Speicherregel für einen oder mehrere Speicherpools zu definieren. Die Speicherregel plant das Tiering zwischen Containerspeicherpools. Sie können eine oder mehrere Speicherregeln für einen Zielcontainerspeicherpool definieren.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DEFine STGRULE--Regelname--Zielspeicherpool----->
                                     .------
                                     v                                     |
>---ACTiontype---Tier-----SRCpools---Quellenpool+----->
    .-TIERDelay---30----- .-MAXPRocess---8-----
>+-----+-----+-----+-----+-----+----->
  '-TIERDelay---Verzögerung-' '-MAXPRocess---Anzahl-'
    .-DURation---NOLimit-.
>+-----+-----+-----+-----+-----+----->
```



## Speicherregel definieren

Eine Speicherregel mit dem Namen tieraction definieren, um Daten aus den Quellenverzeichniscontainerspeicherpools dirpool1 und dirpool2 in den Cloud-Zielcontainerspeicherpool cloudpool1 zu versetzen. Geben Sie als Startzeit 03:00 Uhr und ein Maximum von 10 Prozessen für eine Tiering-Speicherregel an:

```
define stgrule tieraction cloudpool1 srcpools=dirpool1,dirpool2
actiontype=tier maxprocess=10 starttime=03:00:00
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE STGRULE

| Befehl         | Beschreibung                                       |
|----------------|--|
| DELETE STGRULE | Löscht Speicherregeln für Speicherpools.           |
| QUERY STGRULE  | Zeigt Informationen zu Speicherregeln an.          |
| UPDATE STGRULE | Aktualisiert eine Speicherregel für Speicherpools. |

## DEFINE SUBSCRIPTION (Profilsubskription definieren)

Mit diesem Befehl kann ein verwalteter Server für ein Profil subskribiert werden.

Wenn ein Server für sein erstes Profil subskribiert, wird auch eine Subskription für das Standardprofil (falls vorhanden) des Konfigurationsmanagers erstellt. Der Server fragt dann den Konfigurationsmanager in regelmäßigen Abständen nach Konfigurationsaktualisierungen ab.

Einschränkungen:

1. Ein Server kann nicht für Profile von mehreren Konfigurationsmanagern subskribieren.
2. Wenn ein Server für ein Profil mit einem zugeordneten Objekt subskribiert, das bereits auf dem Server definiert ist, wird die lokale Definition durch die Definition vom Konfigurationsmanager ersetzt. Wenn ein Server beispielsweise über den Verwaltungszeitplan WEEKLY\_BACKUP verfügt, dann für ein Profil subskribiert, das ebenfalls einen Verwaltungszeitplan mit dem Namen WEEKLY\_BACKUP hat, wird die lokale Definition ersetzt.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-DEFine SUBSCRIPTION--Profilname--+-----+--<<
                                     '-SERVer-----Servername-'
```

## Parameter

Profilname (Erforderlich)

Gibt den Namen des Profils an, für das der Server subskribiert.

SERVer

Gibt den Namen des Konfigurationsmanagers an, von dem die Konfigurationsdaten abgerufen werden. Dieser Parameter ist erforderlich, wenn der verwaltete Server nicht mindestens eine Subskription hat. Hat der verwaltete Server eine Subskription, kann dieser Parameter übergangen werden. Als Standardwert wird dann der Konfigurationsmanager für diese Subskription verwendet.

## Beispiel: Eine Profilsubskription definieren

Das Profil BETA subskribieren, das sich auf dem Konfigurationsmanager TOM befindet.

```
define subscription beta server=tom
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE SUBSCRIPTION



| Befehl              | Beschreibung   |
|---------------------|--|
| COPY PROFILE        | Erstellt eine Kopie eines Profils.   |
| DEFINE PROFILE      | Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.                  |
| DELETE PROFILE      | Löscht ein Profil aus einem Konfigurationsmanager.   |
| DELETE SUBSCRIBER   | Löscht veraltete Subskriptionen verwalteter Server.  |
| DELETE SUBSCRIPTION | Löscht eine angegebene Profilsubskription.   |
| LOCK PROFILE        | Verhindert die Verteilung eines Konfigurationsprofils.   |
| NOTIFY SUBSCRIBERS  | Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin.                 |
| QUERY PROFILE       | Zeigt Informationen über Konfigurationsprofile an.   |
| QUERY SUBSCRIBER    | Zeigt Informationen über Subskribenten und ihre Subskriptionen für Profile an.                   |
| QUERY SUBSCRIPTION  | Zeigt Informationen über Profilsubskriptionen an.  |
| SET CONFIGREFRESH   | Gibt das Zeitintervall an, in dem verwaltete Server die Konfigurationsmanager ansprechen sollen. |
| UNLOCK PROFILE      | Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server.                         |
| UPDATE PROFILE      | Ändert die Beschreibung eines Profils.   |

## DEFINE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs definieren)

Verwenden Sie diesen Befehl, um eine Zuordnung des virtuellen Dateibereichs zu definieren.

Namen von virtuellen Dateibereichen können in den NAS-Datenoperationen BACKUP NODE und RESTORE NODE ähnlich wie Dateisystemnamen verwendet werden. Die Dokumentation zu Ihrer NAS-Einheit enthält Anleitungen zur Angabe der Parameter für diesen Befehl.

Anmerkung: Dem NAS-Knoten muss eine Definition für eine Einheit zum Versetzen von Daten zugeordnet sein, da bei der Aktualisierung der Zuordnung eines virtuellen Dateibereichs durch den IBM Spectrum Protect-Server der Server versucht, die NAS-Einheit anzusprechen, um das virtuelle Dateisystem und den Dateisystemnamen zu prüfen.

### Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Systemberechtigung
- Uneingeschränkte Maßnahmenberechtigung
- Eingeschränkte Maßnahmenberechtigung für die Domäne, der der NAS-Knoten zugeordnet ist

### Syntax

```
>>-DEfine VIRTUALFSmapping -Knotenname----->
>--Name_des_virtuellen_Dateibereichs--Dateisystemname--Pfad----->
. -NAMeType----SERVER-----
>-----+-----+-----><
' -NAMeType----+SERVER-----+'
      '-HEXadecimal-'
```

### Parameter

Knotenname (Erforderlich)

Gibt den NAS-Knoten an, auf dem sich das Dateisystem und der Pfad befinden. Sie können keine Platzhalterzeichen verwenden und keine Liste mit Namen angeben.

#### Name\_des\_virtuellen\_Dateibereichs (Erforderlich)

Gibt den Namen an, der auf diese Definition des virtuellen Dateibereichs verweist. Bei dem Namen des virtuellen Dateibereichs muss die Groß-/Kleinschreibung beachtet werden, und das erste Zeichen muss ein Schrägstrich / sein. Die Länge des Namens darf 64 Zeichen, einschließlich des erforderlichen Schrägstrichs, nicht überschreiten. Die Namen der virtuellen Dateibereiche sind auf denselben Zeichensatz wie alle anderen Objekte im Server beschränkt, mit der Ausnahme, dass auch der Schrägstrich / zulässig ist.

Der Name des virtuellen Dateibereichs darf mit keinem Dateisystem auf dem NAS-Knoten übereinstimmen. Beachten Sie bei der Auswahl des Namens für einen virtuellen Dateibereich die folgenden Einschränkungen:

- Wird auf der NAS-Einheit ein Dateisystem mit demselben Namen wie ein virtuelles Dateisystem erstellt, tritt eine Namensunverträglichkeit auf dem Server auf, wenn der neue Dateibereich gesichert wird. Verwenden Sie eine Zeichenfolge für den Namen des virtuellen Dateibereichs, die in der Zukunft wahrscheinlich nicht als Name eines realen Dateisystems auf Ihrer NAS-Einheit verwendet wird.

Beispiel: Ein Benutzer verwendet die Namenskonvention zum Erstellen von Dateibereichen auf einer NAS-Einheit mit Namen in der Form /vol1, /vol2, /vol3. Der Benutzer definiert einen virtuellen Dateibereich für den Server mit dem Namen /vol9. Wenn der Benutzer weiterhin dieselbe Namenskonvention verwendet, wird der Name des virtuellen Dateibereichs irgendwann in der Zukunft mit dem Namen eines realen Dateibereichs in Konflikt stehen.

- Bei Sicherungs- und Zurückschreibungsoperationen prüft der Server vor dem Starten der Operation, ob eine Namensunverträglichkeit vorliegt.
- Der Name des virtuellen Dateibereichs erscheint in der Ausgabe des Befehls QUERY FILESPACE sowie in den Sicherungs- und Zurückschreibungsanzeigen des IBM Spectrum Protect-Web-Clients als Dateibereich. Wählen Sie daher einen Namen aus, der dieses Objekt eindeutig als Verzeichnispfad auf der NAS-Einheit identifiziert.

#### Dateisystemname (Erforderlich)

Gibt den Namen des Dateisystems an, in dem sich der Pfad befindet. Der Dateisystemname muss auf dem angegebenen NAS-Knoten vorhanden sein. Der Dateisystemname darf keine Platzhalterzeichen enthalten.

#### Pfad (Erforderlich)

Gibt den Pfad vom Stamm des Dateisystems zum Verzeichnis an. Der Pfad kann nur auf ein Verzeichnis verweisen. Die maximale Länge des Pfads beträgt 1024 Zeichen. Bei dem Pfadnamen muss die Groß-/Kleinschreibung beachtet werden.

#### NAMEType

Gibt an, wie der Server den angegebenen Pfadnamen interpretieren soll. Dieser Parameter ist nützlich, wenn ein Pfad Zeichen enthält, die nicht Teil der Codepage sind, in der der Server ausgeführt wird. Der Standardwert lautet SERVER.

Gültige Werte:

SERVER

Der Server verwendet die Codepage des Servers, um den Pfadnamen zu interpretieren.

HEXadecimal

Der Server interpretiert den eingegebenen Pfad als hexadezimale Darstellung des Pfads. Diese Option sollte verwendet werden, wenn ein Pfad Zeichen enthält, die nicht eingegeben werden können. Diese Situation kann auftreten, wenn für das NAS-Dateisystem eine Sprache definiert ist, die von der Sprache abweicht, in der der Server ausgeführt wird.

## Beispiel: Eine Zuordnung des virtuellen Dateibereichs definieren

Den Namen /mikeshomedir für die Zuordnung des virtuellen Dateibereichs für den Pfad /home/mike in dem Dateisystem /vol/vol1 auf dem NAS-Knoten NAS1 definieren.

```
define virtualfsmapping nas1 /mikeshomedir /vol/vol1 /home/mike
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE VIRTUALFSMAPPING



| Befehl                  | Beschreibung                                       |
|-------------------------|--|
| DELETE VIRTUALFSMAPPING | Zuordnung eines virtuellen Dateibereichs löschen.  |
| QUERY VIRTUALFSMAPPING  | Zuordnung eines virtuellen Dateibereichs abfragen. |

| Befehl                  | Beschreibung  |
|-------------------------|---|
| UPDATE VIRTUALFSMAPPING | Zuordnung eines virtuellen Dateibereichs aktualisieren. |

## DEFINE VOLUME (Datenträger in einem Speicherpool definieren)

Mit diesem Befehl kann einem Speicherpool ein Datenträger mit wahlfreiem Zugriff oder mit sequenziellem Zugriff zugeordnet werden.

Wenn Sie einen Speicherpool datenträger mit wahlfreiem Zugriff (DISK) oder einen Speicherpool datenträger mit sequenziellem Zugriff definieren, der einer Einheitenklasse FILE zugeordnet ist, kann der Datenträger von dem Server erstellt werden, bevor er zugeordnet wird. Sie können auch Speicherbereichsauslöser verwenden, um im voraus zugeordnete Datenträger zu erstellen, wenn zuvor festgelegte Schwellenwerte für die Speicherauslastung überschritten wurden. Ausführliche Informationen zu Speicherbereichsauslösern befinden sich in DEFINE SPACETRIGGER (Speicherbereichsauslöser definieren). Für Datenträger, die anderen Einheitenklassen als DISK oder anderen Einheitentypen als FILE zugeordnet sind, können Sie den Befehl DEFINE VOLUME verwenden, um einen bereits erstellten Datenträger einem Speicherpool zuzuordnen.


 **AIX-Betriebssysteme**  **Linux-Betriebssysteme** Wenn Sie eine Einheitenklasse FILE für Speicher verwenden, der von einem z/OS Media-Server verwaltet wird, ist es nicht erforderlich, Datenträger zu formatieren oder zu definieren. Wenn Sie einen Datenträger für eine solche Einheitenklasse FILE mit dem Befehl DEFINE VOLUME definieren, ordnet der z/OS Media-Server erst dann Speicherbereich für den Datenträger zu, wenn der Datenträger für seine erste Verwendung geöffnet wird.


**Achtung:** Datenträger für den z/OS Media-Server, die mit dem Befehl DEFINE VOLUME erstellt werden, bleiben physisch voll oder zugeordnet, nachdem der Server den Datenträger leert, wie beispielsweise nach der Verfallsverarbeitung oder der Wiederherstellung. Bei FILE-Datenträgern wird der DASD-Speicherbereich nicht für das System freigegeben, wenn der Datenträger geleert wird. Wenn ein Speicherpool einen leeren Datenträger oder einen Datenträger, der gefüllt wird, erfordert, kann der FILE-Datenträger verwendet werden. Im Gegensatz dazu sind Banddatenträger, die logisch leer sind, auch physisch leer. FILE-Datenträger und Banddatenträger bleiben im Server definiert. Dagegen werden Arbeitsdatenträger, einschließlich des physischen Speichers, der FILE-Arbeitsdatenträgern zugeordnet ist, nach der Leerung an das System zurückgegeben.

Um Speicherbereich in Speicherpools mit sequenziellem Zugriff zu erstellen, können Sie Datenträger definieren, oder Sie können es dem Server erlauben, bei Bedarf Arbeitsdatenträger anzufordern, wie mit dem Parameter MAXSCRATCH für den Speicherpool angegeben ist. Für Speicherpools, die der Einheitenklasse FILE zugeordnet sind, kann der Server bei Bedarf unter Verwendung von Speicherbereichsauslösern für den Speicherpool private Datenträger erstellen. Für DISK-Speicherpools ist der Arbeitsdatenträgermechanismus nicht verfügbar. Sie können jedoch Speicherbereich erstellen, indem Sie Datenträger erstellen und dann die Datenträger für den Server definieren. Alternativ kann der Server Datenträger erstellen, die Speicherbereichsauslöser für den Speicherpool verwenden.


Der Server prüft nicht das Vorhandensein eines Datenträgernamens, wenn ein Datenträger in einem Speicherpool definiert wird, der einem Kassettenarchiv zugeordnet ist. Der definierte Datenträger hat die geschätzte Kapazität "0", bis Daten auf den Datenträger geschrieben werden.

**Achtung:** Die Größe eines Speicherpool datenträgers kann nicht mehr geändert werden, nachdem sie für den Server definiert wurde.

 **AIX-Betriebssysteme** Wenn Sie die Größe von IBM Spectrum Protect-Datenträgern ändern, indem Sie unformatierte logische Datenträger mit SMIT erweitern oder indem Sie die Dateigrößen der Datenträger mit Betriebssystembefehlen oder Dienstprogrammen ändern, wird der Server möglicherweise nicht korrekt initialisiert und es können Daten verloren gehen.

 **Windows-Betriebssysteme** Wenn Sie die Größe von Datenträgern ändern, indem Sie die Dateigrößen der Datenträger mit Betriebssystembefehlen oder Dienstprogrammen ändern, wird der Server möglicherweise nicht korrekt initialisiert und es können Daten verloren gehen.

Einschränkungen:

- Sie können diesen Befehl nicht verwenden, um Datenträger in Speicherpools mit der Parametereinstellung RECLAMATIONTYPE=SNAPLOCK zu definieren. Datenträger in diesem Typ des Speicherpools werden mit dem Parameter MAXSCRATCH in der Speicherpooldefinition zugeordnet.
- Sie können keine Datenträger in einem Speicherpool definieren, der mit der Einheitenklasse CENTERA definiert ist.
-  **Linux-Betriebssysteme** Sie können keine unformatierten logischen Datenträger für Speicherpool datenträger verwenden.

Physische Dateien, die mit dem Befehl DEFINE VOLUME zugeordnet werden, werden nicht aus einem Dateibereich entfernt, wenn Sie den Befehl DELETE VOLUME ausgeben.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool erforderlich, dem der Datenträger zugeordnet ist.



| Anforderungen für Datenträgername   | Beispiel   |
|---|--|
| <p>Der Name der Datei, die die Datenträgerdaten enthalten soll, entweder mit dem vollständig qualifizierten Pfadnamen oder mit einem Pfadnamen, der sich auf das aktuelle Arbeitsverzeichnis bezieht.</p> <p> Enthält ein Name eingebettete Leerzeichen, Gleichheitszeichen oder andere Sonderzeichen, ist die Liste in Anführungszeichen einzuschließen.</p> | <p> <br/>/usr/storage/sbkup01.dsm</p> <p> Wird ein logischer AIX-Datenträger verwendet, geben Sie den Pfadnamen wie folgt ein:<br/>/dev/rxxx</p> <p>xxx ist der Name des logischen Datenträgers.<br/><br/>"c:\program files\tivoli\tsm\server\data3.dsm"</p> |

Tabelle 2. Anforderungen an Datenträgernamen für FILE

| Anforderungen für Datenträgername  | Beispiel   |
|--|--|
| <p>Der Name der Datei, die die Datenträgerdaten enthalten soll, entweder mit dem vollständig qualifizierten Pfadnamen oder mit dem Pfadnamen, der sich auf ein Verzeichnis bezieht, das im Parameter DIRECTORY für die Einheitenklasse angegeben ist.</p> <p> Enthält ein Name eingebettete Leerzeichen, Gleichheitszeichen oder andere Sonderzeichen, ist die Liste in Anführungszeichen einzuschließen.</p> <p>Stellen Sie FILE-Datenträger in eines der Verzeichnisse, die mit dem Parameter DIRECTORY des Befehls DEFINE DEVCLASS angegeben werden. Andernfalls haben Speicheragenten möglicherweise keinen Zugriff auf die Datenträger. Ausführliche Informationen siehe DEFINE PATH (Pfad definieren).</p> | <p> <br/>/data/fpool01.dsm</p> <p><br/>"f:\data storage\fpool01.dsm"</p> |

Tabelle 3. z/OS Media-Server: Anforderungen an Datenträgernamen für FILE

| Anforderungen für Datenträgername | Beispiel |
|-----------------------------------|----------|
|-----------------------------------|----------|

| Anforderungen für Datenträgername   | Beispiel   |
|---|--|
| <p>Geben Sie für FILE-Datenträger, die mit dem z/OS Media-Server verwendet werden, einen Dateinamen an. Der Dateiname kann aus einem oder aus mehreren Qualifikationsmerkmalen bestehen, die durch einen Punkt begrenzt werden. Die Qualifikationsmerkmale können maximal 8 Zeichen enthalten. Die maximale Länge des Dateinamens beträgt 44 Zeichen. Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@#\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.</p> <p>Um die zugehörige lineare VSAM-Datei zuzuordnen, wenn der Datenträger auf dem z/OS-System bereitgestellt wird, wird das Qualifikationsmerkmal der höheren Ebene (High Level Qualifier - HLQ) normalerweise von bestimmten ACS-Routinen innerhalb der SMS-Maßnahmenvorgaben auf dem System gefiltert, auf dem der z/OS Media-Server ausgeführt wird.</p> <p>Das Verhalten des Qualifikationsmerkmals der höheren Ebene ähnelt dem Verhalten des PREFIX-Namens bei der Anforderung eines Arbeitsdatenträgers. Das Qualifikationsmerkmal der höheren Ebene wird normalerweise von DFSMS für Zuordnungsattribute verwendet, wie z. B. für die erweiterte Adressierbarkeit für Dateien, von denen eine Erweiterung erwartet wird, wenn der Speicherbereich, der dem Dateidatenträger bereits zugeordnet ist, belegt ist.</p> <p>Wenn die Datei nicht vorhanden ist, wird sie vom Server erstellt, wenn der Datenträger für eine bestimmte IBM Spectrum Protect-Speicheroperation verwendet wird. Die Datei wird nicht erstellt, wenn der Datenträger definiert ist. Ein Datenverlust kann auftreten, wenn Datenträger definiert werden, da der Datenträger oder die lineare VSAM-Datei vom z/OS Media-Server wiederverwendet wird, wenn er bzw. sie zum Zeitpunkt der Zuordnung vorhanden ist.</p> <p>Wichtig: Um dem Server die Erstellung von Datenträgernamen zu ermöglichen, ziehen Sie die Verwendung von Arbeitsdatenträgern in Betracht.</p> |  <br>SERVER1 . BFS . POOL3 . VOLA |

Tabelle 4. Anforderungen an Datenträgernamen für Band

| Anforderungen für Datenträgername   | Beispiel |
|---|----------|
| Verwenden Sie 1 - 32 alphanumerische Zeichen.   | DSMT01   |
| Der Datenträgername darf keine eingebetteten Leerzeichen oder Gleichheitszeichen enthalten. |          |

Tabelle 5. z/OS Media-Server: Anforderungen an Datenträgernamen für Band

| Anforderungen für Datenträgername | Beispiel |
|-----------------------------------|----------|
|-----------------------------------|----------|

| Anforderungen für Datenträgername   | Beispiel |
|---|----------|
| <p>Geben Sie für Bandkassetten einen Banddatenträgernamen mit 1 - 6 alphanumerischen Zeichen an. Der Server setzt Banddatenträgernamen in Großbuchstaben um.</p> <p>Der Datenträgername darf keine eingebetteten Leerzeichen oder Gleichheitszeichen enthalten.</p> <p>Jeder Datenträger, der von einem Server für einen beliebigen Zweck verwendet wird, muss einen eindeutigen Namen haben. Diese Anforderung gilt für alle Datenträger, unabhängig davon, ob die Datenträger für Speicherpools oder für Operationen, wie beispielsweise Datenbanksicherung oder -export, verwendet werden. Die Anforderung gilt auch für Datenträger, die sich in verschiedenen z/OS-Kassettenarchiven befinden, die aber von demselben Server verwendet werden.</p> | DSMT01   |

Tabelle 6. Anforderungen an Datenträgernamen für REMOVABLEFILE

| Anforderungen für Datenträgername   | Beispiel |
|---|----------|
| <p>1–6 alphanumerische Zeichen</p> <p>Der Server setzt Datenträgernamen in Großbuchstaben um.</p> | DSM01    |

#### ACcESS

Gibt an, wie Clientknoten und Serverprozesse (wie Umlagerung) auf Dateien auf dem Speicherpooldatenträger zugreifen können. Dieser Parameter ist wahlfrei. Der Standardwert ist READWRITE. Gültige Werte:

#### READWrite

Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff auf Dateien des Datenträgers haben.

#### READOnly

Gibt an, dass Clientknoten und Serverprozesse nur Lesezugriff auf Dateien des Datenträgers haben.

#### UNAVailable

Gibt an, dass Clientknoten oder Serverprozesse nicht auf Dateien zugreifen können, die auf dem Datenträger gespeichert sind.

Wird ein Datenträger mit wahlfreiem Zugriff als UNAVAILABLE definiert, kann der Datenträger nicht angehängt werden.

Wird ein Datenträger mit sequenziellem Zugriff als UNAVAILABLE definiert, versucht der Server nicht, auf den Datenträger zuzugreifen.

#### OFFsite

Gibt an, dass sich der Datenträger an einem ausgelagerten Standort befindet, von dem er nicht geladen werden kann. Sie können diesen Wert nur für Datenträger in Kopierspeicherpools oder Speicherpools für aktive Daten angeben.

Mit diesem Wert können Datenträger an ausgelagerten Standorten verfolgt werden. Der Server behandelt ausgelagerte Datenträger anders:

- Der Server generiert keine Ladeanforderungen für ausgelagerte Datenträger.
- Der Server fordert Daten von ausgelagerten Datenträgern zurück oder versetzt Daten von ausgelagerten Datenträgern, indem Dateien aus anderen Speicherpools abgerufen werden.
- Der Server löscht nicht automatisch leere ausgelagerte Arbeitsdatenträger aus einem Kopierspeicherpool oder Speicherpool für aktive Daten.

#### LOCation

Gibt den Standort des Datenträgers an. Dieser Parameter ist wahlfrei. Er kann nur für Datenträger in Speicherpools mit sequenziellem Zugriff angegeben werden. Die Standortinformationen dürfen eine maximale Länge von 255 Zeichen haben. Wenn die Beschreibung des Standorts Leerzeichen enthält, muß sie in Anführungszeichen stehen.

#### FormAtsize

Gibt die Größe des Datenträgers mit wahlfreiem Zugriff oder des FILE-Datenträgers an, der in einem Schritt erstellt und formatiert wird. Der Wert wird in Megabyte angegeben. Die maximale Größe beträgt 8 000 000 MB (8 Terabyte). Dieser Parameter ist erforderlich, wenn eine der folgenden Bedingungen zutrifft:

- Ein einzelner FILE- oder DISK-Datenträger wird angegeben, der in einem Schritt erstellt und formatiert werden soll.
- Der Wert für den Parameter NUMBEROFVOLUMES ist größer als 1, und DISK-Datenträger werden erstellt.

- Der Wert des Parameters NUMBEROFVOLUMES ist größer als 1 und der Wert des Parameters FORMATSIZE ist kleiner-gleich dem Parameter MAXCAPACITY des Befehls DEFINE DEVCLASS.

Wenn Sie Datenträger auf einem z/OS Media-Server zuordnen, ist dieser Parameter nicht gültig.

Für einen FILE-Datenträger müssen Sie einen Wert kleiner-gleich dem Wert des Parameters MAXCAPACITY der Einheitenklasse angeben, die dem Speicherpool zugeordnet ist.

Sie können diesen Parameter nicht für mehrere vordefinierte Datenträger verwenden. Die Operation wird als Hintergrundprozess ausgeführt, wenn nicht `WAIT=YES` angegeben wird.

#### Numberofvolumes

Gibt die Anzahl der Datenträger an, die in einem Schritt erstellt und formatiert werden. Dieser Parameter gilt nur für Speicherpools mit Einheitenklassen DISK oder FILE. Dieser Parameter ist wahlfrei. Der Standardwert ist 1. Wird ein Wert größer als 1 angegeben, müssen Sie auch einen Wert für den Parameter FORMATSIZE angeben. Geben Sie eine Zahl von 1 bis 256 an.

Wenn Sie Datenträger auf einem z/OS Media-Server zuordnen, ist der einzige von diesem Parameter unterstützte Wert der Standardwert 1.

Ist der Wert für den Parameter NUMBEROFVOLUMES größer als 1, wird dem angegebenen Datenträgernamen ein numerisches Suffix angehängt, um jeden Namen zu erstellen, z. B. tivolivol001 und tivolivol002. Stellen Sie sicher, dass ein Datenträgername ausgewählt wird, mit dem ein gültiger Dateiname für das Zielsdateisystem erstellt wird, wenn das Suffix angehängt wird.

Wichtig: Sie müssen sicherstellen, dass Speicheragenten auf neu erstellte FILE-Datenträger zugreifen können. Weitere Informationen siehe DEFINE PATH (Pfad definieren).

#### Wait

Gibt an, ob eine Erstellungs- und Formatierungsoperation für einen Datenträger im Vordergrund oder im Hintergrund ausgeführt wird. Dieser Parameter ist wahlfrei. Er wird ignoriert, es sei denn, Sie geben auch den Parameter FORMATSIZE an.






#### No

Gibt an, dass eine Erstellungs- und Formatierungsoperation für einen Datenträger im Hintergrund ausgeführt wird. Der Wert NO ist der Standardwert, wenn auch eine Formatgröße angegeben wird.

#### Yes

Gibt an, dass eine Erstellungs- und Formatierungsoperation für einen Datenträger im Vordergrund ausgeführt wird. Hinweis: Sie können nicht `WAIT=YES` an der Serverkonsole angeben.

## Beispiel: Einen Hintergrundprozess verwenden, um einen neuen Datenträger mit 100 MB für einen Plattenspeicherpool zu definieren

Einen Datenträger mit 100 MB in dem Plattenspeicherpool BACKUPPOOL erstellen.    
Der Datenträgername lautet /var/storage/bf.dsm.  Der Datenträgername lautet j:\storage\bf.dsm. Der Datenträger soll als Hintergrundprozess erstellt werden.  

```
define volume backuppool
/var/storage/bf.dsm formatsize=100
```




```
define volume backuppool j:\storage\bf.dsm formatsize=100
```


## Beispiel: Einen Datenträger für einen Plattenspeicherpool mit Lese- und Schreibzugriff definieren


Der Speicherpool POOL1 ist einer Bandeinheitenklasse zugeordnet. Den Datenträger TAPE01 für diesen Speicherpool mit READWRITE-Zugriff definieren.

```
define volume pool1 tape01 access=readwrite
```

## Beispiel: Einen Datenträger für einen Dateispeicherpool definieren

Der Speicherpool FILEPOOL ist einer Einheitenklasse mit dem Einheitentyp FILE zugeordnet. 

 Für diesen Speicherpool einen Datenträger mit dem Namen filepool\_vol01 definieren.

 Für diesen Speicherpool einen Datenträger mit dem Namen fp\_vol01.dsm definieren.

```
define volume filepool /usr/storage/filepool_vol01
```



```
define volume filepool j:\storage\fp_vol01.dsm
```



## Beispiel: Einen Hintergrundprozess verwenden, um 10 Datenträger für einen Dateispeicherpool mit einer maximalen Kapazität von 5 GB zu definieren

10 Datenträger in einem sequenziellen Speicherpool definieren, der eine Einheitenklasse FILE verwendet. Der Speicherpool hat den Namen FILEPOOL. Der Wert des Parameters MAXCAPACITY für die Einheitenklasse, die diesem Speicherpool zugeordnet ist, lautet 5 GB. Die Erstellung muss im Hintergrund erfolgen.

```
define volume filepool filevol numberofvolumes=10 formatsize=5000
```

Der Server erstellt die Datenträgernamen filevol001 bis filevol010.

Datenträger werden in dem Verzeichnis oder in den Verzeichnissen erstellt, das bzw. die mit dem Parameter DIRECTORY der Einheitenklasse angegeben ist bzw. sind, die dem Speicherpool "filepool" zugeordnet ist. Wenn Sie mehrere Verzeichnisse für die Einheitenklasse angegeben haben, können einzelne Datenträger in den Verzeichnissen in der Liste erstellt werden.

## Zugehörige Befehle

Tabelle 7. Zugehörige Befehle für DEFINE VOLUME

| Befehl           | Beschreibung   |
|------------------|--|
| DEFINE STGPOOL   | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern. |
| QUERY VOLUME     | Zeigt Informationen über Speicherpooldatenträger an.                               |
| UPDATE DEVCLASS  | Ändert die Attribute einer Einheitenklasse.  |
| UPDATE LIBVOLUME | Ändert den Status eines Speicherdatenträgers.                                      |
| UPDATE VOLUME    | Aktualisiert die Attribute der Speicherpooldatenträger.                            |

## DELETE-Befehle

Mit den DELETE-Befehlen kann ein IBM Spectrum Protect-Objekt gelöscht oder entfernt werden.

- DELETE ASSOCIATION (Knotenzuordnung zu einem Zeitplan löschen)
- DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)
- DELETE BACKUPSET (Sicherungsgruppe löschen)
- DELETE CLIENTOPT (Option in einer Optionsgruppe löschen)
- DELETE CLOPTSET (Clientoptionsgruppe löschen)
- DELETE COLLOGROUP (Kollokationsgruppe löschen)
- DELETE COLLOCMEMBER (Kollokationsgruppenmitglied löschen)
- DELETE COPYGROUP (Sicherungs- oder Archivierungskopiengruppe löschen)
- DELETE DATAMOVER (Einheit zum Versetzen von Daten löschen)
- DELETE DEDUPSTATS (Dateneduplizierungsstatistikdaten löschen)
- DELETE DEVCLASS (Einheitenklasse löschen)
- DELETE DOMAIN (Maßnahmendomäne löschen)
- DELETE DRIVE (Laufwerk aus einem Kassettenarchiv löschen)
- DELETE EVENT (Ereignissätze löschen)
- DELETE EVENTSERVER (Definition des Ereignisservers löschen)
- DELETE FILESPACE (Clientknotendaten aus dem Server löschen)
- DELETE GRPMEMBER (Server aus einer Servergruppe löschen)
- DELETE LIBRARY (Kassettenarchiv löschen)
- DELETE MACHINE (Maschineninformationen löschen)
- DELETE MACHNODEASSOCIATION (Zuordnung zwischen Maschine und Knoten löschen)
- DELETE MGMTCLASS (Verwaltungsklasse löschen)
- DELETE NODEGROUP (Knotengruppe löschen)
- DELETE NODEGROUPMEMBER (Eintrag aus der Knotengruppe löschen)
- DELETE PATH (Pfad löschen)
- DELETE POLICYSET (Maßnahmengruppe löschen)
- DELETE PROFASSOCIATION (Profilzuordnung löschen)
- DELETE PROFILE (Profil löschen)
- DELETE RECMEDMACHASSOCIATION (Zuordnung Datenträger/Maschine löschen)
- DELETE RECOVERYMEDIA (Wiederherstellungsdatenträger löschen)
- DELETE SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl löschen)
- DELETE SCRIPT (Befehlszeilen aus Prozedur oder gesamte Prozedur löschen)

- DELETE SERVER (Server-Definition löschen)
- DELETE SERVERGROUP (Servergruppe löschen)
- DELETE SPACETRIGGER (Speicherbereichsauslöser für Speicherpool löschen)
- DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)
- DELETE STGRULE (Speicherregeln für Speicherpools löschen)
- DELETE STGPOOL (Speicherpool löschen)
- DELETE STGPOOLDIRECTORY (Speicherpoolverzeichnis löschen)
- DELETE SUBSCRIBER (Subskriptionen aus Konfigurationsmanagerdatenbank löschen)
- DELETE SUBSCRIPTION (Profilsubskription löschen)
- DELETE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs löschen)
- DELETE VOLHISTORY (Protokolldaten sequenzieller Datenträger löschen)
- DELETE VOLUME (Speicherpoolatenträger löschen)

## DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)

Verwenden Sie diesen Befehl, um eine Nachricht aus der Liste der Alertauslöser zu entfernen.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```

      .-.-.-.-.-.
      v          |
>>-DELeTe ALERTTrigger-+--+Nachrichtennummer-+-----><
  
```

### Parameter

Nachrichtennummer (Erforderlich)

Gibt die Nachrichtennummer an, die aus der Liste der Alertauslöser entfernt werden soll. Geben Sie mehrere Nachrichtennummern durch Kommas getrennt und ohne Leerzeichen an. Nachrichtennummern haben eine maximale Länge von acht Zeichen. Platzhalterzeichen können verwendet werden, um Nachrichtennummern anzugeben.

### Alertauslöser löschen

Mit dem folgenden Befehl zwei Nachrichtennummern löschen, die als Alerts angegeben sind:

```
delete alerttrigger ANR1067E,ANR1073E
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE ALERTTRIGGER

| Befehl   | Beschreibung   |
|--|--|
| DEFINE ALERTTRIGGER (Alertauslöser definieren)   | Ordnet angegebene Nachrichten einem Alertauslöser zu.  |
| QUERY ALERTSTATUS (Status eines Alert abfragen)  | Zeigt Informationen zu Alerts an, die auf dem Server ausgegeben wurden.                          |
| QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)  | Zeigt Nachrichtennummern an, die einen Alert auslösen.   |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen) | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an. |
| UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)  | Aktualisiert die Attribute eines oder mehrerer Alertauslöser.                                    |
| UPDATE ALERTSTATUS (Status eines Alert aktualisieren)  | Aktualisiert den Status eines zurückgemeldeten Alert.  |

## DELETE ASSOCIATION (Knotenzuordnung zu einem Zeitplan löschen)

Mit diesem Befehl kann die Zuordnung eines Clientknotens zu einem Clientzeitplan gelöscht werden. IBM Spectrum Protect führt den Zeitplan nicht mehr auf dem Clientknoten aus.

Wird versucht, eine Zuordnung zwischen einem Client und einem Zeitplan aufzuheben, zwischen denen keine Zuordnung besteht, bleibt dieser Befehl für diesen Client ohne Wirkung.

## Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Systemberechtigung
- Uneingeschränkte Maßnahmenberechtigung
- Eingeschränkte Maßnahmenberechtigung für die Domäne, zu der der Zeitplan gehört

## Syntax

```
>>-DELEte ASSOCIation--Domänenname--Zeitplanname----->>  
      .-,-----.  
      V          |  
>---Knotenname+-----><
```

## Parameter

Domänenname (Erforderlich)

Gibt den Namen der Maßnahmendomäne an, zu der der Zeitplan gehört.

Zeitplanname (Erforderlich)

Gibt den Namen des Zeitplans an, dessen Zuordnung zu Clients aufgehoben werden soll.

Knotenname (Erforderlich)

Gibt den Namen des Client-Knotens an, der nicht mehr dem Client-Zeitplan zugeordnet ist. Es kann eine Liste der Clients angegeben werden, deren Zuordnung zu dem angegebenen Zeitplan aufgehoben werden soll. Trennen Sie die Einträge in der Liste durch Kommas ohne Leerzeichen voneinander. Es kann auch ein Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Die Zuordnung aller übereinstimmenden Clients zu dem angegebenen Zeitplan wird aufgehoben.

## Beispiel: Zuordnung eines Knotens zu einem Zeitplan löschen

Den folgenden Befehl ausgeben, um die Zuordnung des Knotens JEFF, der der Maßnahmendomäne DOMAIN1 zugeordnet ist, zu dem Zeitplan WEEKLY\_BACKUP zu löschen:

```
delete association domain1 weekly_backup jeff
```

## Beispiel: Zuordnung eines Knotens zu einem Zeitplan unter Verwendung eines Platzhalterzeichens für die Knotenauswahl löschen

Die Zuordnung ausgewählter Clients, die der Maßnahmendomäne DOMAIN1 zugeordnet sind, zu dem Zeitplan WEEKLY\_BACKUP löschen, so dass dieser Zeitplan nicht mehr von diesen Clients ausgeführt wird. Die Namen der Knoten, deren Zuordnung zu dem Zeitplan aufgehoben werden soll, enthalten die Buchstaben ABC oder XYZ. Den folgenden Befehl ausgeben:

```
delete association domain1 weekly_backup *abc*,*xyz*
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE ASSOCIATION

| Befehl             | Beschreibung  |
|--------------------|---|
| DEFINE ASSOCIATION | Ordnet Clients einem Zeitplan zu.   |
| QUERY ASSOCIATION  | Zeigt die Clients an, die einem oder mehreren Zeitplänen zugeordnet sind. |

## DELETE BACKUPSET (Sicherungsgruppe löschen)

Mit diesem Befehl können Sie eine Sicherungsgruppe manuell löschen, bevor ihr Aufbewahrungszeitraum abläuft.

Wenn der Server eine Sicherungsgruppe erstellt, bestimmt der der Sicherungsgruppe zugeordnete Aufbewahrungszeitraum, wie lange die Sicherungsgruppe in der Datenbank verbleibt. Wird dieses Datum erreicht, löscht der Server automatisch die Sicherungsgruppe,

wenn die Verfallsverarbeitung ausgeführt wird. Der Benutzer kann jedoch die Sicherungsgruppe des Clients auch manuell vom Server löschen, bevor die Sicherungsgruppe verfällt, indem der Befehl DELETE BACKUPSET verwendet wird.

Achtung: Enthalten die Datenträger mehrere Sicherungsgruppen, kehren Sie erst dann in den Status 'Scratch' zurück, wenn alle Sicherungsgruppen verfallen oder gelöscht sind.

## Berechtigungsklasse

Wird die Serveroption REQSYSAUTHOUTFILE auf YES (Standardwert) gesetzt, muss der Administrator die Systemberechtigung haben. Ist die Serveroption REQSYSAUTHOUTFILE auf NO gesetzt, muss der Administrator über Systemberechtigung oder Maßnahmenberechtigung für die Domäne verfügen, der der Clientknoten zugeordnet ist.

## Syntax

```

      .-,-----
      v,-----|
>>-DELeTe BACKUPSET---+--Knotenname-----+-----+----->
      '-Knotengruppenname-'

      .-,-----
      v,-----|
>---Sicherungsgruppenname+-----+-----+----->
      '-BEGINDate-----Datum-'

>+-----+-----+-----+-----+----->
  '-BEGINTime-----Zeit-'  '-ENDDate-----Datum-'

      .-WHERE DATAType-----ALL-----
>+-----+-----+-----+-----+----->
  '-ENDTime-----Zeit-'  |
                          |      .-,-----
                          |      v,-----| |
                          |      '-WHERE DATAType-----+FILE--+--+-'
                          |      '-IMAGE-'

>+-----+-----+-----+-----+----->
  '-WHERE RETention-----+Tage-----+-'
                          '-NOLimit-'

>+-----+-----+-----+-----+----->
  '-WHERE DESCRIPTION-----Beschreibung-'

      .-Preview-----No-----
>+-----+-----+-----+-----+----->
  '-Preview-----+No--+-'
                          '-Yes-'

```

## Parameter

**Knotenname oder Knotengruppenname (Erforderlich)**

Gibt den Namen der Clientknoten oder Knotengruppen an, deren Daten in den angegebenen Sicherungsgruppendatenträgern enthalten sind. Sollen mehrere Knoten- und Knotengruppenamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Alle angegebenen Knotennamen können Platzhalterzeichen enthalten, aber Knotengruppenamen dürfen keine Platzhalterzeichen enthalten. Wenn Sicherungsgruppendatenträger Sicherungsgruppen von mehreren Knoten enthalten, wird jede Sicherungsgruppe, deren Knotenname mit einem der angegebenen Knotennamen übereinstimmt, gelöscht.

**Sicherungsgruppenname (Erforderlich)**

Gibt den Namen der Sicherungsgruppe an, die gelöscht werden soll. Der angegebene Sicherungsgruppenname kann Platzhalterzeichen enthalten. Es können mehrere Sicherungsgruppenamen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden.

**BEGINDate**

Gibt das Anfangsdatum an, an dem die zu löschende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter BEGINTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird ein Anfangsdatum ohne eine Anfangszeit angegeben, lautet die Zeit 24:00 (Mitternacht) an dem angegebenen Datum. Sie können das Datum mit einem der folgenden Werte angeben:

| Wert       | Beschreibung         | Beispiel   |
|------------|----------------------|------------|
| MM/TT/JJJJ | Ein bestimmtes Datum | 09/15/1999 |
| TODAY      | Das aktuelle Datum   | TODAY      |

| Wert                           | Beschreibung  | Beispiel   |
|--------------------------------|---|--|
| TODAY+Tage <i>oder</i> +Tage   | Das aktuelle Datum plus der Anzahl der angegebenen Tage.  | TODAY +3 <i>oder</i> +3.   |
| TODAY-Tage <i>oder</i> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. | TODAY -3 <i>oder</i> -3.   |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.                             | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.       | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.                       | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.  | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

#### BEGINTime

Gibt die Anfangszeit an, zu der die zu löschende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Dieser Parameter kann zusammen mit dem Parameter BEGINDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird eine Anfangszeit ohne ein Anfangsdatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Uhrzeit. Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert                         | Beschreibung   | Beispiel                      |
|------------------------------|--|-------------------------------|
| HH:MM:SS                     | Eine bestimmte Uhrzeit   | 10:30:08                      |
| NOW                          | Die aktuelle Uhrzeit   | NOW                           |
| NOW+HH:MM <i>oder</i> +HH:MM | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten  | NOW+02:00 <i>oder</i> +02:00. |
| NOW-HH:MM <i>oder</i> -HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten | NOW-02:00 <i>oder</i> -02:00. |

#### ENDDate

Gibt das Enddatum an, an dem die zu löschende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Dieser Parameter kann zusammen mit dem Parameter ENDTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird ein Enddatum ohne eine Endzeit angegeben, lautet die Zeit 23:59:59 am angegebenen Enddatum. Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                           | Beschreibung  | Beispiel   |
|--------------------------------|---|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum                                      | 09/15/1999   |
| TODAY                          | Das aktuelle Datum  | TODAY  |
| TODAY+Tage <i>oder</i> +Tage   | Das aktuelle Datum plus der Anzahl der angegebenen Tage.  | TODAY +3 <i>oder</i> +3.   |
| TODAY-Tage <i>oder</i> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. | TODAY -3 <i>oder</i> -3.   |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.                             | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.       | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.                       | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.  | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

#### ENDTime

Gibt die Endzeit des Bereichs an, in dem die zu löschende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Dieser Parameter kann zusammen mit dem Parameter ENDDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird eine Endzeit ohne ein Enddatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Zeit. Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert                            | Beschreibung   | Beispiel                      |
|---------------------------------|--|-------------------------------|
| HH:MM:SS                        | Eine bestimmte Uhrzeit   | 10:30:08                      |
| NOW                             | Die aktuelle Uhrzeit   | NOW                           |
| NOW+HH:MM <i>oder</i><br>+HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum  | NOW+02:00 <i>oder</i> +02:00. |
| NOW-HH:MM <i>oder</i> -HH:MM    | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum | NOW-02:00 <i>oder</i> -02:00. |

#### WHEREDATAType

Gibt an, dass die Sicherungsgruppen mit den angegebenen Typen von Daten gelöscht werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert gibt an, dass Sicherungsgruppen für alle Typen von Daten (Dateiebene, Image und Anwendung) gelöscht werden sollen. Bei der Angabe mehrerer Datentypen müssen die Datentypen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Gültige Werte:

#### ALL

Gibt an, dass Sicherungsgruppen für alle Typen von Daten (Dateiebene, Image und Anwendung) gelöscht werden sollen. Dies ist der Standardwert.

#### FILE

Gibt an, dass eine Sicherungsgruppe auf Dateiebene gelöscht werden soll. Sicherungsgruppen auf Dateiebene enthalten Dateien und Verzeichnisse, die vom Client für Sichern/Archivieren gesichert wurden.

#### IMAGE

Gibt an, dass eine Imagesicherungsgruppe gelöscht werden soll. Imagesicherungsgruppen enthalten Images, die mit dem Befehl BACKUP IMAGE des Clients für Sichern/Archivieren erstellt wurden.

#### WHERERETention

Gibt den Aufbewahrungszeitraum in Tagen an, der der zu löschenden Sicherungsgruppe zugeordnet ist. Sie können eine ganze Zahl von 0 bis 30000 angeben. Gültige Werte:

#### Tage

Gibt an, dass Sicherungsgruppen, die diese Anzahl Tage aufbewahrt werden, gelöscht werden.

#### NOLimit

Gibt an, dass die Sicherungsgruppen, die unbegrenzt aufbewahrt werden, gelöscht werden.

#### WHEREDEScRiption

Gibt die Beschreibung an, die der zu löschenden Sicherungsgruppe zugeordnet ist. Die angegebene Beschreibung kann ein Platzhalterzeichen enthalten. Dieser Parameter ist wahlfrei. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

#### Preview

Gibt an, ob die Liste der zu löschenden Sicherungsgruppen vorab angezeigt werden soll, ohne die Sicherungsgruppen tatsächlich zu löschen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

#### No

Gibt an, dass die Sicherungsgruppen gelöscht werden.

#### Yes

Gibt an, dass der Server die Liste der zu löschenden Sicherungsgruppen anzeigt, ohne die Sicherungsgruppen tatsächlich zu löschen.

## Beispiel: Eine Sicherungsgruppe löschen

Die Sicherungsgruppe PERS\_DATA.3099 löschen, die zum Clientknoten JANE gehört. Die Sicherungsgruppe wurde am 11/19/1998 um 10:30:05 generiert und die Beschreibung lautet "Documentation Shop".

```
delete backupset pers_data.3099
begindate=11/19/1998 begintime=10:30:05wheredescription="documentation shop"
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE BACKUPSET

| Befehl           | Beschreibung   |
|------------------|--|
| DEFINE BACKUPSET | Definiert eine zuvor generierte Sicherungsgruppe für einen Server. |

| Befehl                  | Beschreibung  |
|-------------------------|---|
| DEFINE NODEGROUP        | Definiert eine Gruppe von Knoten.   |
| DEFINE NODEGROUPMEMBER  | Fügt einer Knotengruppe einen Clientknoten hinzu.                           |
| DELETE NODEGROUP        | Löscht eine Knotengruppe.   |
| DELETE NODEGROUPMEMBER  | Löscht einen Clientknoten aus einer Knotengruppe.                           |
| GENERATE BACKUPSET      | Generiert eine Sicherungsgruppe mit den Daten eines Clients.                |
| GENERATE BACKUPSETTOC   | Generiert ein Inhaltsverzeichnis für eine Sicherungsgruppe.                 |
| QUERY BACKUPSET         | Zeigt Sicherungsgruppen an.   |
| QUERY NODEGROUP         | Zeigt Informationen zu Knotengruppen an.                                    |
| QUERY BACKUPSETCONTENTS | Zeigt den Inhalt in Sicherungsgruppen an.                                   |
| UPDATE BACKUPSET        | Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum. |
| UPDATE NODEGROUP        | Aktualisiert die Beschreibung einer Knotengruppe.                           |

## DELETE CLIENTOPT (Option in einer Optionsgruppe löschen)

Mit diesem Befehl kann eine Clientoption in einer Optionsgruppe gelöscht werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung erforderlich.

### Syntax

```
>>-DELeTe CLIENTOpt--Optionsgruppenname--Optionsname----->
>--+-----+-----><
  '-SEQnumber--==--+-Nummer-+-'
      '-ALL-----'
```

### Parameter

Optionsgruppenname (Erforderlich)

Gibt den Namen der Client-Optionsgruppe an.

Optionsname (Erforderlich)

Gibt eine gültige Client-Option an.

SEQnumber

Gibt eine Folgenummer an, wenn ein Optionsname mehrmals angegeben wird. Dieser Parameter ist wahlfrei. Gültige Werte sind:

n

Gibt eine ganze Zahl größer oder gleich 0 an.

ALL

Gibt alle Folgenummern an.

### Beispiel: Die Option für das Datumsformat löschen

Die Option für das Datumsformat in der Optionsgruppe *ENG* löschen.

```
delete clientopt eng dateformat
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE CLIENTOPT

| Befehl        | Beschreibung                      |
|---------------|-----------------------------------|
| COPY CLOPTSET | Kopiert eine Clientoptionsgruppe. |

| Befehl           | Beschreibung  |
|------------------|---|
| DEFINE CLIENTOPT | Fügt einer Clientoptionsgruppe eine Clientoption hinzu.                       |
| DEFINE CLOPTSET  | Definiert eine Clientoptionsgruppe.   |
| DELETE CLOPTSET  | Löscht eine Clientoptionsgruppe.  |
| QUERY CLOPTSET   | Zeigt Informationen über eine Clientoptionsgruppe an.                         |
| UPDATE CLIENTOPT | Aktualisiert die Folgenummer einer Clientoption in einer Clientoptionsgruppe. |
| UPDATE CLOPTSET  | Aktualisiert die Beschreibung einer Clientoptionsgruppe.                      |

## DELETE CLOPTSET (Clientoptionsgruppe löschen)

Mit diesem Befehl kann eine Clientoptionsgruppe gelöscht werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung erforderlich.

### Syntax

```
>>-DELeTe CLOptset--Optionsgruppenname-----<<
```

### Parameter

Optionsgruppenname (Erforderlich)  
Gibt den Namen der zu löschenden Clientoptionsgruppe an.

### Beispiel: Eine Clientoptionsgruppe löschen

Löschen Sie die Clientoptionsgruppe mit dem Namen ENG.

```
delete cloptset eng
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE CLOPTSET

| Befehl           | Beschreibung  |
|------------------|---|
| COPY CLOPTSET    | Kopiert eine Clientoptionsgruppe.   |
| DEFINE CLIENTOPT | Fügt einer Clientoptionsgruppe eine Clientoption hinzu.                       |
| DEFINE CLOPTSET  | Definiert eine Clientoptionsgruppe.   |
| DELETE CLIENTOPT | Löscht eine Clientoption aus einer Clientoptionsgruppe.                       |
| QUERY CLOPTSET   | Zeigt Informationen über eine Clientoptionsgruppe an.                         |
| UPDATE CLIENTOPT | Aktualisiert die Folgenummer einer Clientoption in einer Clientoptionsgruppe. |
| UPDATE CLOPTSET  | Aktualisiert die Beschreibung einer Clientoptionsgruppe.                      |

## DELETE COLLOGROUP (Kollokationsgruppe löschen)

Verwenden Sie diesen Befehl, um eine Kollokationsgruppe zu löschen. Eine Kollokationsgruppe kann nicht gelöscht werden, wenn sie Mitglieder enthält.

Sie können alle Mitglieder in der Kollokationsgruppe entfernen, indem Sie den Befehl DELETE COLLOCMEMBER mit einem Platzhalterzeichen im Parameter Knotenname ausgeben.



## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-DELEte COLLOCGroup--Gruppenname-----<<
```

## Parameter

Gruppenname  
Gibt den Namen der Kollokationsgruppe an, die gelöscht werden soll.

## Beispiel: Eine Kollokationsgruppe löschen

Die Kollokationsgruppe group1 löschen.

```
delete collogroup group1
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE COLLOGROUP

| Befehl              | Beschreibung  |
|---------------------|---|
| DEFINE COLLOGROUP   | Definiert eine Kollokationsgruppe.  |
| DEFINE COLLOCMEMBER | Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.                                     |
| DEFINE STGPOOL      | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.                            |
| DELETE COLLOCMEMBER | Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.                                     |
| MOVE NODEDATA       | Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen. |
| QUERY COLLOGROUP    | Zeigt Informationen zu Kollokationsgruppen an.  |
| QUERY NODE          | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.                             |
| QUERY NODEDATA      | Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.                               |
| QUERY STGPOOL       | Zeigt Informationen zu Speicherpools an.  |
| REMOVE NODE         | Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.              |
| UPDATE COLLOGROUP   | Aktualisiert die Beschreibung einer Kollokationsgruppe.   |
| UPDATE STGPOOL      | Ändert die Attribute eines Speicherpools.   |

## DELETE COLLOCMEMBER (Kollokationsgruppenmitglied löschen)

Verwenden Sie diesen Befehl, um einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe zu löschen.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
Knoten aus einer Kollokationsgruppe löschen
```

```

      .-,------.
      v          |
>>-DELEte COLLOCMember--Gruppenname----Knotenname-+-----><

```

## Parameter

### Gruppenname

Gibt den Namen der Kollokationsgruppe an, aus der ein Clientknoten gelöscht werden soll.

### Knotenname

Gibt den Namen des Clientknotens an, der aus der Kollokationsgruppe gelöscht werden soll. Sie können einen oder mehrere Namen angeben. Werden mehrere Namen angegeben, sind die Namen durch Kommas voneinander zu trennen; verwenden Sie zwischen den Namen keine Leerzeichen. Sie können auch Platzhalterzeichen verwenden, um mehrere Knoten anzugeben.

Dateibereich aus einer Dateibereichskollokationsgruppe löschen

```
>>-DELEte COLLOCMember--Gruppenname--Knotenname----->
```

```

      .-,------.
      v          |
>>-FILEspace-----Dateibereichsname-+----->

.-NAMeType-----SERVER-----
>+-----+-----+-----+----->
'-NAMeType-----+--SERVER--+-'
      +-UNICode-+
      '-FSID-----'

.-CODEType-----BOTH-----
>+-----+-----+-----+-----><
'-CODEType-----+--BOTH-----+-'
      +-UNICode-----+
      '-NONUNICode-'

```

## Parameter

### Gruppenname

Gibt den Namen der Kollokationsgruppe an, aus der ein Dateibereich gelöscht werden soll.

### Knotenname

Gibt den Clientknoten an, auf dem sich der Dateibereich befindet.

### Filespace

Gibt den *Dateibereichsnamen* auf dem Clientknoten an, der aus der Kollokationsgruppe gelöscht werden soll. Sie können einen oder mehrere Dateibereichsnamen angeben, die sich auf einem bestimmten Clientknoten befinden. Werden mehrere Dateibereichsnamen angegeben, sind die Namen durch Kommas voneinander zu trennen; verwenden Sie zwischen den Namen keine Leerzeichen. Sie können auch Platzhalterzeichen verwenden, wenn mehrere Dateibereichsnamen angegeben werden.

### NAMeType

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unicode-Unterstützung verfügt. Ein Client für Sichern/Archivieren mit Unicode-Unterstützung ist nur für Windows, Macintosh OS 9, Macintosh OS X und NetWare verfügbar. Verwenden Sie diesen Parameter, wenn Sie einen Dateibereichsnamen angeben, der kein einzelnes Platzhalterzeichen ist. Sie können einen vollständig qualifizierten Dateibereichsnamen angeben, der kein Platzhalterzeichen enthält. Sie können auch einen teilweise qualifizierten Dateibereichsnamen angeben, der ein Platzhalterzeichen enthalten kann, aber andere Zeichen enthalten muss. Der Standardwert lautet SERVER. Gültige Werte:

#### SERVER

Der Server verwendet die Zeichenumsetzungstabelle des Servers, um die Dateibereichsnamen zu interpretieren.

#### UNICode

Der Server konvertiert die Dateibereichsnamen aus der Server-Codepage in die Codepage UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in den Namen und der Server-Codepage ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Server-Codepage nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

#### FSID

Der Server interpretiert die Dateibereichsnamen nach ihren Dateibereichs-IDs (FSIDs).

### CODEType

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen verwenden. Der Standardwert lautet BOTH, d. h., die Dateibereiche werden unabhängig vom Codepagetyp eingeschlossen. Die folgenden Werte sind verfügbar:

- BOTH**  
Die Dateibereiche unabhängig vom Codepagetyp einschließen.
- UNICODE**  
Nur Dateibereiche einschließen, die in Unicode sind.
- NONUNICODE**  
Dateibereiche einschließen, die nicht in Unicode sind.

## Kollokationsgruppenmitglieder löschen

Die beiden Knoten NODE1 und NODE2 aus der Kollokationsgruppe GROUP1 löschen.

```
delete collocmember group1 node1,node2
```

## Dateibereich aus einer Dateibereichskollokationsgruppe löschen

Den folgenden Befehl ausgeben, um den Dateibereich *cap\_27400* aus der Kollokationsgruppe *collgrp\_2* auf dem Knoten *hp\_4483* zu löschen:

```
delete collocmember collgrp_2 hp_4483 filespace=cap_27400
```

## Ein Mitglied einer Dateibereichskollokationsgruppe auf einem Knoten löschen, der Unicode verwendet

Befindet sich der Dateibereich auf einem Knoten, der Unicode verwendet, können Sie dies im Befehl angeben. Geben Sie den folgenden Befehl aus, um den Dateibereich *cap\_257* aus der Kollokationsgruppe *collgrp\_3* auf dem Knoten *win\_4687* zu löschen:

```
delete collocmember collgrp_3 win_4687 filespace=cap_257 codetype=unicode
```

## Dateibereich mit einem Namensteil löschen

Wenn der Dateibereich einen Namensteil hat, können Sie ein Platzhalterzeichen verwenden, um den Dateibereich zu löschen. Geben Sie den folgenden Befehl aus, um den Dateibereich *cap\_\** aus der Kollokationsgruppe *collgrp\_4* auf dem Knoten *win\_4687* zu löschen:

```
delete collocmember collgrp_4 win_4687 filespace=cap_* codetype=unicode
```

Sind mehrere Dateibereiche vorhanden, deren Namen mit *cap\_\** beginnen, werden diese Dateibereiche ebenfalls gelöscht.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE COLLOCMEMBER

| Befehl              | Beschreibung   |
|---------------------|--|
| DEFINE COLLOGGROUP  | Definiert eine Kollokationsgruppe.   |
| DEFINE COLLOCMEMBER | Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.  |
| DEFINE STGPOOL      | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.   |
| DELETE COLLOGGROUP  | Löscht eine Kollokationsgruppe.  |
| DELETE FILESPACE    | Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt. |
| MOVE NODEDATA       | Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen.  |
| QUERY COLLOGGROUP   | Zeigt Informationen zu Kollokationsgruppen an.   |
| QUERY NODE          | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.  |



## Beispiel: Eine Archivierungskopiengruppe löschen

Die Archivierungskopiengruppe aus der Verwaltungsklasse MCLASS1 löschen, die sich in der Maßnahmengruppe SUMMER der Maßnahmendomäne PROG1 befindet.

```
delete copygroup prog1 summer mclass1 type=archive
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE COPYGROUP

| Befehl           | Beschreibung  |
|------------------|---|
| DEFINE COPYGROUP | Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse. |
| QUERY COPYGROUP  | Zeigt die Attribute einer Kopiengruppe an.  |
| UPDATE COPYGROUP | Ändert ein oder mehrere Attribute einer Kopiengruppe.   |

## DELETE DATAMOVER (Einheit zum Versetzen von Daten löschen)

Verwenden Sie diesen Befehl, um eine Einheit zum Versetzen von Daten zu löschen. Sie können die Einheit zum Versetzen von Daten nicht löschen, wenn für diese Einheit zum Versetzen von Daten Pfade definiert sind.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-DElete DATAMover--Name_der_Einheit_zum_Versetzen_von_Daten--<<
```

## Parameter

Name\_der\_Einheit\_zum\_Versetzen\_von\_Daten (Erforderlich)

Gibt den Namen der Einheit zum Versetzen von Daten an.

Anmerkung: Mit diesem Befehl wird die Einheit zum Versetzen von Daten auch dann gelöscht, wenn für den entsprechenden NAS-Knoten Daten vorhanden sind.

## Beispiel: Eine Einheit zum Versetzen von Daten löschen




Die Einheit zum Versetzen von Daten für den Knoten NAS1 löschen.

```
delete datamover nas1
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE DATAMOVER

| Befehl           | Beschreibung  |
|------------------|---|
| DEFINE DATAMOVER | Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server. |
| DEFINE PATH      | Definiert einen Pfad von einer Quelle zu einem Ziel.                                |
| DELETE PATH      | Löscht einen Pfad von einer Quelle zu einem Ziel.                                   |
| QUERY DATAMOVER  | Zeigt Definitionen der Einheit zum Versetzen von Daten an.                          |
| QUERY PATH       | Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.                     |
| UPDATE DATAMOVER | Ändert die Definition einer Einheit zum Versetzen von Daten.                        |

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

# DELETE DEDUPSTATS (Dateneduplizierungsstatistikdaten löschen)

Verwenden Sie diesen Befehl, um Dateneduplizierungsstatistikdaten für einen Verzeichniscontainerspeicherpool oder einen Cloudspeicherpool zu löschen. Die neuesten Dateneduplizierungsstatistikdaten für einen Clientknoten und einen Dateibereich können nicht gelöscht werden.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool erforderlich.

## Syntax

```
>>-DELEte DEDUPStats--Poolname--+-+-----+----->
                                     '-Knotenname-'

. -*----- . -CODEType---BOTH-----
>+-----+-----+-----+----->
| .-,----- . | '-CODEType---+UNICODE---+'
| V | | | +-NONUNICODE+
+---Dateibereichsname---+ | '-BOTH-----'
| .-,----- . |
| V | |
'-----FSID-----'

. -NAMEType---SERVER-----
>+-----+-----+-----+----->
'-NAMEType---+SERVER---+' '-TODate-----Datum-'
          +-UNICODE+
          '-FSID-----'

>+-----+-----+-----+-----<
'-TOTime-----Zeit-'
```

## Parameter

### Poolname (Erforderlich)

Gibt den Namen des Verzeichniscontainerspeicherpools an, der in den Dateneduplizierungsstatistikdaten aufgelistet wird. Für den Speicherpoolnamen können bis zu 30 Zeichen angegeben werden. Wenn Sie mehr als 30 Zeichen angeben, schlägt der Befehl fehl.

Einschränkung: Sie können nur Verzeichniscontainerspeicherpools oder Cloudspeicherpools angeben.

### Knotenname

Gibt den Namen des Clientknotens an, der in den Dateneduplizierungsstatistikdaten aufgelistet wird. Dieser Parameter ist wahlfrei. Wird für diesen Parameter kein Wert angegeben, werden alle Knoten angezeigt. Für den Knotennamen können bis zu 64 Zeichen angegeben werden. Wenn Sie mehr als 64 Zeichen angeben, schlägt der Befehl fehl.

### Dateibereichsname oder FSID

Gibt den Namen oder die Dateibereichs-ID (FSID) eines oder mehrerer Dateibereiche an, die in den Dateneduplizierungsstatistikdaten aufgelistet werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Der Standardwert ist ein Stern. Geben Sie einen der folgenden Werte an:

\*

Geben Sie einen Stern (\*) an, um alle Dateibereiche oder IDs anzuzeigen.

### Dateibereichsname

Gibt den Namen des Dateibereichs an. Geben Sie mehrere Dateibereiche an, indem Sie die Namen durch Kommas ohne Zwischenleerschritte voneinander trennen. FSID gibt die Dateibereichs-ID an. Dieser Parameter ist für Clients mit Dateibereichen in Unicode-Format gültig. Geben Sie mehrere Dateibereiche an, indem Sie die Namen durch Kommas ohne Zwischenleerschritte voneinander trennen.

Für Clients mit Dateibereichen in Unicode-Format können Sie entweder einen Dateibereichsnamen oder eine Dateibereichs-ID (FSID) eingeben. Wenn Sie einen Dateibereichsnamen eingeben, muss der Server möglicherweise den eingegebenen Dateibereichsnamen konvertieren. Beispielsweise muss der Server gegebenenfalls den Namen, den Sie eingeben, aus der Codepage des Servers in Unicode konvertieren.

Einschränkungen: Die folgenden Einschränkungen gelten für Dateibereichsnamen und Dateibereichs-IDs (FSID):

- Ein Knotenname muss angegeben werden, wenn ein Dateibereichsname angegeben wird.

- In demselben Befehl dürfen nicht gleichzeitig Dateibereichsnamen und Dateibereichs-IDs (FSIDs) angegeben werden.

#### CODEType

Gibt an, welcher Typ von Dateibereichen in den Bericht eingeschlossen werden soll. Der Standardwert lautet BOTH. Dieser Standardwert gibt an, dass Dateibereiche unabhängig vom Typ der Codepage eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie einen Stern zum Anzeigen von Informationen zu allen Dateibereichen eingeben. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

##### UNICODE

Dateibereiche einschließen, die ein Unicode-Format haben.

##### NONUNICODE

Dateibereiche einschließen, die kein Unicode-Format haben.

##### BOTH

Dateibereiche unabhängig von der Art der Zeichenumsetzungstabelle einschließen. Dies ist der Standardwert.

#### NAMETYPE

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Verwenden Sie diesen Parameter, wenn IBM Spectrum Protect-Clients über Dateibereiche in Unicode-Format verfügen und die Clients unter dem Betriebssystem Windows, NetWare oder Macintosh OS X ausgeführt werden. Dieser Parameter ist wahlfrei.

Dieser Parameter ist erforderlich, wenn Sie einen Knotennamen und einen Dateibereichsnamen bzw. eine Dateibereichs-ID (FSID) angeben.

Einschränkung: Wenn Sie diesen Parameter angeben, darf der Dateibereichsname keinen Stern enthalten.

Geben Sie einen der folgenden Werte an:

##### SERVER

Der Server verwendet die Zeichenumsetzungstabelle des Servers, um die Dateibereichsnamen zu interpretieren. Dies ist der Standardwert.

##### UNICODE

Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetzungstabelle in die Zeichenumsetzungstabelle UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetzungstabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetzungstabelle nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

##### FSID

Der Server interpretiert die Dateibereichsnamen als ihre Dateibereichs-IDs (FSIDs).

#### TODATE

Gibt das späteste Datum für die zu löschenden Statistikdaten an. IBM Spectrum Protect löscht nur die Statistikdaten mit einem Datum bis zu dem angegebenen Datum (einschließlich). Dieser Parameter ist wahlfrei.

Geben Sie einen der folgenden Werte an:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum.  | 10/15/2015<br><br>Wenn Sie ein Datum angeben, werden alle Kandidatensätze, die an diesem Tag (bis 23:59:59 Uhr) geschrieben wurden, ausgewertet.   |
| TODAY                          | Das aktuelle Datum.  | TODAY  |
| TODAY-Tage oder -Tage          | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY-1 oder -1.<br><br>Sollen Informationen angezeigt werden, die bis gestern erstellt wurden, können Sie TODATE=TODAY-1 oder TODATE= -1 angeben. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br><br>Um Sätze einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.   |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |

| Wert      | Beschreibung   | Beispiel  |
|-----------|--|---|
| BOTM+Tage | Der erste Tag des aktuellen Monats plus angegebene Tage. | BOTM+9<br><br>Um Sätze einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren. |

TOTIME

Gibt an, dass Dateneduplizierungsstatistikdaten gelöscht werden sollen, die zu oder vor dieser Zeit am angegebenen Datum erstellt wurden. Dieser Parameter ist wahlfrei. Der Standardwert ist das Ende des Tages (23:59:59). Geben Sie einen der folgenden Werte an:

| Wert                  | Beschreibung   | Beispiel  |
|-----------------------|--|---|
| HH:MM:SS              | Eine bestimmte Uhrzeit am angegebenen Datum.                             | 12:30:22  |
| NOW                   | Die aktuelle Uhrzeit am angegebenen Datum.                               | NOW   |
| NOW+HH:MM oder +HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Datum.  | NOW+03:00 oder +03:00.<br><br>Wenn Sie den Befehl DELETE DEDUPSTATS um 9:00 Uhr mit TOTIME=NOW+03:00 oder TOTIME=+03:00 ausgeben, löscht IBM Spectrum Protect Sätze mit der Uhrzeit 12:00 Uhr oder früher an dem angegebenen Datum. |
| NOW-HH:MM oder -HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Datum. | NOW-03:30 oder -03:30.<br><br>Wenn Sie den Befehl DELETE DEDUPSTATS um 9:00 Uhr mit TOTIME=NOW-3:30 oder TOTIME=-3:30 ausgeben, löscht IBM Spectrum Protect Sätze mit der Uhrzeit 5:30 Uhr oder früher an dem angegebenen Datum.    |




## Beispiel: Dateneduplizierungsstatistikdaten für einen Dateibereich löschen

Dateneduplizierungsstatistikdaten eines Dateibereichs mit dem Namen /srvr löschen, der zum Verzeichniscontainerspeicherpool POOL1 gehört, der auf dem Clientknoten NODE1 gespeichert ist.

```
delete dedupstats pool1 node1 /srvr
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE DEDUPSTATS

| Befehl  | Beschreibung                                 |
|---|--|
| GENERATE DEDUPSTATS   | Generiert Dateneduplizierungsstatistikdaten. |
|  <br> QUERY DEDUPSTATS | Zeigt Dateneduplizierungsstatistikdaten an.  |

## DELETE DEVCLASS (Einheitenklasse löschen)

Mit diesem Befehl kann eine Einheitenklasse gelöscht werden.

Um diesen Befehl verwenden zu können, müssen zunächst alle Speicherpools gelöscht werden, die der Einheitenklasse zugeordnet sind, und, falls erforderlich, alle Datenbankexport- oder -importprozesse abgebrochen werden, die die Einheitenklasse verwenden.

Die bei der Installation vordefinierte Einheitenklasse DISK kann nicht gelöscht werden; es können jedoch alle Einheitenklassen gelöscht werden, die von dem IBM Spectrum Protect-Administrator definiert wurden.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax



```
>>-DElete DEVclass--Einheitenklassenname-----><
```

## Parameter

Einheitenklassenname (Erforderlich)  
Gibt den Namen der Einheitenklasse an, die gelöscht werden soll.


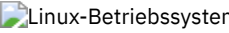

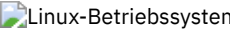




## Beispiel: Eine Einheitenklasse löschen

Die Einheitenklasse mit dem Namen MYTAPE löschen. Der Einheitenklasse sind keine Speicherpools zugeordnet.

```
delete devclass mytape
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE DEVCLASS

| Befehl  | Beschreibung   |
|---|--|
| DEFINE DEVCLASS   | Definiert eine Einheitenklasse.  |
|   DEFINE DEVCLASS (z/OS Media-Server) |   Definiert eine Einheitenklasse für die Verwendung von Speicher, der von einem z/OS Media-Server verwaltet wird. |
| QUERY DEVCLASS  | Zeigt Informationen zu Einheitenklassen an.  |
| QUERY DIRSPACE  | Zeigt Informationen zu Verzeichnissen FILE an.   |
| UPDATE DEVCLASS   | Ändert die Attribute einer Einheitenklasse.  |
|   UPDATE DEVCLASS (z/OS Media-Server) |   Ändert die Attribute einer Einheitenklasse für Speicher, der von einem z/OS Media-Server verwaltet wird.        |

## DELETE DOMAIN (Maßnahmendomäne löschen)

Mit diesem Befehl kann eine Maßnahmendomäne gelöscht werden. Alle zugeordneten Maßnahmengruppen, einschließlich der Maßnahmengruppe ACTIVE, Verwaltungsklassen und Kopiengruppen werden mit der Maßnahmendomäne gelöscht.

Eine Maßnahmendomäne, für die Client-Knoten registriert sind, kann nicht gelöscht werden. Um zu bestimmen, ob Clientknoten für eine Maßnahmendomäne registriert sind, geben Sie den Befehl QUERY DOMAIN oder den Befehl QUERY NODE aus. Versetzen Sie alle Clientknoten in eine andere Maßnahmendomäne oder löschen Sie die Knoten.

Die vordefinierte Maßnahmendomäne STANDARD kann gelöscht werden. Wird der IBM Spectrum Protect-Server jedoch später erneut installiert, schreibt der Prozess alle Maßnahmenobjekte STANDARD zurück.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-DElete Domain--Domänenname-----><
```

## Parameter

Domänenname (Erforderlich)  
Gibt die Maßnahmendomäne an, die gelöscht werden soll.

## Beispiel: Eine Maßnahmendomäne löschen

Die Maßnahmendomäne EMPLOYEE\_RECORDS löschen.

```
delete domain employee_records
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE DOMAIN

| Befehl        | Beschreibung  |
|---------------|---|
| COPY DOMAIN   | Erstellt eine Kopie einer Maßnahmendomäne.                            |
| DEFINE DOMAIN | Definiert eine Maßnahmendomäne, der Clients zugeordnet werden können. |
| QUERY DOMAIN  | Zeigt Informationen über Maßnahmendomänen an.                         |
| UPDATE DOMAIN | Ändert die Attribute einer Maßnahmendomäne.                           |

## DELETE DRIVE (Laufwerk aus einem Kassettenarchiv löschen)

Mit diesem Befehl kann ein Laufwerk aus einem Kassettenarchiv gelöscht werden. Ein Laufwerk, das gerade verwendet wird, kann nicht gelöscht werden.

Alle Pfade zu einem Laufwerk müssen gelöscht werden, bevor das Laufwerk selbst gelöscht werden kann.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-DELeTe DRive--Kassettenarchivname--Laufwerkname-----<<
```

### Parameter

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, in dem sich das Laufwerk befindet.

Laufwerkname (Erforderlich)

Gibt den Namen des Laufwerks an, das gelöscht werden soll.

### Beispiel: Ein Laufwerk aus einem Kassettenarchiv löschen

Laufwerk DRIVE3 aus dem Kassettenarchiv AUTO löschen.

```
delete drive auto drive3
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE DRIVE

| Befehl            | Beschreibung  |
|-------------------|---|
| DEFINE DRIVE      | Ordnet ein Laufwerk einem Kassettenarchiv zu.                       |
| DEFINE LIBRARY    | Definiert ein automatisiertes oder manuelles Kassettenarchiv.       |
| DELETE LIBRARY    | Löscht ein Kassettenarchiv.   |
| DELETE PATH       | Löscht einen Pfad von einer Quelle zu einem Ziel.                   |
| PERFORM LIBACTION | Definiert alle Laufwerke und Pfade für ein Kassettenarchiv.         |
| QUERY DRIVE       | Zeigt Informationen zu Laufwerken an.                               |
| QUERY LIBRARY     | Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an. |
| UPDATE DRIVE      | Ändert die Attribute eines Laufwerks.                               |

## DELETE EVENT (Ereignissätze löschen)

Mit diesem Befehl können Ereignissätze aus der Datenbank gelöscht werden. Ein Ereignissatz wird erstellt, wenn die Verarbeitung eines geplanten Befehls gestartet wird oder fehlschlägt.

Dieser Befehl löscht nur die Ereignissätze, die zum Zeitpunkt der Befehlsverarbeitung vorhanden sind. Ein Ereignissatz wird nicht gefunden, wenn:

- Der Ereignissatz nie erstellt wurde (das Ereignis ist für die Zukunft geplant)
- Das Ereignis bereits stattgefunden hat und der Ereignissatz bereits gelöscht wurde.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

## Syntax

```

                .-00:00-.
>>-DELEte EVent--Datum--+-----+----->
                '-Zeit--'

.-TYPE--==--Client-----
>+-----+-----+-----<
'-TYPE--==--+Client-----+'
      +-Administrative-+
      '-All-----'

```

## Parameter

### Datum (Erforderlich)

Gibt das Datum an, mit dem bestimmt wird, welche Ereignissätze gelöscht werden sollen. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.

Diesen Parameter in Verbindung mit dem Parameter TIME verwenden, um ein Datum und eine Uhrzeit zum Löschen von Ereignissätzen anzugeben. Alle Sätze, deren geplanter Start vor dem angegebenen Datum und der angegebenen Zeit liegt, werden gelöscht. Sätze von Ereignissen, deren Startfenster noch nicht abgelaufen ist, werden jedoch nicht gelöscht.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum                                     | 09/15/1998   |
| TODAY                          | Das aktuelle Datum                                       | TODAY  |
| TODAY-Tage <i>oder</i> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage | TODAY-3 <i>oder</i> -3.  |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.                            | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.      | EOLM-1<br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.                      | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage. | BOTM+9<br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

### Zeit

Gibt die Zeit an, mit der bestimmt wird, welche Ereignissätze gelöscht werden sollen. Diesen Parameter in Verbindung mit dem Parameter DATE verwenden, um ein Datum und eine Uhrzeit zum Löschen von Ereignissätzen anzugeben. Alle Sätze, deren geplanter Start vor dem angegebenen Datum und der angegebenen Zeit liegt, werden gelöscht. Sätze von Ereignissen, deren Startfenster noch nicht abgelaufen ist, werden jedoch nicht gelöscht. Der Standardwert ist 00:00.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert     | Beschreibung           | Beispiel |
|----------|------------------------|----------|
| HH:MM:SS | Eine bestimmte Uhrzeit | 10:30:08 |

| Wert                             | Beschreibung   | Beispiel  |
|----------------------------------|--|---|
| NOW                              | Die aktuelle Uhrzeit   | NOW   |
| NOW+HH:MM <i>oder</i><br>+HH:MM  | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten  | NOW+03:00 <i>oder</i> +03:00<br>Achtung: Wird dieser Befehl um 9:00 Uhr unter Verwendung von NOW+03:00 <i>oder</i> +03:00 ausgegeben, löscht IBM Spectrum Protect Sätze mit der Uhrzeit 12:00 oder einer späteren Uhrzeit an dem Datum, das angegeben wird. |
| NOW-HH:MM <i>oder</i> -<br>HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten | NOW-03:00 <i>oder</i> -03:00  |

#### TYPE

Gibt die Art der zu löschenden Ereignisse an. Dieser Parameter ist wahlfrei. Der Standardwert ist CLIENT. Gültige Werte:

#### Client

Gibt an, dass Ereignissätze für Clientzeitpläne gelöscht werden sollen.

#### ADministrative

Gibt an, dass Ereignissätze für Verwaltungsbefehlszeitpläne gelöscht werden sollen.

#### ALI

Gibt an, dass Ereignissätze für Client- und Verwaltungsbefehlszeitpläne gelöscht werden sollen.

## Beispiel: Ereignissätze löschen

Sätze für Ereignisse löschen, deren geplante Startzeit vor 08:00 am 26. Mai 1998 (05/26/1998) liegt und deren Startfenster abgelaufen sind. Die Sätze für diese Ereignisse werden unabhängig davon gelöscht, ob der durch den Befehl SET EVENTRETENTION angegebene Aufbewahrungszeitraum für Ereignissätze bereits verstrichen ist.

```
delete event 05/26/1998 08:00
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE EVENT

| Befehl             | Beschreibung  |
|--------------------|---|
| QUERY EVENT        | Zeigt Informationen über geplante und abgeschlossene Ereignisse für ausgewählte Clients an. |
| SET EVENTRETENTION | Gibt die Anzahl Tage für die Aufbewahrung von Sätzen geplanter Operationen an.              |

## DELETE EVENTSERVER (Definition des Ereignisservers löschen)

Mit diesem Befehl kann die Definition des Ereignisservers gelöscht werden. Dieser Befehl muss ausgegeben werden, bevor der Befehl DELETE SERVER ausgegeben wird. Wenn der als Ereignisserver definierte Server im Befehl DELETE SERVER angegeben wird, wird eine Fehlermeldung angezeigt.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-DELeTe EVENTSErVer-----<<
```

## Beispiel: Eine Ereignisserverdefinition löschen

Die Definition des Ereignisservers ASTRO löschen.

```
delete eventserver
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE EVENTSERVER

| Befehl             | Beschreibung                               |
|--------------------|--|
| DEFINE EVENTSERVER | Definiert einen Server als Ereignisserver. |
| QUERY EVENTSERVER  | Zeigt den Namen des Ereignisserver an.     |

## DELETE FILESPACE (Clientknotendaten aus dem Server löschen)

Mit diesem Befehl können Dateibereiche aus dem Server gelöscht werden. Dateien, die zu dem Dateibereich gehören, werden aus primären Speicherpools, Speicherpools für aktive Daten und Kopierspeicherpools sowie aus allen Dateibereichskollokationsgruppen gelöscht.

IBM Spectrum Protect löscht einen oder mehrere Dateibereiche als eine Serie von Stapeldatenbanktransaktionen, wodurch eine ROLLBACK- oder COMMIT-Operation für einen vollständigen Dateibereich als eine einzelne Aktion verhindert wird. Wird der Prozess abgebrochen oder tritt ein Systemfehler auf, kann ein partielles Löschen erfolgen. Mit einem nachfolgenden Befehl DELETE FILESPACE für denselben Knoten oder Eigner können die übrigen Daten gelöscht werden.

Wird dieser Befehl auf einen WORM-Datenträger (WORM = Write Once, Read Many) angewendet, kehrt der Datenträger in den Arbeitsdatenträgerstatus zurück, wenn er über Speicherbereich verfügt, in den Daten geschrieben werden können. (Daten auf WORM-Datenträgern, einschließlich gelöschter und verfallener Daten, können nicht überschrieben werden. Daher können Daten nur in Speicherbereich geschrieben werden, der keine aktuellen, gelöschten oder verfallenen Daten enthält.) Verfügt ein WORM-Datenträger über keinen Speicherbereich mehr, in den Daten geschrieben werden können, verbleibt der Datenträger im privaten Status. Soll der Datenträger aus dem Kassettenarchiv entfernt werden, müssen Sie den Befehl CHECKOUT LIBVOLUME verwenden.

Tipps:

- Ist der Aufbewahrungsschutz für Archivierung aktiviert, löscht der Server Archivierungsdateien mit abgelaufenen Aufbewahrungszeiträumen. Weitere Informationen finden Sie in der Beschreibung des Befehls SET ARCHIVERETENTIONPROTECTION.
- Archivierungsdateien, für die "Löschen unzulässig" angegeben wurde, können vom Server erst gelöscht werden, wenn die Löschsperre aufgehoben wird.
- Die Wiederherstellung wird nicht gestartet, solange der Befehl DELETE FILESPACE ausgeführt wird.
- Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.
- Wenn Sie einen Dateibereich in einem deduplizierten Speicherpool löschen, wird der Dateibereichsname DELETED in der Ausgabe des Befehls QUERY OCCUPANCY angezeigt, bis alle Deduplizierungsabhängigkeiten entfernt wurden.
- Wenn die Replikation für einen Dateibereich konfiguriert ist, löscht der Befehl DELETE FILESPACE nur den Dateibereich auf dem Server, auf dem der Befehl ausgegeben wurde. Wird der Befehl REPLICATE NODE ausgegeben, wird der Dateibereich nicht auf dem anderen Replikationsserver gelöscht.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, der der Clientknoten zugeordnet ist.

## Syntax

```
>>-DELeTe Filespace--Knotenname--Dateibereichsname----->
. -Type---ANY----- . -Data---ANY-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -Type---ANY-----+ ' -Data---ANY-----+
      +-Backup-----+          +-Files-----+
      +-ARchive-----+          | (1) |
      +-SPacemanaged+          ' -IMages-----'
      '-SERver-----'

. -Wait---No-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -Wait---No---+ ' -OWNer---Eigername-
      '-Yes-'

. -NAMeType---SERVER-----
>+-----+-----+-----+-----+-----+-----+-----+-----+----->
' -NAMeType---SERVER---+
      +-UNICODE+
      '-FSID-----'
```

```

.-CODEType----BOTH-----
>-----+-----+-----><
'-CODEType----+UNiCode----+'
      +-NONUNiCode-+
      '-BOTH-----'

```

Anmerkungen:

1. Dieser Parameter kann nur verwendet werden, wenn `TYPE=ANY` oder `TYPE=BACKUP` angegeben wird.

## Parameter

---

**Knotenname** (Erforderlich)

Gibt den Namen des Clientknotens an, zu dem der Dateibereich gehört.

**Dateibereichsname** (Erforderlich)

Gibt den Namen des Dateibereichs an, der gelöscht werden soll. Bei diesem Namen muss die Groß-/Kleinschreibung berücksichtigt werden, und der Name muss genau so eingegeben werden, wie er dem Server bekannt ist. Um zu bestimmen, wie der Name eingegeben wird, den Befehl `QUERY FILESPACE` verwenden. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden.

Ein Server, der über Clients mit Unterstützung für Unicode verfügt, muss möglicherweise den Dateibereichsnamen, den Sie eingeben, konvertieren. Beispielsweise muss der Server gegebenenfalls den eingegebenen Namen aus der Codepage des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich unter dem Parameter `NAMETYPE`. Geben Sie keinen Dateibereichsnamen an oder geben Sie nur ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter `CODETYPE` verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

**Type**

Gibt den zu löschenden Datentyp an. Dieser Parameter ist wahlfrei. Der Standardwert ist `ANY`. Sie können die folgenden Werte verwenden:

**ANY**

Nur gesicherte Versionen von Dateien und archivierte Kopien von Dateien löschen.

Wenn Sie `delete filespace Knotenname * type=any` angeben, werden alle gesicherten Daten und archivierten Daten in allen Dateibereichen für diesen Knoten gelöscht. Dateibereiche werden nur gelöscht, wenn sie keine Dateien enthalten, die von einem IBM Spectrum Protect for Space Management-Client versetzt werden.

**Backup**

Sicherungsdaten für den Dateibereich löschen.

**ARchive**

Alle archivierten Daten auf dem Server für den Dateibereich löschen.

**SPacemanaged**

Dateien löschen, die aus dem lokalen Dateisystem eines Benutzers von einem IBM Spectrum Protect for Space Management-Client umgelagert werden. Der Parameter `OWNER` wird ignoriert, wenn `TYPE=SPACEMANAGED` angegeben wird.

**SERver**

Alle archivierten Dateien in allen Dateibereichen für einen Knoten löschen, der als `TYPE=SERVER` registriert ist.

**DAta**

Gibt zu löschende Objekte an. Dieser Parameter ist wahlfrei. Der Standardwert ist `ANY`. Sie können einen der folgenden Werte angeben:

**ANY**

Dateien, Verzeichnisse und Abbilder löschen.

**FIles**

Dateien und Verzeichnisse löschen.

**IMages**

Abbildobjekte löschen. Sie können diesen Parameter nur verwenden, wenn Sie `TYPE=ANY` oder `TYPE=BACKUP` angegeben haben.

**Wait**

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist `No`. Sie können einen der folgenden Werte angeben:

**No**

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

Nachrichten, die von dem Hintergrundprozess erstellt werden, werden entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Erst nachdem der Befehl vollständig ausgeführt wurde, kann mit anderen Aufgaben fortgefahren werden. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungs-Client an, wenn der Befehl beendet ist.

Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

OWNer

Beschränkt die zu löschenden Daten auf Dateien, die zu dem Eigner gehören. Dieser Parameter ist wahlfrei; er wird bei TYPE=SPACEMANAGED ignoriert. Dieser Parameter gilt nur für Clientmehrbennutzersysteme, wie z. B. AIX, Linux und Solaris OS.

NAMEType

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unterstützung für Unicode verfügt. Ein Client für Sichern/Archivieren mit Unterstützung für Unicode ist nur für die folgenden Betriebssysteme verfügbar: Windows, Macintosh OS X und NetWare.

Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen eingeben. Der Standardwert lautet SERVER. Sie können einen der folgenden Werte angeben:

SERVER

Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren.

UNICODE

Der Server konvertiert die Dateibereichsnamen aus der Server-Codepage in die Codepage UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

FSID

Der Server interpretiert die Dateibereichsnamen als ihre Dateibereichs-IDs (FSIDs).

CODEType

Angeben, welche Art von Dateibereichen in der Operation berücksichtigt werden soll. Der Standardwert lautet BOTH. Dieser Standardwert bedeutet, dass Dateibereiche unabhängig vom Typ der Codepage eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben. Sie können einen der folgenden Werte angeben:

UNICODE

Dateibereiche einschließen, die in Unicode sind.

NONUNICODE

Dateibereiche einschließen, die nicht in Unicode sind.

BOTH

Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen.

## Dateibereich löschen

Den Dateibereich C\_Drive löschen, der zum Clientknoten HTANG gehört.

```
delete filespace htang C_Drive
```

## Alle speicherverwalteten Dateien für einen Clientknoten löschen

Alle Dateien löschen, die vom Clientknoten APOLLO umgelagert werden (d. h., alle speicherverwalteten Dateien).

```
delete filespace apollo * type=spacemanaged
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE FILESPACE

| Befehl          | Beschreibung  |
|-----------------|---|
| CANCEL PROCESS  | Bricht einen Serverhintergrundprozess ab.                                       |
| QUERY ACTLOG    | Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.                        |
| QUERY FILESPACE | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören. |
| QUERY OCCUPANCY | Zeigt Dateibereichsdaten anhand des Speicherpools an.                           |

| Befehl           | Beschreibung   |
|------------------|--|
| QUERY PROCESS    | Zeigt Informationen über Hintergrundprozesse an.   |
| REMOVE NODE      | Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne. |
| RENAME FILESPACE | Vergibt einen neuen Namen für einen Clientdateibereich auf dem Server.                           |

## DELETE GRPMEMBER (Server aus einer Servergruppe löschen)

Mit diesem Befehl kann ein Server oder eine Servergruppe aus einer Servergruppe gelöscht werden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```

      .-|-----|
      v          |
>>-DELeTe GRPMEMber--Gruppenname----Name_des_Teils+-----><

```

### Parameter

Gruppenname (Erforderlich)

Gibt die Gruppe an.

Name\_des\_Teils (Erforderlich)

Gibt den Server oder die Gruppe an, der bzw. die aus der Gruppe gelöscht werden soll. Sollen mehrere Namen angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

### Beispiel: Einen Server aus einer Servergruppe löschen

Teil PHOENIX aus Gruppe WEST\_COMPLEX löschen.

```
delete grpmember west_complex phoenix
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE GRPMEMBER

| Befehl             | Beschreibung  |
|--------------------|---|
| DEFINE GRPMEMBER   | Definiert einen Server als Teil einer Servergruppe. |
| DEFINE SERVERGROUP | Definiert eine neue Servergruppe.                   |
| DELETE SERVER      | Löscht die Definition eines Servers.                |
| DELETE SERVERGROUP | Löscht eine Servergruppe.                           |
| MOVE GRPMEMBER     | Versetzt einen Teil einer Servergruppe.             |
| QUERY SERVER       | Zeigt Informationen über Server an.                 |
| QUERY SERVERGROUP  | Zeigt Informationen über Servergruppen an.          |
| RENAME SERVERGROUP | Benennt eine Servergruppe um.                       |
| UPDATE SERVERGROUP | Aktualisiert eine Servergruppe.                     |

## DELETE LIBRARY (Kassettenarchiv löschen)

Mit diesem Befehl kann ein Kassettenarchiv gelöscht werden. Bevor Sie ein Kassettenarchiv löschen, müssen Sie andere zugeordnete Objekte, wie beispielsweise den Pfad, löschen.



Mit diesem Befehl kann ein Kassettenarchiv gelöscht werden. Bevor Sie ein Kassettenarchiv löschen, löschen Sie den Pfad und alle zugeordneten Laufwerke.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
>>-DELeTe LIBRary--Kassettenarchivname-----><
```

## Parameter

---

Speicherarchivname (Erforderlich)  
Gibt den Namen des Kassettenarchivs an, das gelöscht werden soll.

## Beispiel: Ein manuelles Kassettenarchiv löschen

---

Das manuelle Kassettenarchiv LIBR1 löschen.

```
delete library libr1
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für DELETE LIBRARY

| Befehl            | Beschreibung  |
|-------------------|---|
| DEFINE DRIVE      | Ordnet ein Laufwerk einem Kassettenarchiv zu.                       |
| DEFINE LIBRARY    | Definiert ein automatisiertes oder manuelles Kassettenarchiv.       |
| DEFINE PATH       | Definiert einen Pfad von einer Quelle zu einem Ziel.                |
| DELETE DRIVE      | Löscht ein Laufwerk aus einem Kassettenarchiv.                      |
| DELETE PATH       | Löscht einen Pfad von einer Quelle zu einem Ziel.                   |
| PERFORM LIBACTION | Definiert alle Laufwerke und Pfade für ein Kassettenarchiv.         |
| QUERY DRIVE       | Zeigt Informationen zu Laufwerken an.                               |
| QUERY LIBRARY     | Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an. |
| QUERY PATH        | Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.     |
| UPDATE DRIVE      | Ändert die Attribute eines Laufwerks.                               |
| UPDATE LIBRARY    | Ändert die Attribute eines Kassettenarchivs.                        |
| UPDATE PATH       | Ändert die zu einem Pfad gehörigen Attribute.                       |

## DELETE MACHINE (Maschineninformationen löschen)

---

Mit diesem Befehl können Maschineninformationen gelöscht werden. Sollen vorhandene Informationen ersetzt werden, diesen Befehl ausgeben und dann einen Befehl INSERT MACHINE verwenden.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-DELeTe MACHine--Maschinename----->  
.-Type--==--All-----  
>--+-----><
```

```
'-Type--==++-All-----+'
      +-RECOVERYInstructions-+
      '-Characteristics-----'
```

## Parameter

Maschinenname (Erforderlich)

Gibt den Namen der Maschine an, deren Informationen gelöscht werden sollen.

Type

Gibt die Art der Maschineninformationen an. Dieser Parameter ist wahlfrei. Standardwert ist ALL. Gültige Werte:

All

Gibt alle Informationen an.

RECOVERYInstructions

Gibt die Anweisungen zur Fehlerbehebung an.

CHaracteristics

Gibt die Maschinenkenndaten an.

## Beispiel: Informationen zu einer bestimmten Maschine löschen

Die Maschinenkenndaten löschen, die der Maschine DISTRICT5 zugeordnet sind.

```
delete machine district5 type=characteristics
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE MACHINE

| Befehl              | Beschreibung  |
|---------------------|---|
| DEFINE MACHINE      | Definiert eine Maschine für DRM.  |
| INSERT MACHINE      | Fügt Maschinenkenndaten oder Wiederherstellungsanweisungen in die IBM Spectrum Protect-Datenbank ein. |
| QUERY MACHINE       | Zeigt Informationen über Maschinen an.  |
| QUERY RECOVERYMEDIA | Zeigt die für die Maschinenwiederherstellung verfügbaren Datenträger an.                              |
| UPDATE MACHINE      | Ändert die Informationen zu einer Maschine.   |

## DELETE MACHNODEASSOCIATION (Zuordnung zwischen Maschine und Knoten löschen)

Mit diesem Befehl kann die Zuordnung zwischen einer Maschine und einem oder mehreren Knoten gelöscht werden. Dieser Befehl löscht nicht den Knoten aus IBM Spectrum Protect.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-DElete MACHNODEAssociation--Maschinenname----Knotenname+----<<
```

## Parameter

Maschinenname (Erforderlich)

Gibt den Namen einer Maschine an, die einem oder mehreren Knoten zugeordnet ist.

Knotenname (Erforderlich)

Gibt den Namen eines Knotens an, der einer Maschine zugeordnet ist. Wird eine Liste mit Knotennamen angegeben, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um einen Namen

anzugeben. Ist ein Knoten nicht der Maschine zugeordnet, wird dieser Knoten ignoriert.

## Beispiel: Eine Zuordnung zwischen einem Knoten und einer Maschine löschen

Die Zuordnung zwischen Maschine DISTRICT5 und Knoten ACCOUNTSPAYABLE löschen.

```
delete machnodeassociation district5 accountspayable
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE MACHNODEASSOCIATION

| Befehl                     | Beschreibung  |
|----------------------------|---|
| DEFINE MACHNODEASSOCIATION | Ordnet einen IBM Spectrum Protect-Knoten einer Maschine zu. |
| QUERY MACHINE              | Zeigt Informationen über Maschinen an.                      |

## DELETE MGMTCLASS (Verwaltungsklasse löschen)

Mit diesem Befehl kann eine Verwaltungsklasse gelöscht werden. Eine Verwaltungsklasse in der aktiven Maßnahmengruppe (ACTIVE) kann nicht gelöscht werden. Alle Kopiengruppen in der Verwaltungsklasse werden mit der Verwaltungsklasse gelöscht.

Der Benutzer kann die Verwaltungsklasse löschen, die als Standardwert für eine Maßnahmengruppe zugeordnet ist, eine Maßnahmengruppe kann jedoch nur aktiviert werden, wenn sie über eine Standardverwaltungsklasse verfügt.

Die vordefinierte Verwaltungsklasse STANDARD in der Maßnahmendomäne STANDARD kann gelöscht werden. Wird der IBM Spectrum Protect-Server jedoch später erneut installiert, schreibt der Prozess alle Maßnahmenobjekte STANDARD zurück.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Verwaltungsklasse gehört.

## Syntax

```
>>-DElete Mgmtclass--Domänenname--Name_der_Maßnahmengruppe--Klassenname-><
```

## Parameter

Domänenname (Erforderlich)

Gibt die Maßnahmendomäne an, zu der die Verwaltungsklasse gehört.

Name\_der\_Maßnahmengruppe (Erforderlich)

Gibt die Maßnahmengruppe an, zu der die Verwaltungsklasse gehört.

Klassenname (Erforderlich)

Gibt die Verwaltungsklasse an, die gelöscht werden soll.

## Beispiel: Eine Verwaltungsklasse löschen

Die Verwaltungsklasse ACTIVEFILES aus der Maßnahmengruppe VACATION der Maßnahmendomäne EMPLOYEE\_RECORDS löschen.

```
delete mgmtclass employee_records  
vacation activefiles
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE MGMTCLASS

| Befehl              | Beschreibung   |
|---------------------|--|
| ASSIGN DEFMGMTCLASS | Ordnet eine Verwaltungsklasse als Standardklasse für eine angegebene Maßnahmengruppe zu. |
| COPY MGMTCLASS      | Erstellt eine Kopie einer Verwaltungsklasse.   |
| DEFINE MGMTCLASS    | Definiert eine Verwaltungsklasse.  |

| Befehl           | Beschreibung                                  |
|------------------|---|
| QUERY MGMTCLASS  | Zeigt Informationen zu Verwaltungsklassen an. |
| UPDATE MGMTCLASS | Ändert die Attribute einer Verwaltungsklasse. |

## DELETE NODEGROUP (Knotengruppe löschen)

Verwenden Sie diesen Befehl, um eine Knotengruppe zu löschen. Eine Knotengruppe kann nicht gelöscht werden, wenn sie Einträge enthält.

Achtung: Sie können alle Einträge in der Knotengruppe entfernen, indem Sie den Befehl DELETE NODEGROUPMEMBER mit einem Platzhalterzeichen im Parameter Knotenname ausgeben.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

### Syntax

```
>>-DELEte NODEGroup--Gruppenname-----<<
```

### Parameter

Gruppenname  
Gibt den Namen der Knotengruppe an, die gelöscht werden soll.

### Beispiel: Eine Knotengruppe löschen

Die Knotengruppe `group1` löschen.

```
delete nodegroup group1
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE NODEGROUP

| Befehl                 | Beschreibung  |
|------------------------|---|
| DEFINE BACKUPSET       | Definiert eine zuvor generierte Sicherungsgruppe für einen Server.          |
| DEFINE NODEGROUP       | Definiert eine Gruppe von Knoten.   |
| DEFINE NODEGROUPMEMBER | Fügt einer Knotengruppe einen Clientknoten hinzu.                           |
| DELETE BACKUPSET       | Löscht eine Sicherungsgruppe.   |
| DELETE NODEGROUPMEMBER | Löscht einen Clientknoten aus einer Knotengruppe.                           |
| GENERATE BACKUPSET     | Generiert eine Sicherungsgruppe mit den Daten eines Clients.                |
| QUERY BACKUPSET        | Zeigt Sicherungsgruppen an.   |
| QUERY NODEGROUP        | Zeigt Informationen zu Knotengruppen an.                                    |
| UPDATE BACKUPSET       | Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum. |
| UPDATE NODEGROUP       | Aktualisiert die Beschreibung einer Knotengruppe.                           |

## DELETE NODEGROUPMEMBER (Eintrag aus der Knotengruppe löschen)

Verwenden Sie diesen Befehl, um einen Clientknoten aus einer Knotengruppe zu löschen.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

## Syntax

```
>>-DELeTe NOdeGRouPMeMber--Gruppenname---Knotenname-+-----><
```

## Parameter

### Gruppenname

Gibt den Namen der Knotengruppe an, aus der ein Clientknoten gelöscht werden soll.

### Knotenname

Gibt den Namen des Clientknotens an, der aus der Knotengruppe gelöscht werden soll. Sie können einen oder mehrere Namen angeben. Werden mehrere Namen angegeben, sind die Namen durch Kommas voneinander zu trennen; verwenden Sie zwischen den Namen keine Leerzeichen. Sie können auch Platzhalterzeichen verwenden, um mehrere Knoten anzugeben.

## Beispiel: Knoten aus einer Knotengruppe löschen

Die beiden Knoten `node1` und `node2` aus der Knotengruppe `group1` löschen.

```
delete nodegroupmember group1 node1,node2
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE NODEGROUPMEMBER

| Befehl                 | Beschreibung  |
|------------------------|---|
| DEFINE BACKUPSET       | Definiert eine zuvor generierte Sicherungsgruppe für einen Server.          |
| DEFINE NODEGROUP       | Definiert eine Gruppe von Knoten.   |
| DEFINE NODEGROUPMEMBER | Fügt einer Knotengruppe einen Clientknoten hinzu.                           |
| DELETE BACKUPSET       | Löscht eine Sicherungsgruppe.   |
| DELETE NODEGROUP       | Löscht eine Knotengruppe.   |
| GENERATE BACKUPSET     | Generiert eine Sicherungsgruppe mit den Daten eines Clients.                |
| QUERY BACKUPSET        | Zeigt Sicherungsgruppen an.   |
| QUERY NODEGROUP        | Zeigt Informationen zu Knotengruppen an.                                    |
| UPDATE BACKUPSET       | Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum. |
| UPDATE NODEGROUP       | Aktualisiert die Beschreibung einer Knotengruppe.                           |

## DELETE PATH (Pfad löschen)

Verwenden Sie diesen Befehl, um eine Pfaddefinition zu löschen.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-DELeTe PATH--Quellename--Zielname----->
(1)
>--SRCType-----+--DATAMover-----+----->
'-SERVer-----'
(2)
>--DESTType-----+--DRive-----LIBRary-----Kassettenarchivname-+--><
'-LIBRary-----'
```

Anmerkungen:

1. Dieser Parameter ist nur für die Betriebssysteme AIX, HP-UX, Linux, Solaris und Windows verfügbar.
2. Dieser Parameter ist nur für die Betriebssysteme AIX, HP-UX, Linux, Solaris und Windows verfügbar.

## Parameter

---

Quellenname (Erforderlich)

Gibt den Namen der Quelle des Pfads an, der gelöscht werden soll. Dieser Parameter ist erforderlich.

Bei dem angegebenen Namen muss es sich um den Namen eines Servers oder einer Einheit zum Versetzen von Daten handeln, der bereits für den Server definiert ist.

Zielname (Erforderlich)

Gibt den Namen des Ziels des Pfads an, der gelöscht werden soll. Dieser Parameter ist erforderlich.

SRCType (Erforderlich)

Gibt den Typ der Quelle des Pfads an, der gelöscht werden soll. Dieser Parameter ist erforderlich. Gültige Werte:

DATAMover

Gibt an, dass eine Einheit zum Versetzen von Daten die Quelle ist.

SERVER

Gibt an, dass ein Speicheragent die Quelle ist.

DESTType (Erforderlich)

Gibt den Typ des Ziels an. Gültige Werte:

DRive LIBRARY=Kassettenarchivname

Gibt an, dass ein Laufwerk das Ziel ist. Die Parameter DRIVE und LIBRARY sind erforderlich, wenn der Zieltyp DRIVE ist.

LIBRARY

Gibt an, dass ein Kassettenarchiv das Ziel ist.

Achtung: Wird der Pfad von einer Einheit zum Versetzen von Daten zu einem Kassettenarchiv oder der Pfad vom Server zu einem Kassettenarchiv gelöscht, kann der Server nicht auf das Kassettenarchiv zugreifen. Wird bei diesem Status der Server angehalten und erneut gestartet, wird das Kassettenarchiv nicht initialisiert.

## Beispiel: Einen Pfad von einer NAS-Einheit zum Versetzen von Daten löschen

---

Einen Pfad von der NAS-Einheit zum Versetzen von Daten NAS1 zu dem Kassettenarchiv NASLIB löschen.

```
delete path nas1 naslib srctype=datamover desttype=library
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für DELETE PATH

| Befehl            | Beschreibung  |
|-------------------|---|
| DEFINE DATAMOVER  | Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server. |
| DEFINE PATH       | Definiert einen Pfad von einer Quelle zu einem Ziel.                                |
| PERFORM LIBACTION | Definiert alle Laufwerke und Pfade für ein Kassettenarchiv.                         |
| QUERY PATH        | Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.                     |
| UPDATE PATH       | Ändert die zu einem Pfad gehörigen Attribute.                                       |

## DELETE POLICYSET (Maßnahmengruppe löschen)

---

Mit diesem Befehl kann eine Maßnahmengruppe gelöscht werden. Wenn eine Maßnahmengruppe gelöscht wird, werden alle Verwaltungsklassen und Kopiengruppen, die zu der Maßnahmengruppe gehören, ebenfalls gelöscht.

Die Maßnahmengruppe ACTIVE in einer Maßnahmendomäne kann nicht gelöscht werden. Sie können den Inhalt der Maßnahmengruppe ACTIVE ersetzen, indem Sie eine andere Maßnahmengruppe aktivieren. Andernfalls können Sie die Maßnahmengruppe ACTIVE nur entfernen, indem Sie die Maßnahmendomäne löschen, die die Maßnahmengruppe enthält.

Die vordefinierte Maßnahmengruppe STANDARD kann gelöscht werden. Wird der IBM Spectrum Protect-Server jedoch später erneut installiert, schreibt der Prozess alle Maßnahmenobjekte STANDARD zurück.



```

>----->
'-DObains-----+*-----+
| .-,-----+ |
| V          | |
|---Domänennam-----+
>----->
'-ADSHeds-----+*-----+
| .-,-----+ |
| V          | |
|---Zeitplannam-----+
>----->
'-ScripAs-----+*-----+
| .-,-----+ |
| V          | |
|---Scriptnam-----+
>----->
'-CLOpAs-----+*-----+
| .-,-----+ |
| V          | |
|---Optionsgruppennam-----+
>----->
'-SERVers-----+*-----+
| .-,-----+ |
| V          | |
|---Servernam-----+
>-----<
'-SERVERGroups-----+*-----+
| .-,-----+ |
| V          | |
|---Gruppennam-----+

```

## Parameter

### Profilname (Erforderlich)

Gibt das Profil an, aus dem Zuordnungen gelöscht werden sollen.

### ADMins

Gibt die Administratoren an, deren Zuordnung zu dem Profil gelöscht wird. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Das Zeichen \* verwenden, um alle Administratoren aus dem Profil zu löschen. Wird eine Administratorliste angegeben und ist für das Profil eine globale Definition vorhanden, schlägt der Befehl fehl.

Administratordefinitionen werden auf dem Konfigurationsmanager nicht geändert. Sie werden jedoch bei der nächsten Konfigurationsaktualisierung automatisch aus allen subscribierenden verwalteten Servern gelöscht. Dabei gelten folgende Ausnahmen:

- Ein Administrator wird nicht gelöscht, wenn dieser Administrator eine offene Sitzung auf dem Server hat.
- Ein Administrator wird nicht gelöscht, wenn der verwaltete Server als Folge des Löschens über keine Administratoren mit Systemberechtigung verfügen würde.

### DOmains

Gibt die Domänen an, deren Zuordnung zu dem Profil gelöscht wird. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Das Zeichen \* verwenden, um alle Domänen aus dem Profil zu löschen. Wird eine Domänenliste angegeben und ist für das Profil eine globale Domänendefinition vorhanden, schlägt der Befehl fehl.

Die Domäneninformationen werden automatisch aus allen subscribierenden verwalteten Servern gelöscht. Eine Maßnahmendomäne, der Client-Knoten zugeordnet sind, wird jedoch nicht gelöscht. Um die Domäne auf dem verwalteten Server zu löschen, müssen diese Clientknoten einer anderen Maßnahmendomäne zugeordnet werden.

### ADSHeds

Gibt eine Liste der Verwaltungszeitpläne an, deren Zuordnung zu dem Profil gelöscht wird. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird eine Verwaltungszeitplanliste angegeben und ist für das Profil eine globale Verwaltungszeitplandefinition vorhanden, schlägt der Befehl fehl. Das Zeichen \* verwenden, um alle Verwaltungszeitpläne aus dem Profil zu löschen.

Die Verwaltungszeitpläne werden automatisch aus allen subscribierenden verwalteten Servern gelöscht. Ein Verwaltungszeitplan wird jedoch nicht gelöscht, wenn der Zeitplan auf dem verwalteten Server aktiv ist. Um einen aktiven Zeitplan zu löschen, muß der



Zeitplan inaktiviert werden.

#### SCRipts

Gibt die Server-Befehlsprozeduren an, deren Zuordnung zu dem Profil gelöscht wird. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Das Zeichen \* verwenden, um alle Prozeduren aus dem Profil zu löschen. Wird eine Prozedurliste angegeben und ist für das Profil eine globale Prozedurdefinition vorhanden, schlägt der Befehl fehl. Die Server-Befehlsprozeduren werden automatisch aus allen subscribierenden verwalteten Servern gelöscht.

#### CLOptsets

Gibt die Client-Optionsgruppen an, deren Zuordnung zu dem Profil gelöscht wird. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Das Zeichen \* verwenden, um alle Client-Optionsgruppen aus dem Profil zu löschen. Wird eine Client-Optionsgruppenliste angegeben und ist für das Profil eine globale Client-Optionsgruppendefinition vorhanden, schlägt der Befehl fehl. Die Clientoptionsgruppen werden automatisch aus allen subscribierenden verwalteten Servern gelöscht.

#### SERVers

Gibt die Server an, deren Zuordnung zu dem Profil gelöscht wird. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Das Zeichen \* verwenden, um alle Server aus dem Profil zu löschen. Wird eine Server-Liste angegeben und ist für das Profil eine globale Server-Definition vorhanden, schlägt der Befehl fehl. Die Serverdefinitionen werden automatisch aus allen subscribierenden verwalteten Servern gelöscht. Dabei gelten folgende Ausnahmen:

- Eine Serverdefinition wird nicht gelöscht, wenn der verwaltete Server über eine geöffnete Verbindung zu einem anderen Server verfügt.
- Eine Serverdefinition wird nicht gelöscht, wenn der verwaltete Server über eine Einheitenklasse des Einheitentyps SERVER verfügt, die auf den anderen Server verweist.
- Eine Serverdefinition wird nicht gelöscht, wenn es sich um den Ereignisserver für den verwalteten Server handelt.

#### SERVERGroups

Gibt die Server-Gruppen an, deren Zuordnung zu dem Profil gelöscht wird. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Das Zeichen \* verwenden, um alle Server-Gruppen aus dem Profil zu löschen. Wird eine Server-Gruppenliste angegeben und ist für das Profil eine globale Gruppendifinition vorhanden, schlägt der Befehl fehl. Die Servergruppendefinitionen werden automatisch aus allen subscribierenden verwalteten Servern gelöscht.

## Beispiel: Die Domänenzuordnungen für ein bestimmtes Profil löschen

Alle Domänenzuordnungen aus dem Profil MIKE löschen.

```
delete profassociation mike domains=*
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE PROFASSOCIATION

| Befehl                 | Beschreibung   |
|------------------------|--|
| COPY PROFILE           | Erstellt eine Kopie eines Profils.   |
| DEFINE PROFASSOCIATION | Ordnet Objekte einem Profil zu.  |
| DEFINE PROFILE         | Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.  |
| DELETE PROFILE         | Löscht ein Profil aus einem Konfigurationsmanager.                               |
| LOCK PROFILE           | Verhindert die Verteilung eines Konfigurationsprofils.                           |
| NOTIFY SUBSCRIBERS     | Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin. |
| QUERY PROFILE          | Zeigt Informationen über Konfigurationsprofile an.                               |
| SET CONFIGMANAGER      | Gibt an, ob ein Server ein Konfigurationsmanager ist.                            |
| UNLOCK PROFILE         | Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server.         |
| UPDATE PROFILE         | Ändert die Beschreibung eines Profils.   |

## DELETE PROFILE (Profil löschen)

Mit diesem Befehl kann auf einem Konfigurationsmanager ein Profil gelöscht und seine Verteilung an verwaltete Server gestoppt werden.

Ein gesperrtes Profil kann nicht gelöscht werden. Das Profil muss zuerst mit dem Befehl UNLOCK PROFILE entsperrt werden.

Durch das Löschen eines Profils aus einem Konfigurationsmanager werden die diesem Profil zugeordneten Objekte nicht aus den verwalteten Servern gelöscht. Mit dem Befehl DELETE SUBSCRIPTION und dem Parameter DISCARDOBJECTS=YES können auf jedem subscribierenden verwalteten Server Subskriptionen für das Profil und die zugeordneten Objekte gelöscht werden. Auf diese Weise wird auch verhindert, dass die verwalteten Server weitere Aktualisierungen des Profils anfordern.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
..-Force-----No-----.  
>>-DELEte PROFILE--Profilname---+-----+----->>  
'-Force-----+No--+-'  
'-Yes-'
```

## Parameter

Profilname (Erforderlich)

Gibt das Profil an, das gelöscht werden soll.

Force

Gibt an, ob das Profil gelöscht wird, wenn ein oder mehrere verwaltete Server über Subskriptionen für das Profil verfügen. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, dass das Profil nicht gelöscht wird, wenn ein oder mehrere verwaltete Server über Subskriptionen für das Profil verfügen. Die Subskriptionen auf jedem verwalteten Server können mit dem Befehl DELETE SUBSCRIPTION gelöscht werden.

Yes

Gibt an, dass das Profil gelöscht wird, auch wenn ein oder mehrere verwaltete Server über Subskriptionen für das Profil verfügen. Alle subscribierenden Server fordern weiterhin Aktualisierungen für das gelöschte Profil an, bis die Subskription gelöscht wird.

## Beispiele: Ein Profil löschen

Das Profil BETA löschen, auch wenn Subskriptionen von verwalteten Servern vorhanden sind.

```
delete profile beta force=yes
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE PROFILE

| Befehl                 | Beschreibung  |
|------------------------|---|
| COPY PROFILE           | Erstellt eine Kopie eines Profils.  |
| DEFINE PROFASSOCIATION | Ordnet Objekte einem Profil zu.   |
| DEFINE PROFILE         | Definiert ein Profil für die Verteilung von Informationen an verwaltete Server. |
| DEFINE SUBSCRIPTION    | Subskribiert einen verwalteten Server für ein Profil.                           |
| DELETE PROFASSOCIATION | Löscht die Zuordnung zwischen einem Objekt und einem Profil.                    |
| DELETE SUBSCRIPTION    | Löscht eine angegebene Profilsubskription.                                      |
| LOCK PROFILE           | Verhindert die Verteilung eines Konfigurationsprofils.                          |
| QUERY PROFILE          | Zeigt Informationen über Konfigurationsprofile an.                              |
| QUERY SUBSCRIPTION     | Zeigt Informationen über Profilsubskriptionen an.                               |
| SET CONFIGMANAGER      | Gibt an, ob ein Server ein Konfigurationsmanager ist.                           |

| Befehl         | Beschreibung   |
|----------------|--|
| UNLOCK PROFILE | Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server. |
| UPDATE PROFILE | Ändert die Beschreibung eines Profils.                                   |

## DELETE RECMEDMACHASSOCIATION (Zuordnung Datenträger/Maschine löschen)

Mit diesem Befehl kann die Zuordnung von Maschinen zu einem Wiederherstellungsdatenträger aufgehoben werden. Dieser Befehl löscht nicht die Maschine aus IBM Spectrum Protect.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DELEte RECMEDMACHAssociation--Datenträgername----->
      .,-----
      v          |
>---Maschinennamen-----<<
```

### Parameter

Datenträgername (Erforderlich)

Gibt den Namen des Wiederherstellungsdatenträgers an, der einer oder mehreren Maschinen zugeordnet ist.

Maschinennamen (Erforderlich)

Gibt den Namen der Maschine an, die dem Wiederherstellungsdatenträger zugeordnet ist. Soll eine Liste mit Maschinennamen angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Ist eine Maschine nicht dem Wiederherstellungsdatenträger zugeordnet, wird die Maschine ignoriert.

### Beispiel: Die Zuordnung einer Maschine zu Wiederherstellungsdatenträgern löschen

Die Zuordnung zwischen dem Wiederherstellungsdatenträger DIST5RM und den Maschinen DISTRICT1 und DISTRICT5 löschen.

```
delete recmedmachassociation
dist5rm district1,district5
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE RECMEDMACHASSOCIATION

| Befehl                       | Beschreibung   |
|------------------------------|--|
| DEFINE RECMEDMACHASSOCIATION | Ordnet Wiederherstellungsdatenträger einer Maschine zu.                  |
| QUERY MACHINE                | Zeigt Informationen über Maschinen an.                                   |
| QUERY RECOVERYMEDIA          | Zeigt die für die Maschinenwiederherstellung verfügbaren Datenträger an. |

## DELETE RECOVERYMEDIA (Wiederherstellungsdatenträger löschen)

Mit diesem Befehl kann die Definition eines Wiederherstellungsdatenträgers aus IBM Spectrum Protect gelöscht werden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DElete RECOVERYMedia--Datenträgername-----><
```

## Parameter

Datenträgername (Erforderlich)  
Gibt den Namen des Wiederherstellungsdatenträgers an.

## Beispiel: Die Definition eines Wiederherstellungsdatenträgers löschen

Den Wiederherstellungsdatenträger DIST5RM löschen.

```
delete recoverymedia dist5rm
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE RECOVERYMEDIA

| Befehl               | Beschreibung   |
|----------------------|--|
| DEFINE RECOVERYMEDIA | Definiert die Datenträger, die für die Wiederherstellung einer Maschine erforderlich sind. |
| QUERY RECOVERYMEDIA  | Zeigt die für die Maschinenwiederherstellung verfügbaren Datenträger an.                   |
| UPDATE RECOVERYMEDIA | Ändert die Attribute von Wiederherstellungsdatenträgern.                                   |

## DELETE SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl löschen)

Mit diesem Befehl können Zeitpläne aus der Datenbank gelöscht werden.

Der Befehl DELETE SCHEDULE hat zwei Formen: eine Form, wenn der Zeitplan Clientoperationen betrifft, und eine Form, wenn der Zeitplan Verwaltungsbefehle betrifft. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für DELETE SCHEDULE

| Befehl          | Beschreibung  |
|-----------------|---|
| COPY SCHEDULE   | Erstellt eine Kopie eines Zeitplans.  |
| DEFINE SCHEDULE | Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl. |
| QUERY SCHEDULE  | Zeigt Informationen über Zeitpläne an.  |
| UPDATE SCHEDULE | Ändert die Attribute eines Zeitplans.   |

- DELETE SCHEDULE (Clientzeitplan löschen)  
Mit dem Befehl DELETE SCHEDULE können ein oder mehrere Clientzeitpläne aus der Datenbank gelöscht werden. Alle Clientzuordnungen zu einem Zeitplan werden beim Löschen des Zeitplans entfernt.
- DELETE SCHEDULE (Verwaltungszeitplan löschen)  
Mit diesem Befehl können ein oder mehrere Zeitpläne für Verwaltungsbefehle aus der Datenbank gelöscht werden.

## DELETE SCHEDULE (Clientzeitplan löschen)

Mit dem Befehl DELETE SCHEDULE können ein oder mehrere Clientzeitpläne aus der Datenbank gelöscht werden. Alle Clientzuordnungen zu einem Zeitplan werden beim Löschen des Zeitplans entfernt.

## Berechtigungsklasse

Zum Löschen eines Clientzeitplans ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die angegebene Maßnahmendomäne erforderlich.

## Syntax

```
>>-DElete SChedule--Domänennamen--Zeitplannamen----->
```

```
.-Type---Client-.
>+-----+-----><
```

## Parameter

---

Domänenname (Erforderlich)

Gibt den Namen der Maßnahmendomäne an, zu der der Zeitplan gehört.

Zeitplanname (Erforderlich)

Gibt den Namen des zu löschenden Zeitplans an. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.

Type=Client

Gibt an, dass ein Clientzeitplan gelöscht werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist CLIENT.

## Beispiel: Einen bestimmten Zeitplan aus einer bestimmten Maßnahmendomäne löschen

---

Den Zeitplan WEEKLY\_BACKUP löschen, der zu der Maßnahmendomäne EMPLOYEE\_RECORDS gehört.

```
delete schedule employee_records weekly_backup
```

## DELETE SCHEDULE (Verwaltungszeitplan löschen)

---

Mit diesem Befehl können ein oder mehrere Zeitpläne für Verwaltungsbefehle aus der Datenbank gelöscht werden.

## Berechtigungsklasse

---

Zum Löschen eines Zeitplans für Verwaltungsbefehle ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-DElete SCHEDULE--Zeitplanname--Type---Administrative-----><
```

## Parameter

---

Zeitplanname (Erforderlich)

Gibt den Namen des zu löschenden Zeitplans an. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.

Type=Administrative (Erforderlich)

Gibt an, dass ein Zeitplan für Verwaltungsbefehle gelöscht werden soll.

## Beispiel: Einen Zeitplan für Verwaltungsbefehle löschen

---

Den Zeitplan für Verwaltungsbefehle mit dem Namen DATA\_ENG löschen.

```
delete schedule data_eng type=administrative
```

## DELETE SCRATCHPADENTRY (Scratchpadeintrag löschen)

---

Mit diesem Befehl können Sie ein oder mehrere Zeilen mit Daten aus einem Scratchpad löschen.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-DElete SCRATCHPadentry--übergeordnete_Kategorie----->
                                     .-Line---*-----
>>--untergeordnete_Kategorie--Betreff--+-----+-----><
                                     '-Line ----Nummer-'
```

## Parameter

---

übergeordnete\_Kategorie (Erforderlich)

Gibt die übergeordnete Kategorie an, aus der eine oder mehrere Zeilen mit Daten gelöscht werden sollen. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

untergeordnete\_Kategorie (Erforderlich)

Gibt die untergeordnete Kategorie an, aus der eine oder mehrere Zeilen mit Daten gelöscht werden sollen. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

Betreff (Erforderlich)

Gibt den Betreff an, aus dem eine oder mehrere Zeilen mit Daten gelöscht werden sollen. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

Line

Gibt eine Zeile mit Daten an, die gelöscht werden soll. Geben Sie für Nummer die Nummer der Zeile ein, die gelöscht werden soll. Es werden alle Daten in der Zeile gelöscht. Die Nummerierung der anderen Zeilen im Betreffabschnitt ist davon nicht betroffen. Sie können alle Zeilen mit Daten aus einem Betreffabschnitt löschen, indem Sie den Parameter Line in diesem Befehl übergehen.

## Beispiel: Alle Zeilen mit Daten aus einem Betreff in einem Scratchpad löschen

---

Löschen Sie alle Zeilen mit Daten zum Standort eines Administrators, Jane, aus einer Datenbank, in der Informationen zu Administratoren gespeichert sind:

```
delete scratchpadentry admin_info location jane
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für DELETE SCRATCHPADENTRY

| Befehl                  | Beschreibung  |
|-------------------------|---|
| DEFINE SCRATCHPADENTRY  | Erstellt eine Zeile mit Daten im Scratchpad.                    |
| QUERY SCRATCHPADENTRY   | Zeigt Informationen an, die im Scratchpad enthalten sind.       |
| SET SCRATCHPADRETENTION | Gibt den Zeitraum an, den Scratchpadeinträge aufbewahrt werden. |
| UPDATE SCRATCHPADENTRY  | Aktualisiert Daten in einer Zeile im Scratchpad.                |

## DELETE SCRIPT (Befehlszeilen aus Prozedur oder gesamte Prozedur löschen)

---

Mit diesem Befehl kann eine einzelne Zeile aus einer IBM Spectrum Protect-Prozedur oder die vollständige IBM Spectrum Protect-Prozedur gelöscht werden.

## Berechtigungsklasse

---

Um diesen Befehl ausgeben zu können, muß der Administrator die Prozedur zuvor definiert oder die Systemberechtigung haben.

## Syntax

---

```
>>-DElete SCRipt--Prozedurname--+-+-----+-----><  
                                '-Line -==-Nummer-'
```

## Parameter

---

Prozedurname (Erforderlich)

Gibt den Namen der Prozedur an, die gelöscht werden soll. Die Prozedur wird gelöscht, es sei denn, es wird eine Zeilennummer angegeben.

Line

Gibt die Nummer der Zeile an, die aus der Prozedur gelöscht werden soll. Wird keine Zeilennummer angegeben, wird die vollständige Prozedur gelöscht.

## Beispiel: Eine bestimmte Zeile aus einem Script löschen

---

Das folgende Script mit dem Namen QSAMPLE wird verwendet und ein Befehl ausgegeben, um Zeile 005 aus dem Script zu löschen.

```
001 /* Dies ist eine Beispielprozedur */
005 QUERY STATUS
010 QUERY PROCESS

delete script qsample line=5
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE SCRIPT

| Befehl        | Beschreibung   |
|---------------|--|
| COPY SCRIPT   | Erstellt eine Kopie einer Prozedur.                          |
| DEFINE SCRIPT | Definiert eine Prozedur für den IBM Spectrum Protect-Server. |
| QUERY SCRIPT  | Zeigt Informationen über Prozeduren an.                      |
| RENAME SCRIPT | Vergibt einen neuen Namen für eine Prozedur.                 |
| RUN           | Führt ein Script aus.  |
| UPDATE SCRIPT | Ändert Zeilen oder fügt Zeilen in einer Prozedur hinzu.      |

## DELETE SERVER (Server-Definition löschen)

Mit diesem Befehl kann eine Server-Definition gelöscht werden.

Dieser Befehl schlägt fehl, wenn der Server

- als Ereignisserver definiert ist.
- in einer Einheitenklassendefinition mit dem Einheitentyp SERVER angegeben ist.
- eine offene Verbindung zu oder von einem anderen Server hat.
- ein Zielserver für virtuelle Datenträger ist.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-DELEte--SERver--Servername-----<<
```

## Parameter

Servername (Erforderlich)  
Gibt einen Server-Namen an.

## Beispiel: Die Definition eines Servers löschen

Die Definition für den Server SERVER2 löschen.

```
delete server server2
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE SERVER

| Befehl            | Beschreibung  |
|-------------------|---|
| DEFINE SERVER     | Definiert einen Server für die Übertragung zwischen Servern.  |
| QUERY EVENTSERVER | Zeigt den Namen des Ereignisserver an.  |
| QUERY SERVER      | Zeigt Informationen über Server an.   |
| RECONCILE VOLUMES | Stimmt Definitionen von virtuellen Datenträgern auf dem Quellenserver mit Archivierungsobjekten des Zielservers ab. |

| Befehl        | Beschreibung                                  |
|---------------|---|
| UPDATE SERVER | Aktualisiert Informationen über einen Server. |

## DELETE SERVERGROUP (Servergruppe löschen)

Mit diesem Befehl kann eine Server-Gruppe gelöscht werden. Ist die Gruppe, die gelöscht wird, ein Teil anderer Server-Gruppen, entfernt IBM Spectrum Protect die Gruppe auch aus den anderen Server-Gruppen.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DELeTe SERVERGroup--Gruppenname-----<<
```

### Parameter

Gruppenname (Erforderlich)  
Gibt die Server-Gruppe an, die gelöscht werden soll.

### Beispiel: Eine Servergruppe löschen

Die Server-Gruppe WEST\_COMPLEX löschen.

```
delete servergroup west_complex
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE SERVERGROUP

| Befehl             | Beschreibung  |
|--------------------|---|
| COPY SERVERGROUP   | Erstellt eine Kopie einer Servergruppe.             |
| DEFINE GRPMEMBER   | Definiert einen Server als Teil einer Servergruppe. |
| DEFINE SERVERGROUP | Definiert eine neue Servergruppe.                   |
| DELETE GRPMEMBER   | Löscht einen Server aus einer Servergruppe.         |
| MOVE GRPMEMBER     | Versetzt einen Teil einer Servergruppe.             |
| QUERY SERVERGROUP  | Zeigt Informationen über Servergruppen an.          |
| RENAME SERVERGROUP | Benennt eine Servergruppe um.                       |
| UPDATE SERVERGROUP | Aktualisiert eine Servergruppe.                     |

## DELETE SPACETRIGGER (Speicherbereichsauslöser für Speicherpool löschen)

Mit diesem Befehl kann die Definition des Speicherbereichsauslösers für den Speicherpool gelöscht werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-DELeTe SPACETriGger--STG--+-STGPOOL----Speicherpoolname-'<
```



## Parameter

---

STG

Gibt einen Speicherbereichsauslöser für den Speicherpool an.

STGPOOL

Gibt den Speicherpoolauslöser an, der gelöscht werden soll. Wird STG ohne STGPOOL angegeben, ist der standardmäßige Speicherbereichsauslöser für den Speicherpool das Lösziel.

## Beispiel: Die Definition eines Speicherbereichsauslösers löschen

---

Die Definition des Speicherbereichsauslösers für den Speicherpool WINPOOL1 löschen.

```
delete spacetrigger stg stgpool=winpool1
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für DELETE SPACETRIGGER

| Befehl              | Beschreibung  |
|---------------------|---|
| DEFINE SPACETRIGGER | Definiert einen Speicherbereichsauslöser zum Erweitern des Speicherbereichs für einen Speicherpool. |
| QUERY SPACETRIGGER  | Zeigt Informationen zu einem Speicherbereichsauslöser für den Speicherpool an.                      |
| UPDATE SPACETRIGGER | Ändert Attribute des Speicherbereichsauslösers für den Speicherpool.                                |

## DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)

---

Mit diesem Befehl können Sie einen vorhandenen Schwellenwert für die Statusüberwachung löschen.

Mit Statusüberwachungsschwellenwerten werden die definierten Bedingungen mit den Serverabfragen für die Statusüberwachung verglichen und die Ergebnisse in die Statusüberwachungstabelle eingefügt.

Es können mehrere Schwellenwerte für eine Aktivität definiert werden. Sie können beispielsweise einen Schwellenwert erstellen, der einen Warnstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 80 % ist. Sie können dann einen anderen Schwellenwert erstellen, der einen Fehlerstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 90 % ist.

Anmerkung: Wenn bereits ein Schwellenwert für eine Bedingung EXISTS definiert ist, können Sie keinen anderen Schwellenwert mit einem der anderen Bedingungsstypen definieren.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-DElEte STATusthreshold--Schwellenwertname-----<<
```

## Parameter

---

Schwellenwertname (Erforderlich)

Gibt den Schwellenwertnamen an, der gelöscht werden soll.

## Einen vorhandenen Statusschwellenwert löschen

---

Mit dem folgenden Befehl einen vorhandenen Statusschwellenwert löschen:

```
delete statusthreshold avgstgpl
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für DELETE STATUSTHRESHOLD

| Befehl   | Beschreibung   |
|--|--|
| DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)  | Definiert einen Schwellenwert für die Statusüberwachung.   |
| QUERY MONITORSTATUS (Überwachungsstatus abfragen)  | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an. |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen) | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an. |
| QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)  | Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.                             |
| SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)  | Gibt an, ob die Statusüberwachung aktiviert werden soll.   |
| SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)                            | Gibt das Aktualisierungsintervall für die Statusüberwachung an.                                  |
| UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)                                       | Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.                 |

## DELETE STGPOOL (Speicherpool löschen)

Mit diesem Befehl kann ein Speicherpool gelöscht werden. Um einen Speicherpool zu löschen, müssen zuerst alle Datenträger gelöscht werden, die dem Speicherpool zugeordnet sind.

Ein Speicherpool, der als nächster Speicherpool für einen anderen Speicherpool angegeben ist, kann nicht gelöscht werden. Weitere Informationen zur Speicherpoolhierarchie befinden sich unter dem Parameter NEXTSTGPOOL im Befehl DEFINE STGPOOL.

Einschränkungen:

- Löschen Sie für Containerspeicherpools alle Speicherpoolverzeichnisse, bevor Sie den Speicherpool löschen.
- Es darf kein Speicherpool gelöscht werden, der als Zielort für eine Verwaltungsklasse oder eine Kopiengruppe in der aktiven Maßnahmengruppe angegeben ist. Client-Operationen könnten fehlschlagen.
- Wird ein Kopierspeicherpool gelöscht, der zuvor in der Definition eines primären Speicherpools enthalten war (speziell in der COPYSTGPOOLS-Liste), müssen Sie den Kopierspeicherpool vor dem Löschen aus der Liste entfernen. Andernfalls schlägt der Befehl DELETE STGPOOL fehl, bis alle Verweise auf diesen Kopienpool entfernt werden. Entfernen Sie für jeden primären Speicherpool mit einem Verweis auf den zu löschenden Kopierspeicherpool den Verweis, indem Sie den Befehl UPDATE STGPOOL mit dem Parameter COPYSTGPOOLS mit allen vorherigen Kopierspeicherpools außer dem zu löschenden Kopierspeicherpool eingeben.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-DElete STGpool--Poolname-----><
```

## Parameter

Poolname (Erforderlich)  
Gibt den Speicherpool an, der gelöscht werden soll.





## Beispiel: Einen Speicherpool löschen

Den Speicherpool POOLA löschen.

```
delete stgpool poola
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE STGPOOL

| Befehl   | Beschreibung   |
|--|--|
| BACKUP STGPOOL   | Sichert einen primären Speicherpool in einem Kopierspeicherpool.   |
| DEFINE STGPOOL   | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.   |
| DEFINE STGPOOLDIRECTORY  | Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool.  |
| DELETE STGPOOLDIRECTORY  | Löscht ein Speicherpoolverzeichnis aus einem Verzeichniscontainer- oder Cloud-Containerspeicherpool.   |
| QUERY STGPOOL  | Zeigt Informationen zu Speicherpools an.   |
| QUERY STGPOOLDIRECTORY   | Zeigt Informationen zu Speicherpoolverzeichnissen an.  |
|   SET DRMCOPYSTGPOOL |   Gibt an, dass Kopierspeicherpools von DRM verwaltet werden. |
| UPDATE STGPOOL   | Ändert die Attribute eines Speicherpools.  |
| UPDATE STGPOOLDIRECTORY  | Ändert die Attribute eines Speicherpoolverzeichnisses.   |

## DELETE STGPOOLDIRECTORY (Speicherpoolverzeichnis löschen)

Mit diesem Befehl kann eine Definition für ein Speicherpoolverzeichnis gelöscht werden.

Möglicherweise möchten Sie ein Speicherpoolverzeichnis aus den folgenden Gründen löschen:

- Alter Speicher soll stillgelegt werden.
- Die lokale Platte soll nicht weiterverwendet werden, bevor Daten in die Cloud versetzt werden.
- Es besteht kein Bedarf mehr, die Daten in dem Speicherpoolverzeichnis aufzubewahren.

Einschränkungen:

- Sie können diesen Befehl nur ausgeben, wenn keine Container dem Speicherpoolverzeichnis zugeordnet sind. Geben Sie den Befehl QUERY CONTAINER aus, um zu bestimmen, ob dem Speicherpoolverzeichnis Container zugeordnet sind.
- Sollen Container aus einem Speicherpoolverzeichnis entfernt werden, müssen Sie den Befehl UPDATE STGPOOLDIRECTORY ausgeben und den Parameter ACCESS=DESTROYED angeben. Geben Sie dann den Befehl AUDIT CONTAINER aus und geben Sie den Parameter ACTION=REMOVEDAMAGED an. Überprüfen Sie, ob die Container entfernt wurden. Der Parameter ACTION=REMOVEDAMAGED entfernt die Informationen zum Bestand für die Objekte, die gesichert oder archiviert wurden. Sie sollten die Informationen zum Bestand nur dann entfernen, wenn Sie die Sicherungen nicht benötigen.

Falls ein Hardwarefehler oder ein Verlust des Verzeichnisses auftritt, finden Sie weitere Informationen in den Abschnitten über die Befehle AUDIT und REPAIR. Etwaige Reparaturen an der IBM Spectrum Protect-Umgebung sollten Sie vornehmen, bevor Sie das Speicherpoolverzeichnis löschen.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DELeTe STGPOOLDIRectory--Poolname--Verzeichnis-----<<
```

### Parameter

Poolname (Erforderlich)

Gibt den Speicherpool an, der das zu löschende Verzeichnis enthält. Dieser Parameter ist erforderlich.

Verzeichnis (Erforderlich)

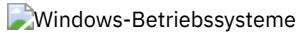
Gibt das zu löschende Dateisystemverzeichnis des Speicherpools an. Dieser Parameter ist erforderlich.

### Beispiel: Ein Speicherpoolverzeichnis aktualisieren, um es zum Löschen vorzubereiten

Das Speicherpoolverzeichnis mit dem Namen DIR1 im Speicherpool POOLA aktualisieren, um es als dauerhaft beschädigt zu markieren. Wenn ein Speicherpool als dauerhaft beschädigt markiert ist, kann er gelöscht werden.

```
update stgpooldirectory poola /storage/dir1 access=destroyed
```



```
update stgpooldirectory poola e:\storage\dir1 access=destroyed
```

## Beispiel: Ein Speicherpoolverzeichnis löschen

Das Speicherpoolverzeichnis mit dem Namen DIR1 im Speicherpool POOLA löschen.

```
delete stgpooldirectory poola /storage/dir1
```



```
delete stgpooldirectory poola e:\storage\dir1
```

Tabelle 1. Zugehörige Befehle für DELETE STGPOOLDIRECTORY

| Befehl                  | Beschreibung  |
|-------------------------|---|
| DEFINE STGPOOL          | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.                      |
| DEFINE STGPOOLDIRECTORY | Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool. |
| QUERY STGPOOLDIRECTORY  | Zeigt Informationen zu Speicherpoolverzeichnissen an.   |
| UPDATE STGPOOLDIRECTORY | Ändert die Attribute eines Speicherpoolverzeichnisses.  |
| QUERY EXTENTUPDATES     | Zeigt Informationen zu Aktualisierungen an Datenbereichen in Verzeichniscontainerspeicherpools an.      |

## DELETE STGRULE (Speicherregeln für Speicherpools löschen)

Verwenden Sie diesen Befehl, um Speicherregeln für einen oder mehrere Speicherpools zu löschen.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DELeTe STGRULE--Regelname-----><
```

### Parameter

Regelname (Erforderlich)

Gibt den Namen der Speicherregel an, die gelöscht werden muss. Die maximale Länge des Namens beträgt 30 Zeichen.

### Speicherregel löschen

Eine Speicherregel mit dem Namen stgrule1 löschen:

```
delete stgrule stgrule1
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE STGRULE

| Befehl | Beschreibung |
|--------|--------------|
|--------|--------------|

| Befehl         | Beschreibung                                       |
|----------------|--|
| DEFINE STGRULE | Definiert eine Speicherregel für Speicherpools.    |
| QUERY STGRULE  | Zeigt Informationen zu Speicherregeln an.          |
| UPDATE STGRULE | Aktualisiert eine Speicherregel für Speicherpools. |

## DELETE SUBSCRIBER (Subskriptionen aus Konfigurationsmanagerdatenbank löschen)

Verwenden Sie diesen Befehl auf einem Konfigurationsmanager, um Subskriptionen für einen verwalteten Server aus der Datenbank des Konfigurationsmanagers zu löschen. Verwenden Sie diesen Befehl, wenn ein verwalteter Server nicht mehr vorhanden ist oder den Konfigurationsmanager nach dem Löschen einer Subskription nicht informieren kann.

Achtung: Diesen Befehl nur in seltenen Fällen verwenden, in denen die Datenbank des Konfigurationsmanagers einen Eintrag für eine Subskription enthält, der verwaltete Server aber nicht über eine solche Subskription verfügt. Diesen Befehl beispielsweise verwenden, wenn ein verwalteter Server nicht mehr vorhanden ist oder den Konfigurationsmanager nach dem Löschen einer Subskription nicht informieren kann.

Unter normalen Umständen den Befehl DELETE SUBSCRIPTION verwenden, um eine Subskription auf dem verwalteten Server zu löschen. Der verwaltete Server informiert den Konfigurationsmanager, der dann die Subskription aus seiner Datenbank löscht.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DELEte SUBSCRIBer--Servername-----><
```

### Parameter

Servername (Erforderlich)

Gibt den Namen des verwalteten Servers an, dessen Subskriptionseinträge gelöscht werden sollen.

### Beispiel: Subskriptionseinträge für einen bestimmten verwalteten Server löschen

Alle Subskriptionseinträge für den verwalteten Server DAN löschen.

```
delete subscriber dan
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE SUBSCRIBER

| Befehl              | Beschreibung   |
|---------------------|--|
| DEFINE SUBSCRIPTION | Subskribiert einen verwalteten Server für ein Profil.                            |
| DELETE SUBSCRIPTION | Löscht eine angegebene Profilsubskription.                                       |
| NOTIFY SUBSCRIBERS  | Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin. |
| QUERY SUBSCRIBER    | Zeigt Informationen über Subskribenten und ihre Subskriptionen für Profile an.   |
| QUERY SUBSCRIPTION  | Zeigt Informationen über Profilsubskriptionen an.                                |

## DELETE SUBSCRIPTION (Profilsubskription löschen)

Mit diesem Befehl kann auf einem verwalteten Server eine Profilsubskription gelöscht werden. Außerdem können auf dem verwalteten Server alle Objekte gelöscht werden, die dem Profil zugeordnet sind.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-DELEte SUBSCRIPtion--Profilname----->
. -DISCARDobjects----No-----
>--+-----+-----><
' -DISCARDobjects----+No--+-'
      '-Yes-'
```

## Parameter

Profilname (Erforderlich)

Gibt den Namen des Profils an, für das die Subskription gelöscht werden soll.

DISCARDobjects

Gibt an, ob Objekte, die dem Profil zugeordnet sind, auf dem verwalteten Server gelöscht werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

No

Gibt an, daß die Objekte nicht gelöscht werden sollen.

Yes

Gibt an, daß die Objekte gelöscht werden sollen, es sei denn, sie sind einem anderen Profil zugeordnet, für das eine Subskription definiert ist.

## Beispiel: Eine Profilsubskription löschen

Eine Subskription für das Profil ALPHA und seine zugeordneten Objekte aus einem verwalteten Server löschen.

```
delete subscription alpha discardobjects=yes
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE SUBSCRIPTION

| Befehl              | Beschreibung   |
|---------------------|--|
| DEFINE SUBSCRIPTION | Subskribiert einen verwalteten Server für ein Profil.                            |
| DELETE SUBSCRIBER   | Löscht veraltete Subskriptionen verwalteter Server.                              |
| NOTIFY SUBSCRIBERS  | Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin. |
| QUERY SUBSCRIBER    | Zeigt Informationen über Subskribenten und ihre Subskriptionen für Profile an.   |
| QUERY SUBSCRIPTION  | Zeigt Informationen über Profilsubskriptionen an.                                |

## DELETE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs löschen)

Verwenden Sie diesen Befehl, um eine Definition für die Zuordnung des virtuellen Dateibereichs zu löschen. Virtuelle Dateibereiche, die Daten enthalten, können nur gelöscht werden, wenn zuerst der Befehl DELETE FILESPACE verwendet wird.

## Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Systemberechtigung
- Uneingeschränkte Maßnahmenberechtigung
- Eingeschränkte Maßnahmenberechtigung für die Domäne, der der NAS-Knoten zugeordnet ist

## Syntax

```
>>-DElete VIRTUALFSmapping -Knotenname----->  
>--Name_des_virtuellen_Dateibereichs----->>
```

## Parameter

Knotenname (Erforderlich)

Gibt den NAS-Knoten an, auf dem sich das Dateisystem und der Pfad befinden. Sie können keine Platzhalterzeichen verwenden und keine Liste mit Namen angeben.

Name\_des\_virtuellen\_Dateibereichs (Erforderlich)

Gibt den Namen der zu löschenden Definition für die Zuordnung des virtuellen Dateibereichs an. Platzhalterzeichen sind zulässig.

## Beispiel: Eine Zuordnung des virtuellen Dateibereichs löschen

Die Definition /mikeshomdir für die Zuordnung des virtuellen Dateibereichs für den NAS-Knoten NAS1 löschen.

```
delete virtualfsmapping nas1 /mikeshomdir
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE VIRTUALFSMAPPING

| Befehl                  | Beschreibung  |
|-------------------------|---|
| DEFINE VIRTUALFSMAPPING | Zuordnung eines virtuellen Dateibereichs definieren.    |
| QUERY VIRTUALFSMAPPING  | Zuordnung eines virtuellen Dateibereichs abfragen.      |
| UPDATE VIRTUALFSMAPPING | Zuordnung eines virtuellen Dateibereichs aktualisieren. |

## DELETE VOLHISTORY (Protokolldaten sequenzieller Datenträger löschen)

Mit diesem Befehl können Sätze in der Protokolldatei für Datenträger gelöscht werden, die nicht mehr benötigt werden (beispielsweise Sätze für veraltete Datenbanksicherungsdatenträger).

Werden Sätze für Datenträger gelöscht, die sich nicht in Speicherpools befinden (beispielsweise Datenbanksicherungs- oder Exportdatenträger), werden die Datenträger auch dann in den Arbeitsdatenträgerstatus zurückversetzt, wenn IBM Spectrum Protect die Datenträger als private Datenträger angefordert hat. Arbeitsdatenträger mit dem Einheitentyp FILE werden gelöscht. Werden die Sätze für Speicherpooldatenträger gelöscht, verbleiben die Datenträger in der IBM Spectrum Protect-Datenbank. Werden Sätze für Wiederherstellungsplandateiobjekte aus einem Quellenserver gelöscht, werden die Objekte auf dem Zielsystem zum Löschen markiert. Einschränkung: Verwenden Sie nicht den Befehl DELETE VOLHISTORY, um Informationen zu Sicherungsgruppendatenträgern aus der Protokolldatei für Datenträger zu löschen. Verwenden Sie zu diesem Zweck den Befehl DELETE BACKUPSET.

Benutzer von DRM müssen sicherstellen, dass der Verfall von Datenbanksicherungen über den Befehl SET DRMDBBACKUPEXPIREDAYS und nicht über diesen Befehl DELETE VOLHISTORY gesteuert wird. Verwenden Sie den Befehl DELETE VOLHISTORY, um einen Satz des Datenträgers zu entfernen. Dadurch können Datenträger verloren gehen, die über den Befehl MOVE DRMEDIA verwaltet wurden. Verwenden Sie den Befehl SET DRMDBBACKUPEXPIREDAYS, um den automatischen Verfall von DRM-Datenbanksicherungsdatenträgern zu verwalten.

Tipps:

- Datenträger für die neueste Datenbanksicherungsserie werden nicht gelöscht.
- Vorhandene Protokolldateien für Datenträger werden mit diesem Befehl nicht automatisch aktualisiert.
- Mit dem Befehl DEFINE SCHEDULE können Datenträgerprotokollsätze in regelmäßigen Abständen gelöscht werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-DElete VOLHistory--TODate----Datum----->
```

```

.-TOTime-----23:59:59-.
>-----+----->
'-TOTime-----Zeit-----'

>--Type-----+All-----+-----><
+-DBBackup-----+-----+-----+-----+-----+
|           '-DEVclass-----Klassenname-' |
+-DBSnapshot-----+-----+-----+-----+-----+
|           '-DEVclass-----Klassenname-' |
+-DBRpf-----+-----+-----+-----+-----+
+-EXPort-----+-----+-----+-----+-----+
|           .-DELETELatest-----No-----.|
+-RPFfile-----+-----+-----+-----+-----+
|           '-DELETELatest-----+No--+-' |
|           '-Yes-' |
|           .-DELETELatest-----No-----.|
+-RPFsSnapshot-----+-----+-----+-----+-----+
|           '-DELETELatest-----+No--+-' |
|           '-Yes-' |
+-STGNew-----+-----+-----+-----+-----+
+-STGReuse-----+-----+-----+-----+-----+
+-STGDelete-----+-----+-----+-----+-----+

```

## Parameter

### TODate (Erforderlich)

Gibt das Datum an, das für die Auswahl der Protokolldaten sequenzieller Datenträger, die gelöscht sollen, verwendet werden soll. Sie können nur die Sätze mit einem Datum bis zu dem angegebenen Datum einschließlich löschen. Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 01/23/1999   |
| TODAY                          | Das aktuelle Datum   | TODAY  |
| TODAY-Tage oder -Tage          | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY-30 oder -30.<br>Um Sätze zu löschen, die mindestens 30 Tage alt sind, kann TODAY-30 oder einfach -30 angegeben werden. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.                               |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.                                    |

### TOTime

Gibt an, dass Sätze gelöscht werden sollen, die zu oder vor dieser Zeit am angegebenen Datum erstellt wurden. Dieser Parameter ist wahlfrei. Der Standardwert ist das Ende des Tages (23:59:59). Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert     | Beschreibung                                | Beispiel |
|----------|---|----------|
| HH:MM:SS | Eine bestimmte Uhrzeit am angegebenen Datum | 12:30:22 |
| NOW      | Die aktuelle Uhrzeit am angegebenen Datum   | NOW      |



| Wert                  | Beschreibung  | Beispiel  |
|-----------------------|---|---|
| NOW+HH:MM oder +HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Datum  | NOW+03:00 oder +03:00.<br><br>Wird der Befehl DELETE VOLHISTORY um 9:00 Uhr mit TOTIME=NOW+03:00 oder TOTIME=+03:00 ausgegeben, löscht IBM Spectrum Protect Sätze mit der Uhrzeit 12:00 Uhr oder früher an dem angegebenen Datum. |
| NOW-HH:MM oder -HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Datum | NOW-03:30 oder -03:30.<br><br>Wird der Befehl DELETE VOLHISTORY um 9:00 Uhr mit TOTIME=NOW-3:30 oder TOTIME=-3:30 ausgegeben, löscht IBM Spectrum Protect Sätze mit der Uhrzeit 5:30 Uhr oder früher an dem angegebenen Datum.    |

#### Type (Erforderlich)

Gibt den Typ der Sätze an (die auch den Datums- und Zeitkriterien entsprechen), die aus der Protokolldatei für Datenträger gelöscht werden sollen. Gültige Werte:

#### All

Gibt an, dass alle Sätze gelöscht werden sollen.

Einschränkung: Mit dem Befehl DELETE VOLHISTORY werden keine Sätze von fernen Datenträgern gelöscht.

#### DBBackup

Gibt an, dass nur Sätze gelöscht werden, die Informationen zu Datenträgern enthalten, die für Gesamt- und Teilsicherungen der Datenbank verwendet werden, d. h. Datenträger mit den Datenträgertypen BACKUPFULL und BACKUPINCR, und die die angegebenen Datums- und Zeitkriterien erfüllen. Die Sätze aus der letzten Gesamt- und Teilsicherungsserie der Datenbank werden nicht gelöscht.

#### DEVclass=Klassenname

Gibt den Namen der Einheitenklasse an, die zum Erstellen der Datenbanksicherungen verwendet wurde. Dieser wahlfreie Parameter kann verwendet werden, um Datenbanksicherungen zu löschen, die mithilfe einer Einheitenklasse für virtuelle Datenträger für die Übertragung zwischen Servern erstellt werden. Der Typ der Einheitenklasse muss SERVER lauten. Mit diesem Parameter können nur Datenträgerprotokolleinträge des Typs BACKUPFULL, BACKUPINCR oder DBSNAPSHOT gelöscht werden.

Ein Datenträger für Gesamt- oder Teilsicherungen der Datenbank kann zum Löschen ausgewählt werden, wenn alle folgenden Bedingungen zutreffen:

- Die Einheitenklasse, die zum Erstellen des Datenbanksicherungsdatenträgers verwendet wurde, stimmt mit der angegebenen Einheitenklasse überein.
- Der Datenträger wurde an oder vor dem angegebenen Datum und zu oder vor der angegebenen Uhrzeit erstellt.
- Der Datenträger ist nicht Teil der letzten Gesamt- und Teilsicherungsserie der Datenbank.
- Der Datenträger ist nicht Teil einer Gesamt- und Teilsicherungsserie mit einer Datenbankteilsicherung, die nach dem angegebenen Datum und nach der angegebenen Zeit erstellt wurde.

#### DBSnapshot

Gibt an, dass nur Sätze gelöscht werden, die Informationen zu Datenträgern enthalten, die für Datenbankmomentaufnahmesicherungen verwendet werden und die die angegebenen Datums- und Zeitkriterien erfüllen. Sätze, die sich auf die letzte Datenbankmomentaufnahmesicherung beziehen, werden nicht gelöscht.

#### DEVclass=Klassenname

Gibt den Namen der Einheitenklasse an, die zum Erstellen der Datenbanksicherungen verwendet wurde. Dieser wahlfreie Parameter kann verwendet werden, um Datenbanksicherungen zu löschen, die mithilfe einer Einheitenklasse für virtuelle Datenträger für die Übertragung zwischen Servern erstellt werden. Der Typ der Einheitenklasse muss SERVER lauten. Mit diesem Parameter können nur Datenträgerprotokolleinträge des Typs BACKUPFULL, BACKUPINCR oder DBSNAPSHOT gelöscht werden.

Ein Datenträger für Datenbankmomentaufnahmesicherungen kann zum Löschen ausgewählt werden, wenn alle folgenden Bedingungen zutreffen:

- Die Einheitenklasse, die zum Erstellen des Datenbanksicherungsdatenträgers verwendet wird, stimmt mit der angegebenen Einheitenklasse überein
- Der Datenträger wurde an oder vor dem angegebenen Datum und zu oder vor der angegebenen Uhrzeit erstellt
- Der Datenträger ist nicht Teil der letzten Datenbankmomentaufnahmesicherungsserie

#### DBRpf

Gibt an, dass nur Sätze gelöscht werden, die Informationen über Datenträger mit Gesamt- und Teilsicherungen der Datenbank und über Datenträger mit Wiederherstellungsplandateien enthalten.

#### EXPort

Gibt an, dass nur Sätze gelöscht werden, die Informationen über Exportdatenträger enthalten.

#### RPFfile

Gibt an, dass nur Sätze gelöscht werden, die Informationen über Wiederherstellungsplandateiobjekte enthalten, die auf einem Zielsever gespeichert sind, und die die angegebenen Datums- und Zeitkriterien erfüllen.

#### DELETEDatest

Gibt an, ob die letzte Wiederherstellungsplandatei zum Löschen ausgewählt werden kann. Dieser wahlfreie Parameter kann verwendet werden, um die letzten Wiederherstellungsplandateien zu löschen, die mithilfe einer Einheitenklasse für virtuelle Datenträger für die Übertragung zwischen Servern erstellt wurden.

Mit diesem Parameter können nur Datenträgerprotokolleinträge des Typs RPFfile gelöscht werden (beispielsweise die Wiederherstellungsplandateien, die mit dem Parameter DEVCLASS im Befehl PREPARE erstellt wurden). Wird dieser Parameter nicht angegeben, werden die letzten RPFfile-Einträge nicht gelöscht.

#### No

Gibt an, dass die letzte RPFfile-Datei nicht gelöscht wird.

#### Yes

Gibt an, dass die letzte RPFfile-Datei gelöscht wird, wenn sie den angegebenen Datums- und Zeitkriterien entspricht.

#### RPFSnapshot

Gibt an, dass nur Sätze gelöscht werden, die Informationen zu Wiederherstellungsplandateiobjekten enthalten, die für Datenbankmomentaufnahmesicherungen erstellt wurden, die auf einem Zielsever gespeichert sind und die die angegebenen Datums- und Zeitkriterien erfüllen. Die letzte RPFSnapshot-Datei wird nicht gelöscht, es sei denn, sie erfüllt die angegebenen Datums- und Zeitkriterien und der Parameter DELETE ist auf Yes gesetzt.

#### DELETEDatest

Gibt an, ob die letzte Wiederherstellungsplandatei zum Löschen ausgewählt werden kann. Dieser wahlfreie Parameter kann verwendet werden, um die letzten Wiederherstellungsplandateien zu löschen, die mithilfe einer Einheitenklasse für virtuelle Datenträger für die Übertragung zwischen Servern erstellt wurden.

Mit diesem Parameter können nur Datenträgerprotokolleinträge des Typs RPFSnapshot gelöscht werden (beispielsweise die Wiederherstellungsplandateien, die mit dem Parameter DEVCLASS im Befehl PREPARE erstellt wurden). Wird dieser Parameter nicht angegeben, werden die letzten RPFSnapshot-Einträge nicht gelöscht.

#### No

Gibt an, dass die letzte RPFSnapshot-Datei nicht gelöscht wird.

#### Yes

Gibt an, dass die letzte RPFSnapshot-Datei gelöscht wird, wenn sie den angegebenen Datums- und Zeitkriterien entspricht.

#### STGNew

Gibt an, dass nur Sätze gelöscht werden, die Informationen über neue Speicherdatenträger mit sequenziellem Zugriff enthalten.

#### STGReuse

Gibt an, dass nur Sätze gelöscht werden, die Informationen über wiederverwendete sequenzielle Datenträger aus dem Speicherpool enthalten.

#### STGDelete

Gibt an, dass nur Sätze gelöscht werden, die Informationen über gelöschte sequenzielle Datenträger aus dem Speicherpool enthalten.

## Beispiel: Informationen zur Wiederherstellungsplandatei löschen

Alle Informationen zu Wiederherstellungsplandateien löschen, die am oder vor dem 03/28/2016 erstellt wurden.

```
delete volhistory type=rpfile todate=03/28/2016
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE VOLHISTORY

| Befehl            | Beschreibung  |
|-------------------|---|
| BACKUP VOLHISTORY | Zeichnet Datenträger-History-Daten in externen Dateien auf. |

| Befehl                    | Beschreibung   |
|---------------------------|--|
| DEFINE SCHEDULE           | Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl.    |
| DELETE VOLUME             | Löscht einen Datenträger aus einem Speicherpool.                                   |
| EXPIRE INVENTORY          | Startet die Verfallsverarbeitung für den Datenträgerbestandsverfall manuell.       |
| MOVE DRMEDIA              | Versetzt DRM-Datenträger vor Ort und lagert sie aus.                               |
| PREPARE                   | Erstellt eine Wiederherstellungsplandatei.   |
| QUERY RPFFILE             | Zeigt Informationen über Wiederherstellungsplandateien an.                         |
| QUERY VOLHISTORY          | Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden. |
| SET DRMRPFEXPIREDAYS      | Definiert Verfallskriterien für Wiederherstellungsplandateien.                     |
| SET DRMDBBACKUPEXPIREDAYS | Gibt die Kriterien für den Verfall von Datenbanksicherungsserien an.               |

## DELETE VOLUME (Speicherpoolatenträger löschen)

Mit diesem Befehl können ein Datenträger aus dem Speicherpool und wahlweise die Dateien in dem Datenträger gelöscht werden.

Enthält der Datenträger Daten, muß einer der folgenden Schritte ausgeführt werden, um den Datenträger zu löschen:

- Vor dem Löschen des Datenträgers den Befehl MOVE DATA verwenden, um alle Dateien auf einen anderen Datenträger zu versetzen.
- Das Löschen aller Dateien auf dem Datenträger explizit anfordern, wenn der Datenträger gelöscht wird (durch Angabe von DISCARDDATA=YES).

Werden mehrere Datenträger gelöscht, die Datenträger einzeln löschen. Werden mehrere Datenträger gleichzeitig gelöscht, kann dies negative Auswirkungen auf die Server-Leistung haben.

Speicherpoolatenträger können nicht gelöscht werden, wenn sie gerade verwendet werden. Ein Datenträger kann beispielsweise nicht gelöscht werden, wenn ein Benutzer eine Datei zurückschreibt oder abrufen, die sich auf dem Datenträger befindet, wenn der Server Informationen auf den Datenträger schreibt oder wenn ein Wiederherstellungsprozess den Datenträger verwendet.

Wenn Sie den Befehl DELETE VOLUME ausgeben, werden Datenträgerinformationen aus der IBM Spectrum Protect-Datenbank gelöscht. Die physischen Dateien, die mit dem Befehl DEFINE VOLUME zugeordnet wurden, werden jedoch nicht aus dem Dateibereich entfernt.

Wird dieser Befehl auf einen WORM-Datenträger (WORM = Write Once, Read Many) angewendet, kehrt der Datenträger in den Arbeitsdatenträgerstatus zurück, wenn er noch über Speicherbereich verfügt, in den Daten geschrieben werden können. Daten auf WORM-Datenträgern, einschließlich gelöschter und verfallener Daten, können nicht überschrieben werden. Daher können Daten nur in Speicherbereich geschrieben werden, der keine aktuellen, gelöschten oder verfallenen Daten enthält. Verfügt ein WORM-Datenträger über keinen Speicherbereich mehr, in den Daten geschrieben werden können, verbleibt der Datenträger im privaten Status. Soll der Datenträger aus dem Kassettenarchiv entfernt werden, müssen Sie den Befehl CHECKOUT LIBVOLUME verwenden.

Mit dem Befehl DELETE VOLUME wird der Datenträgerbestand im Kassettenarchiv des Servers automatisch für sequenzielle Datenträger aktualisiert, wenn der Datenträger in den Status "Arbeitsdatenträger" zurückgesetzt wird, sobald der Datenträger leer wird. Um zu bestimmen, ob ein Datenträger in den Status "Arbeitsdatenträger" zurückgesetzt wird, geben Sie den Befehl QUERY VOLUME aus und überprüfen Sie die Ausgabe. Wenn der Wert für das Attribut "Arbeitsdatenträger?" "Yes" lautet, wird der Datenträgerbestand im Kassettenarchiv des Servers automatisch aktualisiert.

Lautet der Wert "No", können Sie mit dem Befehl UPDATE LIBVOLUME den Status als Arbeitsdatenträger angeben. Es wird empfohlen, den Befehl UPDATE LIBVOLUME auszugeben, nachdem der Befehl DELETE VOLUME ausgegeben wurde.

Der Versuch, den Befehl DELETE VOLUME zum Löschen von WORM-FILE-Datenträgern in einem Speicherpool mit RECLAMATIONTYPE=SNAPLOCK zu verwenden, schlägt mit einer Fehlermeldung fehl. Das Löschen von leeren WORM-FILE-Datenträgern wird nur durch den Wiederherstellungsprozess ausgeführt.

Wenn Sie den Befehl DELETE VOLUME für einen Datenträger in einem Speicherpool ausgeben, der einen Wert größer als 0 für den Parameter SHRED hat, wird der Datenträger bis zur Ausführung des Schredderns in den Wartestatus versetzt. Das Schreddern ist erforderlich, um das Löschen abzuschließen, auch wenn der Datenträger leer ist.

Wenn Sie den Befehl DELETE VOLUME für einen Datenträger in einem Speicherpool ausgeben, der für die Deduplizierung von Daten definiert ist, löscht der Server alle Objekte, die auf Daten auf diesem Datenträger verweisen.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool erforderlich, in dem der Datenträger definiert ist.

## Syntax

---

```
>>-DELEte Volume--Datenträgername----->
. -DISCARDdata-----No----- . -Wait-----No-----
>--+-----+-----+-----+-----+-----+-----+-----+-----+-----><
' -DISCARDdata-----+No--+-' ' -Wait-----+No--+-'
      '-Yes-'                '-Yes-'
```

## Parameter

---

### Datenträgername (Erforderlich)

Gibt den Namen des Datenträgers an, der gelöscht werden soll.

### DISCARDdata

Gibt an, ob die auf dem Datenträger gespeicherten Dateien gelöscht werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

#### No

Gibt an, daß die auf dem Datenträger gespeicherten Dateien nicht gelöscht werden. Enthält der Datenträger Dateien, wird der Datenträger nicht gelöscht.

#### Yes

Gibt an, daß alle auf dem Datenträger gespeicherten Dateien gelöscht werden. Der Server muß den Datenträger für diese Art des Löschens nicht laden.

Hinweis:

1. Der Server löscht keine Archivierungsdateien, für die angegeben wurde, dass sie nicht gelöscht werden dürfen.
2. Ist der Aufbewahrungsschutz für Archivierung aktiviert, löscht der Server nur Archivierungsdateien, deren Aufbewahrungszeitraum abgelaufen ist.

Ist der Datenträger, der gelöscht wird, ein Datenträger für den primären Speicherpool, überprüft der Server, ob ein Kopierspeicherpool Kopien von Dateien enthält, die gelöscht werden. Werden Dateien gelöscht, die auf einem Datenträger für den primären Speicherpool gespeichert sind, werden alle Kopien dieser Dateien in Kopierspeicherpools ebenfalls gelöscht.

Wird ein Plattendatenträger in einem primären Speicherpool gelöscht, löscht der Befehl auch alle Dateien, die Cache-Kopien sind (Kopien von Dateien, die in den nächsten Speicherpool umgelagert wurden). Beim Löschen der Cache-Kopien von Dateien werden nicht die Dateien gelöscht, die bereits in Kopierspeicherpools umgelagert oder gesichert wurden. Es sind nur die Cache-Kopien der Dateien betroffen.

Ist der Datenträger, der gelöscht wird, ein Kopierspeicherpoolatenträger, werden nur Dateien auf dem Kopienpoolatenträger gelöscht. Die Dateien im primären Speicherpool sind nicht betroffen.

Der Befehl DELETE VOLUME darf nicht mit DISCARDATA=YES verwendet werden, wenn ein Zurückschreibungsprozess (RESTORE STGPOOL oder RESTORE VOLUME) aktiv ist. Durch den Befehl DELETE VOLUME könnte die Zurückschreibung unvollständig sein.

Wird der Befehl DELETE VOLUME während der Verarbeitung abgebrochen oder tritt ein Systemfehler auf, verbleiben einige Dateien möglicherweise auf dem Datenträger. Derselbe Datenträger kann erneut gelöscht werden, damit der Server die verbleibenden Dateien und dann den Datenträger löscht.

### Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter hat nur dann Auswirkungen auf die Verarbeitung, wenn auch das Löschen aller Daten auf dem Datenträger angefordert wurde. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

#### No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

Bei dem Hintergrundprozess erstellte Nachrichten werden vom Server entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Der Befehl muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist.

Hinweis: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

## Beispiel: Einen Speicherpooldatenträger löschen

Datenträger aus dem Speicherpool stgvol.1 aus dem Speicherpool FILEPOOL löschen.

```
delete volume stgvol.1
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE VOLUME

| Befehl         | Beschreibung   |
|----------------|--|
| CANCEL PROCESS | Bricht einen Serverhintergrundprozess ab.  |
| DEFINE VOLUME  | Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll. |
| MOVE DATA      | Versetzt Daten aus einem angegebenen Speicherpooldatenträger in einen anderen Speicherpooldatenträger.         |
| MOVE DRMEDIA   | Versetzt DRM-Datenträger vor Ort und lagert sie aus.   |
| QUERY CONTENT  | Zeigt Informationen über Dateien in einem Speicherpooldatenträger an.  |
| QUERY DRMEDIA  | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.                  |
| QUERY PROCESS  | Zeigt Informationen über Hintergrundprozesse an.   |
| QUERY VOLUME   | Zeigt Informationen über Speicherpooldatenträger an.   |
| UPDATE VOLUME  | Aktualisiert die Attribute der Speicherpooldatenträger.  |

## DISABLE-Befehle

Mit den DISABLE-Befehlen können Sie einige durch den Server ausgeführte Operationstypen verhindern.

- DISABLE EVENTS (Ereignisse für Ereignisprotokollierung inaktivieren)
- DISABLE REPLICATION (Verarbeitung abgehender Replikation auf einem Server verhindern)
- DISABLE SESSIONS (Verhindern, dass neue Sitzungen auf IBM Spectrum Protect zugreifen)

## DISABLE EVENTS (Ereignisse für Ereignisprotokollierung inaktivieren)

Mit diesem Befehl kann die Verarbeitung eines oder mehrerer Ereignisse inaktiviert werden. Geben Sie einen Empfänger an, der auf keiner Plattform unterstützt wird, oder geben Sie ein ungültiges Ereignis oder einen ungültigen Namen an, gibt IBM Spectrum Protect eine Fehlermeldung aus. Alle gültigen Empfänger, Ereignisse oder Namen, die angegeben wurden, sind jedoch noch aktiviert.

Tipp: Nachrichten der Kategorie SEVERE und Nachricht ANR9999D können wertvolle Diagnoseinformationen liefern, wenn schwerwiegende Server-Probleme vorliegen. Aus diesem Grund sollten diese Nachrichten nicht inaktiviert werden.

Einschränkung:

- Bestimmte Nachrichten erscheinen an der Konsole, auch wenn sie inaktiviert wurden. Hierzu gehören einige Nachrichten, die während des Systemstarts und des Systemabschlusses des Servers ausgegeben werden, sowie Antworten auf Verwaltungsbefehle.
- Servernachrichten von dem Server, auf dem dieser Befehl ausgegeben wurde, können nicht für das Aktivitätenprotokoll inaktiviert werden.

ANR1822I gibt an, daß die Ereignisprotokollierung für den angegebenen Empfänger beendet wird. Wird der Befehl DISABLE EVENTS ausgegeben, wird diese Nachricht auch dann für den Empfänger protokolliert, wenn es sich um ein Ereignis handelt, das inaktiviert wurde. Damit wird bestätigt, dass die Ereignisprotokollierung für diesen Empfänger beendet wurde. Nachfolgende Nachrichten ANR1822I werden nicht für diesen Empfänger protokolliert.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
.-,------.
V          |
>>-DISable EVents---+--Empfänger-----+----->
                    +-ALL-----+
                    +-CONSOLE-----+
                    +-ACTLOG-----+
                    +-EVENTSERVER---+
                    +-FILE-----+
                    +-FILETEXT-----+
                    |               |
                    |             (1) |
                    +-NTEVENTLOG-----+
                    |             (2) |
                    +-SYSLOG-----+
                    +-TIVOLI-----+
                    '-USEREXIT-----'
```

```
.-,------.
V          |
>---+--Ereignisname+---+-----+-----<<
    +-ALL-----+   |               |
    +-INFO-----+  |               |
    +-WARNING-----+ +--NODEname---+--Knotenname---+
    +-ERROR-----+  |               |
    '-SEVERE-----+' |               |
                    |               |
                    |             V |
                    |             | |
                    |             | |
                    '-SERVername---+--Servername---+'
```

Anmerkungen:

1. NTEVENTLOG ist nur unter Windows verfügbar.
2. SYSLOG ist nur unter Linux verfügbar.

## Parameter

Empfänger (Erforderlich)

Gibt den Namen der Empfänger an, für die Ereignisse inaktiviert werden sollen. Mehrere Empfänger können angegeben werden, indem sie ohne Leerzeichen durch Kommas voneinander getrennt werden. Gültige Werte:

ALL

Alle Empfänger, außer Server-Ereignisse im Aktivitätenprotokollempfänger (ACTLOG). Nur Client-Ereignisse können für den Aktivitätenprotokollempfänger inaktiviert werden.

CONSOLE

Die Standardserverkonsole als Empfänger.

ACTLOG

Das Aktivitätenprotokoll als Empfänger. Es können nur Client-Ereignisse, keine Server-Ereignisse, für das Aktivitätenprotokoll inaktiviert werden.

EVENTSERVER

Der Ereignis-Server als Empfänger.

FILE


Eine Benutzerdatei als Empfänger. Jedes protokollierte Ereignis ist ein Satz in der Datei. Die Sätze können von Personen nicht einfach gelesen werden.

FILETEXT

Eine Benutzerdatei als Empfänger. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.

NTEVENTLOG

Das Windows-Anwendungsprotokoll als Empfänger.

 Linux-BetriebssystemeSYSLOG

 Linux-BetriebssystemeSchreibt Nachrichten direkt in das Systemprotokoll unter Linux.

TIVOLI

Tivoli Enterprise Console (TEC) als Empfänger.

USEREXIT

Ein benutzerdefiniertes Programm als Empfänger. Der Server schreibt Informationen in das Programm.

Ereignisse (Erforderlich)

Gibt die Ereignisse an, die inaktiviert werden sollen. Es können mehrere Ereignisse angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden. Gültige Werte:

ALL

Alle Ereignisse.

Ereignisname

Eine vierstellige Nachrichtennummer, die bei Server-Ereignissen mit den Buchstaben ANR beginnt, und bei Client-Ereignissen mit den Buchstaben ANE. Gültige Bereiche sind ANR0001 bis ANR9999 und ANE4000 bis ANE4999. Den Parameter NODENAMES angeben, wenn Clientereignisse für übereinstimmende Knoten inaktiviert werden sollen. Den Parameter SERVERNAME angeben, wenn Serverereignisse für übereinstimmende Server inaktiviert werden sollen. Nur für den TIVOLI-Ereignisempfänger können die folgenden Ereignisnamen für die IBM Spectrum Protect-Anwendungsclients angegeben werden:

| IBM Spectrum Protect-Anwendungsclient         | Präfix | Bereich   |
|---|--------|-----------|
| Data Protection for Microsoft Exchange Server | ACN    | 3500–3649 |
| Data Protection for Lotus Domino              | ACD    | 5200–5299 |
| Data Protection for Oracle                    | ANS    | 500–599   |
| Data Protection for Informix                  | ANS    | 600–699   |
| Data Protection for Microsoft SQL Server      | ACO    | 3000–3999 |

Hinweis: Bei Angabe von ALL werden diese Nachrichten inaktiviert. Die Optionen INFO, WARNING, ERROR und SEVERE haben jedoch keine Auswirkungen auf die Nachrichten.

Bewertungskategorien

Wenn die Ereignisliste eine Bewertungskategorie enthält, werden alle Ereignisse mit dieser Bewertung für die angegebenen Knoten inaktiviert. Die Nachrichtenarten sind:

INFO

Informationsnachrichten (Art I).

WARNING

Warnungen (Art W).

ERROR

Fehlernachrichten (Art E).

SEVERE

Schwerwiegende Fehlernachrichten (Art S).

NODENAME

Gibt die Knotennamen an, für die Ereignisse inaktiviert werden sollen. Es können Platzhalterzeichen (\*) verwendet werden, um alle Knoten anzugeben. Der Benutzer kann NODENAME oder SERVERNAME angeben. Wird keiner der Parameter angegeben, werden die Ereignisse für den Server inaktiviert, auf dem dieser Befehl ausgeführt wird.

SERVERNAME

Gibt die Server-Namen an, für die Ereignisse inaktiviert werden sollen. Es können Platzhalterzeichen (\*) verwendet werden, um alle anderen Server anzugeben, auf denen dieser Befehl nicht ausgeführt wird. Der Benutzer kann NODENAME oder SERVERNAME angeben. Wird keiner der Parameter angegeben, werden die Ereignisse für den Server inaktiviert, auf dem dieser Befehl ausgeführt wird.

## Beispiel: Bestimmte Kategorien von Ereignissen inaktivieren

Alle Clientereignisse in den Kategorien INFO und WARNING für das Aktivitätenprotokoll und die Konsole für alle Knoten inaktivieren.

```
disable events actlog,console
info,warning nodename=*
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DISABLE EVENTS

| Befehl             | Beschreibung   |
|--------------------|--|
| BEGIN EVENTLOGGING | Startet das Ereignisprotokoll für einen bestimmten Empfänger.                    |
| ENABLE EVENTS      | Aktiviert bestimmte Ereignisse für Empfänger.                                    |
| END EVENTLOGGING   | Beendet das Ereignisprotokoll für einen bestimmten Empfänger.                    |
| QUERY ENABLED      | Zeigt aktivierte bzw. inaktivierte Ereignisse für einen bestimmten Empfänger an. |

| Befehl           | Beschreibung   |
|------------------|--|
| QUERY EVENTRULES | Zeigt Informationen über Regeln für Server- und Clientereignisse an.   |
| QUERY STATUS     | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## DISABLE REPLICATION (Verarbeitung abgehender Replikation auf einem Server verhindern)

Mit diesem Befehl kann verhindert werden, dass ein Quellenreplikationsserver neue Replikationsprozesse startet.

Mit diesem Befehl werden keine aktiven Replikationsprozesse gestoppt. Aktive Replikationsprozesse werden fortgesetzt, bis sie abgeschlossen sind oder ohne Abschluss beendet werden. Verwenden Sie diesen Befehl und den Befehl ENABLE REPLICATION, um die Replikationsverarbeitung zu steuern.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-DISAbLe REPLiCation-----<<
```

### Parameter

Keine.

### Beispiel: Replikationsverarbeitung inaktivieren

Die Replikationsverarbeitung auf einem Quellenreplikationsserver inaktivieren.

```
disable replication
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DISABLE REPLICATION

| Befehl             | Beschreibung   |
|--------------------|--|
| CANCEL REPLICATION | Bricht Knotenreplikationsprozesse ab.  |
| DISABLE SESSIONS   | Verhindert, dass neue Sitzungen auf IBM Spectrum Protect zugreifen, lässt jedoch zu, dass bestehende Sitzungen fortgesetzt werden. |
| ENABLE REPLICATION | Ermöglicht die Verarbeitung abgehender Replikation auf einem Server.   |
| ENABLE SESSIONS    | Nimmt die Serveraktivität nach einem Befehl DISABLE oder ACCEPT DATE wieder auf.   |
| QUERY STATUS       | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.               |
| REPLICATE NODE     | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |

## DISABLE SESSIONS (Verhindern, dass neue Sitzungen auf IBM Spectrum Protect zugreifen)



Verwenden Sie diesen Befehl, um zu verhindern, dass neue Sitzungen auf IBM Spectrum Protect zugreifen. Aktive Sitzungen werden abgeschlossen. Für einen bestimmten Server können Sie angeben, ob eingehende Sitzungen und/oder abgehende Sitzungen inaktiviert werden sollen.

Serverprozesse, wie beispielsweise die Umlagerung und Wiederherstellung, sind nicht betroffen, wenn Sie den Befehl DISABLE SESSIONS ausgeben.

## Berechtigungsklasse

---

Für diesen Befehl ist die System- oder die Bedienerberechtigung erforderlich.

## Syntax

---

```
>>-DISAbLe SESSions----->
. -CLient-----
>--+-----+<
'|++-CLient-----+'
'|++ALL-----+'
'|++ADMin-----+'
'|--SERVer-----+'
|          |
|          | .-DIRection---Both-----|
'|--Servername-----+'
'|++-DIRection---Both-----+'
'|++-DIRection---INbound---+'
'|--DIRection---OUTbound--+'
```

## Parameter

---

Gibt den Typ der Sitzung an, der inaktiviert werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist CLIENT. Sie können einen der folgenden Werte angeben:

### CLIENT

Inaktiviert nur Sicherungs- und Archivierungsclientsitzungen.

### ALL

Inaktiviert alle Sitzungstypen.

### ADMIN

Inaktiviert nur Verwaltungssitzungen.

### SERVer

Inaktiviert nur Sitzungen zwischen Servern. Es werden nur die folgenden Typen von Sitzungen inaktiviert:

- Ereignisprotokollierung zwischen Servern
- Unternehmensverwaltung
- Serverregistrierung
- LAN-unabhängig: Speicheragent - Server
- Virtuelle Datenträger
- Knotenreplikation

Sie können auch angeben, ob eingehende Sitzungen und/oder abgehende Sitzungen für einen bestimmten Server inaktiviert werden sollen.

### Servername

Gibt den Namen eines Servers an, dessen Sitzungen inaktiviert werden sollen. Dieser Parameter ist wahlfrei. Wenn Sie diesen Parameter nicht angeben, werden neue Sitzungen mit anderen Servern nicht gestartet. Aktive Sitzungen werden nicht abgebrochen.

### DIRection

Gibt an, ob eingehende Sitzungen und/oder abgehende Sitzungen inaktiviert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist BOTH. Die folgenden Werte sind gültig:

#### Both

Gibt an, dass eingehende Sitzungen vom angegebenen Server und abgehende Sitzungen zum angegebenen Server inaktiviert werden.

#### INbound

Gibt an, dass nur eingehende Sitzungen vom angegebenen Server inaktiviert werden.

#### OUTbound

Gibt an, dass nur abgehende Sitzungen zum angegebenen Server inaktiviert werden.

## Beispiel: Neue Clientknotensicherungs- und -archivierungssitzungen auf dem Server verhindern

Den Zugriff neuer Client-Knotensitzungen auf den Server vorübergehend verhindern.

```
disable sessions
```

## Beispiel: Alle neuen Sitzungen auf dem Server verhindern

Den Zugriff neuer Sitzungen auf den Server vorübergehend verhindern.

```
disable sessions all
```

## Beispiel: Abgehende Sitzungen zu einem Server inaktivieren

Abgehende Sitzungen zu dem Server REPLSRV inaktivieren.

```
disable sessions server replsrv direction=outbound
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DISABLE SESSIONS

| Befehl              | Beschreibung   |
|---------------------|--|
| CANCEL SESSION      | Bricht aktive Sitzungen mit dem Server ab.   |
| DISABLE REPLICATION | Verhindert die Verarbeitung abgehender Replikation auf einem Server.   |
| ENABLE SESSIONS     | Nimmt die Serveraktivität nach einem Befehl DISABLE oder ACCEPT DATE wieder auf.                                     |
| QUERY SESSION       | Zeigt Informationen zu allen aktiven Administrator- und Clientsitzungen mit IBM Spectrum Protect an.                 |
| QUERY STATUS        | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## DISMOUNT-Befehl

Mit dem Befehl DISMOUNT kann ein Datenträger nach der Adresse der realen Einheit oder nach dem Datenträgernamen entladen werden.

- DISMOUNT VOLUME (Datenträger nach Datenträgernamen entladen)

## DISPLAY OBJNAME (Vollständigen Objektnamen anzeigen)

Mit diesem Befehl kann IBM Spectrum Protect einen vollständigen Objektnamen anzeigen, wenn der in einer Nachricht oder in einer Abfrageausgabe angezeigte Name aufgrund der Länge abgekürzt wurde. Objektnamen, die sehr lang sind, sind über normale Betriebssystemfunktionen schwer anzuzeigen und zu verwenden. Der IBM Spectrum Protect-Server kürzt lange Namen ab und ordnet ihnen eine Token-ID zu, die verwendet werden kann, wenn der Objektpfadname 1024 Byte überschreitet. Die Token-ID wird in einer Zeichenfolge angezeigt, die IDs für den Knoten, den Dateibereich und den Objektnamen einschließt. Das Format ist: [TSMOBJ:nID.fsID.objID]. Bei Angabe mit dem Befehl DISPLAY OBJNAME kann die Token-ID verwendet werden, um den vollständigen Objektnamen anzuzeigen.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-DISplay OBJname--Token-ID-----<<
```

## Parameter

Token-ID (Erforderlich)

Gibt die im Tag [TSMOBJ:] zurückgemeldete ID an, wenn ein Objektname zu lang ist, um angezeigt werden zu können.

## Beispiel: Den vollständigen Objektnamen einer Token-ID in einer Nachricht anzeigen

Angenommen, Sie empfangen die folgende Nachricht:

```
ANR9999D file.c(1999) Fehler bei der Bearbeitung von Datei [TSMOBJ:1.1.649498]
aufgrund fehlender Serverressourcen.
```

Den vollständigen Objektnamen für die Datei anzeigen, auf die in der Fehlnachricht verwiesen wird, indem die Token-ID im Befehl DISPLAY OBJNAME angegeben wird.

```
display obj 1.1.649498
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DISPLAY OBJNAME

| Befehl        | Beschreibung  |
|---------------|---|
| QUERY CONTENT | Zeigt Informationen über Dateien in einem Speicherpooldatenträger an. |

## ENABLE-Befehle

Mit den ENABLE-Befehlen können Sie einige durch den Server ausgeführte Operationstypen zulassen.

- ENABLE EVENTS (Server- oder Clientereignisse zum Protokollieren aktivieren)
- ENABLE REPLICATION (Verarbeitung abgehender Replikation auf einem Server ermöglichen)
- ENABLE SESSIONS (Benutzeraktivität auf dem Server wiederaufnehmen)

## ENABLE EVENTS (Server- oder Clientereignisse zum Protokollieren aktivieren)

Mit diesem Befehl kann die Verarbeitung eines oder mehrerer Ereignisse aktiviert werden. Geben Sie einen Empfänger an, der auf keiner Plattform unterstützt wird, oder geben Sie ein ungültiges Ereignis oder einen ungültigen Namen an, gibt IBM Spectrum Protect eine Fehlnachricht aus. Alle gültigen Empfänger, Ereignisse oder Namen, die angegeben wurden, sind jedoch noch aktiviert.

Einschränkung: Bestimmte Ereignisse, wie z. B. während des Starts oder des Systemabschlusses des Servers ausgegebene Nachrichten, werden automatisch an die Konsole weitergeleitet. Sie werden nicht an andere Empfänger weitergeleitet, auch wenn sie aktiviert sind.

Verwaltungsbefehle werden an den zurückgegeben, der den Befehl ausgegeben hat, und werden nur als nummerierte Ereignisse protokolliert. Diese nummerierten Ereignisse werden nicht an der Systemkonsole, sondern in anderen Empfängern protokolliert, einschließlich Verwaltungsbefehlszeilensitzungen, die im Konsolenmodus ausgeführt werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
.-,-----
v |
>>-ENable--EEvents---+--ALL-----+----->
      +-CONSOLE-----+
      +-ACTLOG-----+
      +-EVENTSERVER---+
      +-FILE-----+
      +-FILETEXT-----+
      |                |
      |                (1) |
      +-NTEVENTLOG----+
      |                |
      |                (2) |
      +-SYSLOG-----+
      +-TIVOLI-----+
      '-USEREXIT-----'
```

```

      .-,-----
      v          |
>-----+--Ereignisname--+-----+----->>
      +-ALL-----+      |          .-,-----
      +-INFO-----+      |          v          |
      +-WARNING-----+  +-NODEname-----Knotenname-----+
      +-ERROR-----+      |          .-,-----
      +-SEVERE-----+'    |          v          |
                          +-SERVername-----Servername-----+'

```

Anmerkungen:

1. NTEVENTLOG ist nur unter Windows verfügbar.
2. Dieser Parameter ist nur für das Linux-Betriebssystem verfügbar.

## Parameter

### Empfänger (Erforderlich)

Gibt einen oder mehrere Empfänger an, für die aktivierte Ereignisse protokolliert werden sollen. Es können mehrere Empfänger angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden. Gültige Werte sind:

ALL

Alle Empfänger.

CONSOLE

Die Standardserverkonsole als Empfänger.

ACTLOG

Das Serveraktivitätenprotokoll als Empfänger.

EVENTSERVER


Der Ereignis-Server als Empfänger.


FILE


Eine Benutzerdatei als Empfänger. Jedes protokollierte Ereignis ist ein Satz in der Datei. Die Sätze können von Personen nicht einfach gelesen werden.


FILETEXT

Eine Benutzerdatei als Empfänger. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.

 Windows-BetriebssystemeNTEVENTLOG

 Windows-BetriebssystemeDas Windows-Anwendungsprotokoll als Empfänger.

 Linux-BetriebssystemeSYSLOG

 Linux-BetriebssystemeGibt das Linux-Systemprotokoll als Empfänger an.

TIVOLI

Tivoli Enterprise Console (TEC) als Empfänger.

USEREXIT

Ein benutzerdefiniertes Programm als Empfänger. Der Server schreibt Informationen in das Programm.

### Ereignisse (Erforderlich)

Gibt die Art der Ereignisse an, die aktiviert werden sollen. Es können mehrere Ereignisse angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden. Gültige Werte:

ALL

Alle Ereignisse.

Ereignisname

Eine vierstellige Nachrichtennummer, die bei Server-Ereignissen mit den Buchstaben ANR beginnt, und bei Client-Ereignissen mit den Buchstaben ANE. Gültige Bereiche sind ANR0001 bis ANR9999 und ANE4000 bis ANE4999. Den Parameter NODENAME angeben, wenn Clientereignisse für übereinstimmende Knoten aktiviert werden sollen. Den Parameter SERVERNAME angeben, wenn Serverereignisse für übereinstimmende Server aktiviert werden sollen. Für den TIVOLI-Ereignisempfänger können die folgenden zusätzlichen Bereiche für die IBM Spectrum Protect-Anwendungsclients angegeben werden:

| IBM Spectrum Protect-Anwendungsclient         | Präfix | Bereich   |
|---|--------|-----------|
| Data Protection for Microsoft Exchange Server | ACN    | 3500–3649 |
| Data Protection for Lotus Domino              | ACD    | 5200–5299 |
| Data Protection for Oracle                    | ANS    | 500–599   |
| Data Protection for Informix                  | ANS    | 600–699   |
| Data Protection for Microsoft SQL Server      | ACO    | 3000–3999 |

Einschränkung: Für den Anwendungsclient muss die erweiterte Tivoli Event Console-Unterstützung aktiviert sein, damit diese Nachrichten an die Tivoli Event Console weitergeleitet werden.

Tipp:

- Bei Angabe der Option ALL werden diese Nachrichten aktiviert. Die Optionen INFO, WARNING, ERROR und SEVERE haben jedoch keine Auswirkungen auf die Nachrichten.
- Aufgrund der Anzahl der Nachrichten sollten nicht alle Nachrichten eines Knotens zum Protokollieren auf der Tivoli Event Console aktiviert werden.

#### Bewertungskategorien

Wenn die Ereignisliste eine Bewertungskategorie enthält, werden alle Ereignisse mit dieser Bewertung für die angegebenen Knoten aktiviert. Die Nachrichtenarten sind:

##### INFO

Informationsnachrichten (Art I) werden aktiviert.

##### WARNING

Warnungen (Art W) werden aktiviert.

##### ERROR

Fehlernachrichten (Art E) werden aktiviert.

##### SEVERE

Schwerwiegende Fehlernachrichten (Art S) werden aktiviert.

#### NODENAME

Gibt einen oder mehrere Clientknoten an, für die Ereignisse aktiviert werden. Es kann ein Platzhalterzeichen verwendet werden, um alle Clientknoten anzugeben. Der Benutzer kann NODENAME oder SERVERNAME angeben. Wird keiner der Parameter angegeben, werden Ereignisse für den Server aktiviert, auf dem dieser Befehl ausgeführt wird.

#### SERVername

Gibt einen oder mehrere Server an, für die Ereignisse aktiviert werden sollen. Es kann ein Platzhalterzeichen verwendet werden, um alle anderen Server anzugeben, von denen dieser Befehl nicht ausgegeben wird. Der Benutzer kann SERVERNAME oder NODENAME angeben. Wird keiner der Parameter angegeben, werden die Ereignisse für den Server aktiviert, auf dem dieser Befehl ausgeführt wird.

## Beispiel: Bestimmte Kategorien von Ereignissen aktivieren

Alle Client-Ereignisse ERROR und SEVERE für den Empfänger USEREXIT und den Knoten BONZO aktivieren.

```
enable events userexit error,severe nodename=bonzo
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für ENABLE EVENTS

| Befehl             | Beschreibung   |
|--------------------|--|
| BEGIN EVENTLOGGING | Startet das Ereignisprotokoll für einen bestimmten Empfänger.  |
| DISABLE EVENTS     | Inaktiviert bestimmte Ereignisse für Empfänger.  |
| END EVENTLOGGING   | Beendet das Ereignisprotokoll für einen bestimmten Empfänger.  |
| QUERY ENABLED      | Zeigt aktivierte bzw. inaktivierte Ereignisse für einen bestimmten Empfänger an.                                     |
| QUERY EVENTRULES   | Zeigt Informationen über Regeln für Server- und Clientereignisse an.   |
| QUERY STATUS       | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## ENABLE REPLICATION (Verarbeitung abgehender Replikation auf einem Server ermöglichen)

Verwenden Sie diesen Befehl, um es einem Quellenreplikationsserver zu ermöglichen, die normale Replikationsverarbeitung nach einer Datenbankzurückschreibung zu starten. Sie können diesen Befehl auch verwenden, um die Replikationsverarbeitung wiederaufzunehmen, nachdem der Befehl DISABLE REPLICATION ausgegeben wurde.

Achtung: Bevor die Replikation nach einer Datenbankzurückschreibung aktiviert wird, bestimmen Sie, ob Kopien von Daten, die sich auf dem Zielsystem befinden, benötigt werden. Ist dies der Fall, müssen Sie Clientknotendaten synchronisieren, indem die Daten vom

Zielreplikationsserver auf den Quellenreplikationsserver repliziert werden. Der Replikationsprozess ersetzt die Daten auf dem Quellenserver, die aufgrund der Datenbankzurückschreibung nicht mehr vorhanden waren.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-ENable REPLication-----<<
```

## Parameter

---

Keine.

## Beispiel: Replikationsverarbeitung ermöglichen

---

Die Replikationsverarbeitung auf einem Quellenreplikationsserver ermöglichen.

```
enable replication
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für ENABLE REPLICATION

| Befehl              | Beschreibung   |
|---------------------|--|
| DISABLE REPLICATION | Verhindert die Verarbeitung abgehender Replikation auf einem Server.   |
| DISABLE SESSIONS    | Verhindert, dass neue Sitzungen auf IBM Spectrum Protect zugreifen, lässt jedoch zu, dass bestehende Sitzungen fortgesetzt werden. |
| ENABLE SESSIONS     | Nimmt die Serveraktivität nach einem Befehl DISABLE oder ACCEPT DATE wieder auf.   |
| QUERY STATUS        | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.               |
| REPLICATE NODE      | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |

## ENABLE SESSIONS (Benutzeraktivität auf dem Server wiederaufnehmen)

---

Verwenden Sie diesen Befehl nach der Ausgabe des Befehls DISABLE SESSIONS, um neue Sitzungen zu starten, die auf einen Server zugreifen können. Für einen bestimmten Server können Sie angeben, ob eingehende Sitzungen und/oder abgehende Sitzungen aktiviert werden sollen.

Die Verarbeitung dieses Befehls hat keine Auswirkungen auf Systemprozesse, wie beispielsweise Umlagerung und Wiederherstellung.

Mit dem Befehl QUERY STATUS kann die Verfügbarkeit des Servers angezeigt werden.

## Berechtigungsklasse

---

Für diesen Befehl ist die System- oder die Bedienerberechtigung erforderlich.

## Syntax

---

```
>>-ENable SESSions----->
.-CLient-----
>--+-----+><
'--+CLient-----+'
```

```

+-ALL-----+
+-Admin-----+
'-SERVer-----+'
      |           .-DIRection---Both-----|
      '-Servername-----+'
              '+-DIRection---Both-----+'
              '+-DIRection---INbound---+'
              '-DIRection---OUTbound-'

```

## Parameter

Gibt den Typ der Sitzung an, der aktiviert werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist CLIENT. Sie können einen der folgenden Werte angeben:

### CLient

Aktiviert nur Sicherungs- und Archivierungsclientsitzungen.

### ALL

Aktiviert alle Sitzungstypen.

### ADMin

Aktiviert nur Verwaltungssitzungen.

### SERVer

Aktiviert nur Sitzungen zwischen Servern. Sie können auch angeben, ob eingehende Sitzungen und/oder abgehende Sitzungen für einen bestimmten Server aktiviert werden sollen.

### Servername

Gibt den Namen eines bestimmten Servers an, dessen Sitzungen aktiviert werden sollen. Dieser Parameter ist wahlfrei. Wenn Sie diesen Parameter nicht angeben, werden neue Sitzungen mit allen anderen Servern aktiviert.

### DIRection

Gibt an, ob eingehende Sitzungen und/oder abgehende Sitzungen aktiviert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist BOTH. Die folgenden Werte sind gültig:

#### Both

Gibt an, dass eingehende Sitzungen vom angegebenen Server und abgehende Sitzungen zum angegebenen Server aktiviert werden.

#### INbound

Gibt an, dass nur eingehende Sitzungen zum angegebenen Server aktiviert werden.

#### OUTbound

Gibt an, dass nur abgehende Sitzungen vom angegebenen Server aktiviert werden.

## Beispiel: Clientknotenaktivität auf dem Server wieder aufnehmen

Den Normalbetrieb wiederaufnehmen und den Zugriff der Client-Knoten auf den Server ermöglichen.

```
enable sessions
```

## Beispiel: Alle Aktivitäten auf dem Server wieder aufnehmen

Den Normalbetrieb wiederaufnehmen und den Zugriff aller Sitzungen auf den Server ermöglichen.

```
enable sessions all
```

## Beispiel: Abgehende Sitzungen zu einem Server aktivieren

Abgehende Sitzungen zu dem Server REPLSRV aktivieren.

```
enable sessions server replsrv direction=outbound
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für ENABLE SESSIONS

| Befehl         | Beschreibung                                  |
|----------------|---|
| ACCEPT DATE    | Akzeptiert das aktuelle Datum auf dem Server. |
| CANCEL SESSION | Bricht aktive Sitzungen mit dem Server ab.    |

| Befehl             | Beschreibung   |
|--------------------|--|
| ENABLE REPLICATION | Ermöglicht die Verarbeitung abgehender Replikation auf einem Server.   |
| DISABLE SESSIONS   | Verhindert, dass neue Sitzungen auf IBM Spectrum Protect zugreifen, lässt jedoch zu, dass bestehende Sitzungen fortgesetzt werden. |
| QUERY SESSION      | Zeigt Informationen zu allen aktiven Administrator- und Clientsitzungen mit IBM Spectrum Protect an.                               |
| QUERY STATUS       | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.               |

## ENCRYPT STGPOOL (Daten in einem Speicherpool verschlüsseln)

Mit diesem Befehl können Daten in einem Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool verschlüsselt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

                                .-MAXPRocess---4-----
>>-ENCRypt STGpool--Poolname--+-----+----->
                                '-MAXPRocess---Anzahl-'

.-Preview---No----- .-Wait---No-----
>+-----+-----+-----+-----><
  '-Preview---+Yes--+' '-Wait---+No--+'
      '-No--'          '-Yes-'

```

### Parameter

#### Poolname (Erforderlich)

Gibt den Namen des Speicherpools an, der Daten enthält, die verschlüsselt werden müssen.

Einschränkungen:

- Sie können nur Verzeichniscontainerspeicherpools oder Cloud-Containerspeicherpools angeben.
- Für den Speicherpoolnamen können bis zu 30 Zeichen angegeben werden. Wenn Sie mehr als 30 Zeichen angeben, schlägt der Befehl fehl.

#### MAXPRocess

Gibt die maximale Anzahl paralleler Prozesse an, die ausgeführt werden können, wenn der Speicherpool Daten verschlüsselt.

Dieser Parameter ist wahlfrei. Geben Sie einen Wert im Bereich von 1 bis 99 ein. Der Standardwert ist 4.

#### Preview

Gibt an, ob eine Voranzeige mit allen Befehlen angezeigt wird, die als Teil des Befehls ENCRYPT STGPOOL verarbeitet werden.

Dieser Parameter ist wahlfrei. Die folgenden Werte sind gültig:

No

Gibt an, dass keine Voranzeige der Befehle angezeigt wird. Dies ist der Standardwert.

Yes

Gibt an, dass eine Voranzeige der Befehle angezeigt wird.

#### Wait

Gibt an, ob die Speicherpoolverschlüsselung im Vordergrund oder Hintergrund ausgeführt wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass die Operation im Hintergrund ausgeführt wird. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden. Dies ist der Standardwert.

Yes







## FILE


Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist ein Satz in der Datei, und eine Person kann jedes protokollierte Ereignis nicht einfach lesen.


## FILETEXT

Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.

 Windows-Betriebssysteme NTEVENTLOG

 Windows-Betriebssysteme Gibt das Windows-Anwendungsprotokoll als Empfänger an.

 Linux-Betriebssysteme SYSLOG

 Linux-Betriebssysteme Gibt das Linux-Systemprotokoll als Empfänger an.

## TIVOLI

Gibt Tivoli Management Environment (TME) als Empfänger an.

## USEREXIT

Gibt eine benutzerdefinierte Routine, in die IBM Spectrum Protect Informationen schreibt, als Empfänger an.

## Beispiel: Das Protokollieren von Ereignissen stoppen

Das Protokollieren von Ereignissen für den Benutzerausgang beenden.

```
end eventlogging userexit
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für END EVENTLOGGING

| Befehl             | Beschreibung   |
|--------------------|--|
| BEGIN EVENTLOGGING | Startet das Ereignisprotokoll für einen bestimmten Empfänger.  |
| DISABLE EVENTS     | Inaktiviert bestimmte Ereignisse für Empfänger.  |
| ENABLE EVENTS      | Aktiviert bestimmte Ereignisse für Empfänger.  |
| QUERY ENABLED      | Zeigt aktivierte bzw. inaktivierte Ereignisse für einen bestimmten Empfänger an.                                     |
| QUERY EVENTRULES   | Zeigt Informationen über Regeln für Server- und Clientereignisse an.   |
| QUERY STATUS       | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## EXPIRE INVENTORY (Datenträgerbestandsverfall manuell starten)

Mit diesem Befehl kann die Verarbeitung des Datenträgerbestandsverfalls manuell gestartet werden. Beim Bestandsverfallsprozess werden Kopien von Clientsicherungs- und Archivierungsdateien aus dem Serverspeicher entfernt. Das Entfernen basiert auf Maßnahmenspezifikationen in den Sicherungs- und Archivierungskopiengruppen der Verwaltungsklassen, an die die Dateien gebunden sind.

Ist die Disaster Recovery Manager-Funktion für den IBM Spectrum Protect-Server verfügbar, entfernt der Bestandsverfallsprozess auch auswählbare virtuelle Datenträger, die von den folgenden Prozessen verwendet werden:

- Datenbanksicherungen der Art BACKUPFULL, BACKUPINCR und DBSNAPSHOT. Der Befehl SET DRMDBBACKUPEXPIREDAYS steuert, wann diese Datenträger für den Verfall auswählbar sind.
- Wiederherstellungsplandateien der Art RPFIL und RPFNSAPSHOT. Der Befehl SET DRMRPFEXPIREDAYS steuert, wann diese Datenträger für den Verfall auswählbar sind.

Der Datenträgerbestandsverfall, der während der Serverinitialisierung ausgeführt wird, entfernt nicht diese virtuellen Datenträger.

Es kann nur jeweils ein Verfallsprozess ausgeführt werden, aber dieser Prozess kann auf maximal 40 Threads verteilt werden. Wird ein Verfallsprozess ausgeführt, kann kein anderer Prozess gestartet werden.

Mit der Serveroption EXPINTERVAL kann die automatische Verfallsverarbeitung konfiguriert werden. Wird die Option EXPINTERVAL auf 0 gesetzt, wird die Verfallsverarbeitung von dem Server nicht automatisch ausgeführt, und Sie müssen den Befehl EXPIRE INVENTORY ausgeben, um die Verfallsverarbeitung zu starten.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.



Bei dem Hintergrundprozess erstellte Nachrichten werden vom Server entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Sie warten auf die Beendigung des Befehls, bevor Sie mit anderen Tasks fortfahren. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist.

Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

SKipdirs

Gibt an, ob der Server während der Verfallsverarbeitung Objekte mit einem Verzeichnistyp überspringt. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, dass der Server Dateien und Verzeichnisse auf der Basis der entsprechenden Maßnahmekriterien als verfallen kennzeichnet.

Yes

Gibt an, dass der Server Sicherungs- und Archivierungsobjekte mit einem Verzeichnistyp während der Verfallsverarbeitung überspringt, auch wenn die Verzeichnisse für die Verfallsverarbeitung ausgewählt werden können. Bei Angabe von YES verhindern Sie das Löschen von Verzeichnissen und die Verfallsverarbeitung kann schneller ausgeführt werden.

Achtung: Diese Option sollte nicht immer verwendet werden. Mit IBM Spectrum Protect Version 6.0 und höher können Sie mehrere Threads (Ressourcen) für einen Verfallsprozess ausführen. Wird YES oft angegeben, wächst außerdem die Datenbank an, da die Verzeichnisobjekte akkumulieren, und es erhöht sich die für die Verfallsverarbeitung benötigte Zeit. Führen Sie SKIPDIRS=NO regelmäßig aus, um die Verzeichnisse als verfallen zu kennzeichnen und die Größe der Datenbank zu reduzieren.

Nodes

Gibt den Namen der Clientknoten oder Knotengruppen an, deren Daten verarbeitet werden sollen. Sollen mehrere Knoten- und Knotengruppenamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Knotennamen können Platzhalterzeichen enthalten, Knotengruppenamen dagegen nicht. Dieser Parameter ist wahlfrei.

Sie können NODES, EXCLUDENODES, DOMAIN oder eine beliebige Kombination angeben. Wenn Sie mehrere dieser Parameter angeben, werden nur die Knoten verarbeitet, die den Kriterien für die Befehlsparameter NODES und DOMAIN entsprechen, und nicht den Kriterien für den Befehlsparameter EXCLUDENODES entsprechen. Wenn Sie keinen Wert für NODES, EXCLUDENODES oder DOMAIN angeben, werden Daten für alle Knoten verarbeitet.

EXCLUDENodes

Gibt die Namen der Clientknoten oder Knotengruppen an, deren Daten nicht verarbeitet werden sollen. Sollen mehrere Knoten- und Knotengruppenamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Knotennamen können Platzhalterzeichen enthalten, Knotengruppenamen dagegen nicht. Dieser Parameter ist wahlfrei.

Sie können NODES, EXCLUDENODES, DOMAIN oder eine beliebige Kombination angeben. Wenn Sie mehrere dieser Parameter angeben, werden nur die Knoten verarbeitet, die den Kriterien für die Befehlsparameter NODES und DOMAIN entsprechen, und nicht den Kriterien für den Befehlsparameter EXCLUDENODES entsprechen. Wenn Sie keinen Wert für NODES, EXCLUDENODES oder DOMAIN angeben, werden Daten für alle Knoten verarbeitet.

Domain

Gibt an, dass nur Daten für Clientknoten verarbeitet werden sollen, die der angegebenen Domäne zugeordnet sind. Dieser Parameter ist wahlfrei. Sie können NODES, EXCLUDENODES, DOMAIN oder eine beliebige Kombination angeben. Wenn Sie mehrere dieser Parameter angeben, werden nur die Knoten verarbeitet, die den Kriterien für die Befehlsparameter NODES und DOMAIN entsprechen, und nicht den Kriterien für den Befehlsparameter EXCLUDENODES entsprechen. Wenn Sie keinen Wert für NODES, EXCLUDENODES oder DOMAIN angeben, werden Daten für alle Knoten verarbeitet.

Type

Gibt den Typ der Daten an, die verarbeitet werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist ALL. Gültige Werte:

ALL

Alle Typen von Daten verarbeiten, die für die Verfallsverarbeitung auswählbar sind.

Archive

Nur Clientarchivierungsdaten verarbeiten.

Backup

Nur Clientsicherungsdaten verarbeiten.

Other

Nur Elemente für Disaster Recovery Manager-Funktionen verarbeiten, wie beispielsweise Wiederherstellungsplandateien und veraltete Datenbanksicherungen.

REsource

Gibt die Anzahl der Threads an, die parallel ausgeführt werden können. Geben Sie einen Wert im Bereich von 1 bis 40 an. Dieser Parameter ist wahlfrei. Der Standardwert ist vier.

Die Verfallsverarbeitung wird als einzelner Prozess ausgeführt, obwohl die Ressourcen parallele Arbeit durch den Server innerhalb des einzelnen Verfallsprozesses darstellen. Der Verfallsprozess für Archivierungsdaten für einen Knoten wird nur auf einer einzelnen Ressource ausgeführt, aber der Verfallsprozess für Sicherungsdaten kann auf Ressourcen auf Dateibereichsebene verteilt werden. Geben Sie beispielsweise `NODE=X, Y, Z` mit jeweils drei Dateibereichen und `RESOURCE=5` an, wird die Verfallsverarbeitung für die drei Clientknoten X, Y und Z parallel ausgeführt. Mindestens eine Ressource verarbeitet jeden Knoten und mindestens ein Knoten verwendet mehrere Ressourcen für die Verarbeitung der Sicherungsdaten in den Dateibereichen.

#### DURATION

Gibt die maximale Anzahl Minuten für die Ausführung des Verfallsprozesses an. Der Prozess stoppt, wenn die angegebene Anzahl Minuten überschritten wird oder wenn alle auswählbaren verfallenen Objekte gelöscht werden (je nachdem, welches Ereignis zuerst eintritt). Geben Sie einen Wert im Bereich von 1 bis 2880 an. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, ist die Dauer des Verfallsprozesses nicht zeitlich begrenzt.

### Beispiel: Die Bestandsverfallsverarbeitung für einen bestimmten Zeitraum ausführen

---

Den Verfallsprozess zwei Stunden lang ausführen.

```
expire inventory duration=120
```

### Beispiel: Die Bestandsverfallsverarbeitung für Sicherungsdaten für zwei Clientknoten ausführen

---

Die Bestandsverfallsverarbeitung für die Sicherungsdaten der beiden Clientknoten CHARLIE und ROBBIE ausführen. Der Server soll die Verfallsverarbeitung ausführen, bis sie abgeschlossen ist.

```
expire inventory nodes=charlie,robbie resource=2 type=backup
```

### Beispiel: Die Bestandsverfallsverarbeitung für alle Clientknoten mit Ausnahme von zwei Knoten ausführen

---

Die Bestandsverfallsverarbeitung für alle Clientknoten mit Ausnahme der beiden Knoten CHARLIE und ROBBIE ausführen. Der Server soll die Verfallsverarbeitung ausführen, bis sie abgeschlossen ist.

```
expire inventory excludenodes=charlie,robbie
```

### Beispiel: Die Bestandsverfallsverarbeitung für alle Clientknoten in einer Domäne mit Ausnahme eines Knotens ausführen

---

Die Bestandsverfallsverarbeitung für alle Clientknoten in einer Domäne mit Ausnahme des Knotens ROBBIE ausführen. Der Server soll die Verfallsverarbeitung ausführen, bis sie abgeschlossen ist.

```
expire inventory domain=standard excludenodes=robbie
```

### Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für EXPIRE INVENTORY

| Befehl            | Beschreibung                                     |
|-------------------|--|
| AUDIT LICENSES    | Prüft die Einhaltung der definierten Lizenzen.   |
| CANCEL EXPIRATION | Bricht die Bestandsverfallsverarbeitung ab.      |
| CANCEL PROCESS    | Bricht einen Serverhintergrundprozess ab.        |
| QUERY PROCESS     | Zeigt Informationen über Hintergrundprozesse an. |

### EXPORT-Befehle

---

Mit den EXPORT-Befehlen können Informationen von einem IBM Spectrum Protect-Server auf sequenzielle austauschbare Datenträger kopiert werden.

Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten exportiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver

verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls EXPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.

- EXPORT ADMIN (Administratorinformationen exportieren)
- EXPORT NODE (Clientknoteninformationen exportieren)
- EXPORT POLICY (Maßnahmeninformationen exportieren)
- EXPORT SERVER (Serverinformationen exportieren)

## EXPORT ADMIN (Administratorinformationen exportieren)

Mit diesem Befehl können Administrator- und Berechtigungsdefinitionen von einem Server exportiert werden. Sie können die Informationen auf sequenzielle Datenträger exportieren, um sie später auf einen anderen Server zu importieren, oder Sie können die Informationen direkt auf einen anderen Server exportieren.

Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten exportiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls EXPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.

IBM Spectrum Protect exportiert folgende Administratorinformationen:

- Name, Kennwort und Kontaktinformationen des Administrators
- Dem Administrator erteilte Verwaltungsberechtigungsklassen
- Die Angabe, ob die Administrator-ID für den Server-Zugriff gesperrt ist

Mit dem Befehl QUERY ACTLOG kann der Status der Exportoperation angezeigt werden. Diese Informationen können auch über die Serverkonsole angezeigt werden.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn Sie Informationen auf sequenzielle Datenträger exportieren und der Hintergrundprozess abgebrochen wird, sind die sequenziellen Datenträger, auf denen sich die exportierten Daten befinden, unvollständig und dürfen nicht zum Importieren von Daten verwendet werden. Wird ein Hintergrundprozess abgebrochen, bei dem Daten von einem Server auf einen anderen Server exportiert werden, kann dies zu einem Teilimport von Daten führen. Werten Sie alle importierten Daten auf dem Zielsystem aus, um zu bestimmen, ob die importierten Daten behalten oder gelöscht werden sollen. Überprüfen Sie die Importnachrichten auf Details. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Die folgenden Einschränkungen gelten für die Exportfunktion:

- Exportoperationen aus einer höheren Version und einem höheren Release in eine frühere Version und ein früheres Release werden nicht unterstützt.
- Exportoperationen zwischen Servern, die dieselbe Version und dasselbe Release, aber verschiedene Fixpacks aufweisen, können fehlschlagen. Beispielsweise können Sie keinen Export von einem Server der Version 7.1.3 auf einen Server der Version 7.1.1 oder einen früheren Server ausführen.
- Exportierte Daten von einem Server mit aktiviertem Aufbewahrungsschutz sind nicht durch Aufbewahrung geschützt, wenn sie auf einen anderen Server importiert werden.
- Die Exportverarbeitung schließt Knoten des Typs NAS (Network-attached Storage) aus.
- Das Exportieren von Daten in eine Centera-Einheitenklasse oder das Importieren von Daten aus einer Centera-Einheitenklasse wird nicht unterstützt. Dateien, die in Centera-Speicherpools gespeichert werden, können jedoch exportiert werden, und Dateien, die importiert werden müssen, können auf einer Centera-Speichereinheit gespeichert werden.

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomenen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

Der Befehl EXPORT ADMIN hat zwei Formen: Zum Exportieren von Daten direkt auf einen anderen Server in dem Netz oder zum Exportieren von Daten auf sequenzielle Datenträger. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für EXPORT ADMIN

| Befehl         | Beschreibung                              |
|----------------|---|
| CANCEL PROCESS | Bricht einen Serverhintergrundprozess ab. |

| Befehl        | Beschreibung  |
|---------------|---|
| EXPORT NODE   | Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.                       |
| EXPORT POLICY | Kopiert Maßnahmeninformationen auf externe Datenträger oder direkt auf einen anderen Server.                          |
| EXPORT SERVER | Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server. |
| IMPORT ADMIN  | Schreibt Verwaltungsdaten von externen Datenträgern zurück.   |
| QUERY ACTLOG  | Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.  |
| QUERY PROCESS | Zeigt Informationen über Hintergrundprozesse an.  |

- EXPORT ADMIN (Administratordefinitionen auf sequenzielle Datenträger exportieren)  
Sie können Administrator- und Berechtigungsdefinitionen von einem Server auf sequenzielle Datenträger exportieren, um sie später auf einen anderen Server zu importieren.
- EXPORT ADMIN (Administratorinformationen direkt auf einen anderen Server exportieren)  
Mit diesem Befehl können Administrator- und Berechtigungsdefinitionen direkt auf einen anderen Server in dem Netz exportiert werden. Dies hat einen sofortigen Import auf den Zielsever zur Folge.

## EXPORT ADMIN (Administratordefinitionen auf sequenzielle Datenträger exportieren)

Sie können Administrator- und Berechtigungsdefinitionen von einem Server auf sequenzielle Datenträger exportieren, um sie später auf einen anderen Server zu importieren.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```

>>-EXPort Admin-----+----->
| .,-----+-----|
| V-----+-----|
|'---Administratorname---+'
|
|-----+-----|
|.-Preview---No-----+----->
|-----+-----|
| (1) (2) |
|'-Preview-----No---+'
|'-Yes-'
|
|-----+-----|
| (1) |
|'-DEVclass-----Einheitenklassenname-'
|
|.-Scratch---Yes-----+----->
|-----+-----|
| (2) |
|'-Scratch-----Yes---+'
|'-No--'
|
|-----+-----|
|-----+-----|
| (2) V-----+-----|
|'-VOLumenames-----+---Datenträgername---+'
|'-FILE:---Dateiname---+'
|
|-----+-----|
|'-USEDVolumelist---Dateiname-'
|
|.-ENCrptionstrength---AES-----+----->
|-----+-----|
|'-ENCrptionstrength---AES---+'

```

Anmerkungen:

1. Wenn PREVIEW=NO gilt, muss eine Einheitenklasse angegeben werden.
2. Wenn PREVIEW=NO und SCRATCH=NO gilt, müssen Datenträger angegeben werden.

## Parameter

---

### Administratorname

Gibt die Administratoren an, für die Informationen exportiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Administratoren.

Die Einträge in der Liste ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

### Preview

Gibt an, ob die Ergebnisse der Exportoperation vorangezeigt werden sollen, ohne die Informationen zu exportieren. Mit diesem Parameter kann der Umfang der zu übertragenden Daten (Byte) vorangezeigt und bestimmt werden, wie viele Datenträger erforderlich sind. Die folgenden Parameterwerte werden unterstützt:

#### No

Gibt an, dass die Administratorinformationen exportiert werden sollen. Wird dieser Wert angegeben, muss eine Einheitenklasse angegeben werden.

#### Yes

Gibt an, dass die Operation vorangezeigt, aber nicht ausgeführt wird. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet. Wird dieser Wert angegeben, muss keine Einheitenklasse angegeben werden.

Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

### DEVclass

Gibt die Einheitenklasse an, in die die Exportdaten geschrieben werden sollen. Dieser Parameter ist erforderlich, wenn Sie PREVIEW=NO angeben.

Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Exports aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, um ein Laufwerk verfügbar zu machen.

Tipp: Daten können in einen Speicherpool auf einem anderen Server exportiert werden, indem eine Einheitenklasse mit dem Einheitentyp SERVER angegeben wird.

### Scratch

Gibt an, ob Arbeitsdatenträger verwendet werden können. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

#### Yes

Gibt an, dass Arbeitsdatenträger zum Exportieren verwendet werden können. Wird auch eine Liste mit Datenträgern angegeben, werden Arbeitsdatenträger nur verwendet, wenn auf den angegebenen Datenträgern nicht genügend Speicherbereich vorhanden ist.

#### No

Gibt an, dass keine Arbeitsdatenträger zum Exportieren verwendet werden können. Um zu bestimmen, wie viele Datenträger benötigt werden, können Sie den Befehl mit der Angabe PREVIEW=YES ausführen.

### VOLumenames

Gibt die Datenträger an, die zum Speichern der exportierten Daten verwendet werden sollen. Dieser Parameter ist wahlfrei, es sei denn, es wird SCRATCH=NO und PREVIEW=NO angegeben. Wird kein Datenträgername angegeben, werden Arbeitsdatenträger verwendet.

Sie können einen der folgenden Werte angeben:

#### Datenträgername


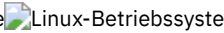
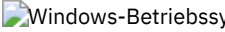


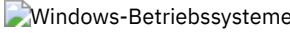

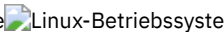
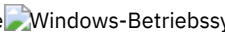
Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

#### FILE: Dateiname

Gibt den Namen einer Datei an, die eine Liste mit Datenträgern enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

Folgende Namenskonventionen bei der Angabe von Datenträgern verwenden, die folgenden Einheitentypen zugeordnet sind:



| Für Einheit  | Angeben   |
|--|---|
| Band   | 1 - 6 alphanumerische Zeichen.  |
| FILE   | Beliebige, vollständig qualifizierte Dateinamenzeichenfolge. Beispiel:<br>  Linux-Betriebssysteme/imdata/mt1.<br> Windows-Betriebssysteme:\Programdateien\tivoli\tsm\data1.dsm. |
| <br><br><br>REMOVABLEFILE |    Windows-Betriebssysteme1 - 6 alphanumerische Zeichen.  |
| SERVER   | 1 - 250 alphanumerische Zeichen.  |

#### USEDVolumelist

Gibt die Datei an, in der eine Liste der Datenträger gespeichert wird, die in der Exportoperation verwendet werden. Dieser Parameter ist wahlfrei.

Diese Datei kann für die Importoperation verwendet werden. Diese Datei enthält Kommentarzeilen mit dem Exportdatum und der Exportuhrzeit sowie dem Befehl, der zum Erstellen des Exports ausgegeben wurde.

Achtung: Wird eine vorhandene Datei angegeben, wird die Datei überschrieben.

#### ENCryptionstrength

Gibt an, welcher Algorithmus für die Verschlüsselung von Kennwörtern verwendet werden soll, wenn Verwaltungs- und Knotensätze exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist AES. Erfolgt der Export auf einen Server, der AES nicht unterstützt, geben Sie DES an. Sie können einen der folgenden Werte angeben:

AES

Gibt den Advanced Encryption Standard an.

DES

Gibt den Data Encryption Standard an.

## Beispiel: Administratordefinitionen auf Banddatenträger exportieren

Vom Server die Informationen für alle definierten Administratoren auf die Banddatenträger TAPE01, TAPE02 und TAPE03 exportieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist. Die Anzahl und die Typen der exportierten Objekte werden an die Systemkonsole und an das Aktivitätenprotokoll gemeldet. Den folgenden Befehl ausgeben:

```
export admin devclass=menu1
volumenames=tape01,tape02,tape03
```

## Beispiel: Administratordefinitionen auf Banddatenträger exportieren, die in einer Datei aufgelistet sind

Vom Server die Informationen für alle definierten Administratoren auf die Banddatenträger exportieren, die in der folgenden Datei aufgelistet sind:

-   TAPEVOL
-  TAPEVOL.DATA

Diese Datei enthält die folgenden Zeilen:

```
TAPE01
TAPE02
TAPE03
```

Angeben, dass diese Banddatenträger von einer Einheit verwendet werden, die der Einheitenklasse MENU1 zugeordnet ist. Den folgenden Befehl ausgeben:

```
export admin devclass=menu1 volumenames=file:tapevol
```



```
export admin devclass=menu1 volumenames=file:tapevol.data
```

Die Anzahl und die Typen der exportierten Objekte werden an die Systemkonsole und an das Aktivitätenprotokoll gemeldet.



Gibt an, ob Definitionen (nicht Dateidaten) auf dem Server ersetzt werden sollen. Der Standardwert ist NO.

Gültige Werte sind:

Yes

Gibt an, dass Definitionen auf dem Server ersetzt werden, wenn Definitionen mit demselben Namen wie die zu importierenden Definitionen auf dem Zielserver vorhanden sind.

No

Gibt an, dass importierte Definitionen übersprungen werden, wenn ihre Namen mit Definitionen in Konflikt stehen, die bereits auf dem Zielserver definiert sind.

ENCryptionstrength

Gibt an, welcher Algorithmus für die Verschlüsselung von Kennwörtern verwendet werden soll, wenn Verwaltungs- und Knotensätze exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist AES. Erfolgt der Export auf einen Server, der AES nicht unterstützt, geben Sie DES an. Sie können einen der folgenden Werte angeben:

AES

Gibt den Advanced Encryption Standard an.

DES

Gibt den Data Encryption Standard an.

## Beispiel: Administratordefinitionen auf einen Zielserver exportieren

---

Alle Administratordefinitionen auf den Zielserver exportieren, der als OTHERSERVER definiert ist. Die Importoperationen auf dem Zielserver voranzeigen. Den folgenden Befehl ausgeben:

```
export admin * toserver=otherserver previewimport=yes
```

Auf dem Zielserver OTHERSERVER können Sie die Importoperationen anzeigen, indem Sie folgenden Befehl ausgeben:

```
query process
```

## EXPORT NODE (Clientknoteninformationen exportieren)

---

Mit diesem Befehl können Clientknotendefinitionen oder Dateidaten auf sequenzielle Datenträger oder für den sofortigen Import auf einen anderen Server exportiert werden.

Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten exportiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls EXPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben. Die folgenden Informationen sind in jeder Clientknotendefinition enthalten:

- Benutzer-ID, Kennwort und Kontaktinformationen.
- Name der zugeordneten Maßnahmendomäne des Clients.
- Dateikomprimierungsstatus.
- Die Angabe, ob der Benutzer eine Berechtigung zum Löschen von gesicherten oder archivierten Dateien aus dem Serverspeicher hat.
- Die Angabe, ob der Serverzugriff auf die Clientknoten-ID gesperrt ist.

Wahlweise können auch folgende Elemente exportiert werden:

- Dateibereichsdefinitionen.
- Gesicherte Dateien, archivierte Dateien und Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.
- Zugriffsberechtigungsinformationen zu den exportierten Dateibereichen.
- Archivierungsdaten mit dem Status "Löschen unzulässig" (der Status wird beibehalten). Werden die Archivierungsdaten importiert, verbleiben sie im Status "Löschen unzulässig".

Wenn Sie einen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden, müssen alle Server, auf die exportiert wird, für LDAP-Kennwörter konfiguriert werden. Auf Knotendaten, die von einem Knoten exportiert werden, der sich mit einem LDAP-Verzeichnisserver authentifiziert, kann nicht zugegriffen werden, wenn der Zielserver nicht korrekt konfiguriert ist. Ist Ihr Zielserver nicht konfiguriert, können Daten von einem LDAP-Knoten dennoch exportiert werden. Der Zielserver muss jedoch für die Verwendung von LDAP konfiguriert werden, damit Sie auf die Daten zugreifen können.

Die folgenden Einschränkungen gelten für die Exportfunktion:

- Exportoperationen aus einer höheren Version und einem höheren Release in eine frühere Version und ein früheres Release werden nicht unterstützt.
- Exportoperationen zwischen Servern, die dieselbe Version und dasselbe Release, aber verschiedene Fixpacks aufweisen, können fehlschlagen. Beispielsweise können Sie keinen Export von einem Server der Version 7.1.3 auf einen Server der Version 7.1.1 oder einen früheren Server ausführen.
- Exportierte Daten von einem Server mit aktiviertem Aufbewahrungsschutz sind nicht durch Aufbewahrung geschützt, wenn sie auf einen anderen Server importiert werden.
- Die Exportverarbeitung schließt Knoten des Typs NAS (Network-attached Storage) aus.
- Das Exportieren von Daten in eine Centera-Einheitenklasse oder das Importieren von Daten aus einer Centera-Einheitenklasse wird nicht unterstützt. Dateien, die in Centera-Speicherpools gespeichert werden, können jedoch exportiert werden, und Dateien, die importiert werden müssen, können auf einer Centera-Speichereinheit gespeichert werden.
- Mit den Befehlen EXPORT NODE und EXPORT SERVER werden keine Daten aus einem Schredderpool exportiert, es sei denn, dies wird explizit zugelassen, indem der Parameter ALLOWSHREDDABLE auf YES gesetzt wird. Wenn dieser Wert angegeben wird und die exportierten Daten Daten aus Schredderpools einschließen, können diese Daten nicht geschreddert werden. Es wird keine Warnung ausgegeben, wenn die Exportoperation Daten aus Schredderpools einschließt.
- Das inkrementelle Exportieren oder Importieren der folgenden Typen von Clientdaten auf einen anderen IBM Spectrum Protect-Server wird nicht unterstützt:
  - VMware-Sicherungen, bei denen Gesamt- und Teilsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen
  - Sicherungsgruppen, bei denen Gesamt- und Differenzsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen
  - Windows-Systemstatusdaten, die periodisch, inkrementell auf einen anderen Server übertragen werden

Der vollständige Export oder Import dieser Daten in ein neues Dateisystem auf dem Ziel wird unterstützt, indem der gesamte Dateibereich, der die Daten enthält, exportiert wird. Bei dem Export darf nicht der Parameter FILEDATA=ALLACTIVE, FROMDATE, TODATE oder MERGEFILESPPACES verwendet werden.

Die Verwendung der Knotenreplikation zur inkrementellen Übertragung dieses Typs von Clientdaten zwischen zwei Servern ist optimal.

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

Der Befehl EXPORT NODE generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn Sie Knoteninformationen auf sequenzielle Datenträger exportieren und der Hintergrundprozess abgebrochen wird, sind die sequenziellen Datenträger, auf denen sich die exportierten Daten befinden, unvollständig und dürfen nicht zum Importieren von Daten verwendet werden. Wird ein Hintergrundprozess abgebrochen, bei dem Daten von einem Server auf einen anderen Server exportiert werden, kann dies zu einem Teilimport von Daten führen. Werten Sie alle importierten Daten auf dem Zielsystem aus, um zu bestimmen, ob die importierten Daten behalten oder gelöscht werden sollen. Überprüfen Sie die Importnachrichten auf Details. Um Informationen zu Hintergrundprozessen anzuzeigen, geben Sie den Befehl QUERY PROCESS aus.

Um Informationen zu aktiven und ausgesetzten Exportoperation zwischen Servern anzuzeigen, geben Sie den Befehl QUERY EXPORT aus. Mit dem Befehl QUERY EXPORT werden nur Informationen für Exporte angezeigt, die ausgesetzt sind oder ausgesetzt werden können. Exportoperationen, die ausgesetzt und dann erneut gestartet werden können, sind die Exportoperationen zwischen Servern, die einen anderen Wert für FILEDATA als NONE haben. Mit dem Befehl QUERY ACTLOG kann der Status der Exportoperation angezeigt werden.

Aufgrund unvorhersehbarer Ergebnisse führen Sie keine Verfallsverarbeitung, Umlagerung, Sicherung oder Archivierung aus, wenn Sie den Befehl EXPORT NODE ausgeben.

Bei einem Server, der über Clients mit Unterstützung für Unicode verfügt, kann der Server den Dateibereichsnamen konvertieren oder Sie können einen der folgenden Parameter verwenden:

- FSID
- UNIFILESPACE

Der Befehl EXPORT NODE hat zwei Formen: Zum Exportieren von Daten direkt auf einen anderen Server in dem Netz oder zum Exportieren von Daten auf sequenzielle Datenträger. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für EXPORT NODE





Gibt die Dateibereiche an, für die Daten exportiert werden sollen. Dieser Parameter ist wahlfrei. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Einschränkung: Wenn ein Dateibereich angegeben wird, werden Unicode-fähige Dateibereiche nicht exportiert.

#### FSID

Gibt die Dateibereiche an, indem ihre Dateibereichs-IDs (File Space IDs = FSIDs) verwendet werden. Der Server verwendet die FSIDs zum Lokalisieren der Dateibereiche, die exportiert werden sollen. Zum Lokalisieren der FSID eines Dateibereichs verwenden Sie den Befehl QUERY FILESPACE. Mehrere Dateibereichs-IDs müssen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Dieser Parameter ist wahlfrei.

#### UNIFILESpace

Gibt die Dateibereiche an, die dem Server als Unicode-aktiviert bekannt sind. Der Server konvertiert die Namen, die Sie eingeben, aus der Zeichenumsetztabelle des Servers in die Zeichenumsetztabelle UTF-8, um die Dateibereiche zu lokalisieren, die exportiert werden sollen. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es kann ein Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Dieser Parameter ist wahlfrei.

#### DOMains

Gibt die Maßnahmendomänen an, aus denen Knoten exportiert werden sollen. Dieser Parameter ist wahlfrei. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Werden Domänen angegeben, wird ein Knoten nur exportiert, wenn er zu einer der angegebenen Domänen gehört. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.

#### FILEData

Gibt den Typ der Dateien an, die für alle Knoten exportiert werden sollen, die auf den Server exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NONE.

Anmerkung: Wenn Sie einen Knoten exportieren, der über Gruppendaten verfügt, werden möglicherweise Daten exportiert, die nicht Teil der Zielobjekte sind. Beispiele für Gruppendaten sind Daten virtueller Maschinen und Systemstatussicherungsdaten. Wird beispielsweise bei FILEDATA=BACKUPACTIVE der Parameter FROMDATE oder TODATE angegeben, ist es möglich, dass inaktive Sicherungsdaten eingeschlossen werden. Die Teilsicherungsverarbeitung für die Daten kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden.

Export auf sequenzielle Datenträger: Die von den Dateidaten verwendete Einheitenklasse wird durch die Einheitenklasse des Speicherpools bestimmt. Handelt es sich um dieselbe Einheitenklasse wie in diesem Befehl, werden zum Exportieren von Knoteninformationen zwei Laufwerke benötigt. Das Mountlimit für die Einheitenklasse muss mindestens 2 betragen.

Wichtig: Werden Clientknoten exportiert, die als TYPE=SERVER registriert sind, ALL, ARCHIVE oder ALLACTIVE angeben.

In den folgenden Beschreibungen werden *aktive* und *inaktive* Versionen von Sicherungsdateien erwähnt. Eine aktive Version einer Sicherungsdatei ist die aktuellste Sicherungsversion für eine Datei, die noch auf der Client-Workstation vorhanden ist. Alle anderen Versionen der Sicherungsdatei werden als inaktive Kopien bezeichnet. Dieser Parameter unterstützt die folgenden Werte:

#### ALL

Der Server exportiert alle Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

#### None

Der Server exportiert keine Dateien, nur Knotendefinitionen.

#### ARchive

Der Server exportiert nur archivierte Dateien.

#### Backup

Der Server exportiert nur Sicherungsversionen, unabhängig davon, ob sie aktiv oder inaktiv sind.

#### BACKUPActive

Der Server exportiert nur aktive Sicherungsversionen. Diese aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl EXPORT ausgegeben wird.

#### ALLActive

Der Server exportiert alle aktiven Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden. Die aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl EXPORT ausgegeben wird.

#### SPAcemanaged

Der Server exportiert nur Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

#### Preview

Gibt an, ob die Ergebnisse der Exportoperation vorangezeigt werden sollen, ohne die Informationen zu exportieren. Mit diesem Parameter kann der Umfang der zu übertragenden Daten (Byte) vorangezeigt werden, um zu bestimmen, wie viele Datenträger benötigt werden. Dieser Parameter unterstützt die folgenden Werte:

#### No

Gibt an, dass die Knoteninformationen exportiert werden sollen. Wird dieser Wert angegeben, muss auch eine Einheitenklasse angegeben werden.

#### Yes

Gibt an, dass die Operation vorangezeigt, aber nicht ausgeführt wird. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet. Wird dieser Wert angegeben, muss keine Einheitenklasse angegeben werden.

Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

#### DEVclass

Gibt die Einheitenklasse an, in die die Exportdaten geschrieben werden sollen. Dieser Parameter ist erforderlich, wenn Sie PREVIEW=NO angeben.

Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Exports aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, um ein Laufwerk verfügbar zu machen.

Tipp: Daten können in einen Speicherpool auf einem anderen Server exportiert werden, indem eine Einheitenklasse mit dem Einheitentyp SERVER angegeben wird.

#### Scratch

Gibt an, ob Arbeitsdatenträger verwendet werden können. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

##### Yes

Gibt an, dass Arbeitsdatenträger zum Exportieren verwendet werden können. Wird auch eine Liste mit Datenträgern angegeben, werden Arbeitsdatenträger nur verwendet, wenn auf den angegebenen Datenträgern nicht genügend Speicherbereich vorhanden ist.

##### No

Gibt an, dass keine Arbeitsdatenträger zum Exportieren verwendet werden können. Um zu bestimmen, wie viele Datenträger benötigt werden, können Sie den Befehl mit der Angabe PREVIEW=YES ausführen.

#### VOLumenames

Gibt die Datenträger an, die zum Speichern der exportierten Daten verwendet werden sollen. Dieser Parameter ist wahlfrei, es sei denn, es wird SCRATCH=NO und PREVIEW=NO angegeben. Wird kein Datenträgername angegeben, werden Arbeitsdatenträger verwendet.

Sie können einen der folgenden Werte angeben:










##### Datenträgername

Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

##### FILE: Dateiname

Gibt den Namen einer Datei an, die eine Liste mit Datenträgern enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

Folgende Namenskonventionen bei der Angabe von Datenträgern verwenden, die folgenden Einheitentypen zugeordnet sind:

| Für Einheit  | Angeben  |
|--|--|
| Band   | 1 - 6 alphanumerische Zeichen.   |
| FILE   | Beliebige, vollständig qualifizierte Dateinamenzeichenfolge. Beispiel:<br> AIX-Betriebssysteme  Linux-Betriebssysteme/imdata/mt1.<br> Windows-Betriebssysteme:\Programdateien\tivoli\tsm\data1.dsm. |
|  AIX-Betriebssysteme<br> Linux-Betriebssysteme<br> Windows-Betriebssysteme<br>REMOVABLEFILE |  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme1 - 6 alphanumerische Zeichen.  |
| SERVER   | 1 - 250 alphanumerische Zeichen.   |

#### USEDVolumelist

Gibt die Datei an, in der eine Liste der Datenträger gespeichert wird, die in der Exportoperation verwendet werden. Dieser Parameter ist wahlfrei.

Diese Datei kann für die Importoperation verwendet werden. Diese Datei enthält Kommentarzeilen mit dem Exportdatum und der Exportuhrzeit sowie dem Befehl, der zum Erstellen des Exports ausgegeben wurde.

Achtung: Wird eine vorhandene Datei angegeben, wird die Datei überschrieben.

#### FROMDate

Gibt das früheste Datum an, für das Dateien, die exportiert werden sollen, auf dem Server gespeichert wurden. Dateien, die vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. Dieser Parameter gilt nur für



Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter FROMDATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Verzeichnisverarbeitung: Der Parameter FROMDATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.

Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Gruppendaten auf dem Knoten sind beispielsweise Daten virtueller Maschinen oder Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 09/15/1998   |
| TODAY                          | Das aktuelle Datum   | TODAY  |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY -3 <b>oder</b> -3.   |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

Wird dieser Parameter nicht angegeben, exportiert IBM Spectrum Protect alle Objekte, die vor dem Datum im Parameter TODATE gespeichert wurden und die durch den Parameter FILEDATA qualifiziert sind. Wird kein Parameter TODATE angegeben, werden alle Daten exportiert, die durch den Parameter FILEDATA qualifiziert sind.

Wenn eine Exportoperation zwischen Servern ein relatives FROMDATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird FROMDATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und zehn Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

#### TODate

Gibt das späteste Datum für Dateien an, die vom Server exportiert werden sollen. Dateien, die auf dem Server an einem späteren Datum als dem für TODATE angegebenen Datum gespeichert werden, werden nicht exportiert. TODATE gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen.

- IBM Spectrum Protect ignoriert den Parameter TODATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.
- Wenn ein Parameter TODATE ohne einen Parameter TOTIME angegeben wird, exportiert der Server alle Objekte, die an oder vor dem durch den Parameter TODATE angegebenen Tag eingefügt wurden.
- Wurde der Parameter FROMDATE angegeben, muss der Wert von TODATE größer-gleich dem Wert von FROMDATE sein. Sind TODATE und FROMDATE gleich, muss der Wert für den Parameter TOTIME größer als der Wert für den Parameter FROMTIME sein.
- Der Parameter TODATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.

Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die nach dem Datum oder der Zeit im Parameter TODATE oder TOTIME gesichert wurden, exportiert werden. Beispiele für Gruppendaten sind Daten virtueller Maschinen und Systemstatussicherungsdaten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 10/15/2006   |
| TODAY                          | Das aktuelle Datum   | TODAY  |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY -3 <b>oder</b> -3.   |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

Wenn eine Exportoperation zwischen Servern ein relatives TODATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird TODATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und 10 Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

#### FROMTime

Gibt die früheste Uhrzeit an, für die Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Geben Sie FROMTIME an, müssen Sie auch den Parameter FROMDATE verwenden. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. Objekte, die vor der angegebenen Uhrzeit und vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. IBM Spectrum Protect ignoriert den Parameter FROMTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Beispiele für Gruppendaten auf dem Knoten sind Daten virtueller Maschinen und Systemstausicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Bei Verwendung mit dem Parameter FROMDATE lautet der Standardwert für diesen Parameter Mitternacht (00:00:00).

Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

| Wert                         | Beschreibung   | Beispiel  |
|------------------------------|--|---|
| HH:MM:SS                     | Eine bestimmte Uhrzeit   | 10:30:08  |
| NOW                          | Die aktuelle Uhrzeit   | NOW   |
| NOW+HH:MM <b>oder</b> +HH:MM | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten. FROMTIME+ kann nur mit einem FROMDATE vor heute verwendet werden. | NOW+02:00 <b>oder</b> +02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW+02:00 oder FROMTIME=+02:00 ausgegeben, enthält die Exportoperation nur Dateien, die nach 7:00 Uhr an dem angegebenen FROMDATE auf den Server gestellt wurden. |
| NOW-HH:MM <b>oder</b> -HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten   | NOW -02:00 <b>oder</b> -02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW-02:00 oder FROMTIME=-2:00 ausgegeben, enthält der Export Dateien, die nach 3:00 Uhr auf den Server gestellt wurden.  |

## TOTime

Gibt den spätesten Zeitpunkt an, an dem Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Sie müssen den Parameter TODATE angeben, um den Parameter TOTIME verwenden zu können. TOTIME gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter TOTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Bei Verwendung mit dem Parameter TODATE lautet der Standardwert für diesen Parameter Mitternacht minus eine Sekunde (23:59:59).

Wichtig: Die Werte für die Parameter TOTIME und TODATE müssen größer als die Werte für die Parameter FROMDATE und FROMTIME sein.

Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

| Wert                             | Beschreibung  | Beispiel  |
|----------------------------------|---|---|
| HH:MM:SS                         | Eine bestimmte Uhrzeit  | 10:30:08  |
| NOW+HH:MM <b>oder</b><br>+HH:MM  | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.  | NOW+02:00 <b>oder</b> +02:00.<br><br>Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW+02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 7 Uhr gespeichert wurden. |
| NOW-HH:MM <b>oder</b> -<br>HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten. | NOW-02:00 <b>oder</b> -02:00.<br><br>Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW-02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 3 Uhr gespeichert wurden. |

## ENCryptionstrength

Gibt an, welcher Algorithmus für die Verschlüsselung von Kennwörtern verwendet werden soll, wenn Verwaltungs- und Knotensätze exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist AES. Erfolgt der Export auf einen Server, der AES nicht unterstützt, geben Sie DES an. Sie können einen der folgenden Werte angeben:

AES

Gibt den Advanced Encryption Standard an.

DES

Gibt den Data Encryption Standard an.

## ALLOWSHREDdable

Gibt an, ob Daten aus einem Speicherpool, der das Schreddern erzwingt, exportiert werden. Dieser Parameter unterstützt die folgenden Werte:

No

Gibt an, dass Daten nicht aus einem Speicherpool exportiert werden, der das Schreddern erzwingt.

Yes

Gibt an, dass Daten aus einem Speicherpool exportiert werden können, der das Schreddern erzwingt. Die Daten auf den Exportdatenträgern werden nicht geschreddert.

Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

## Beispiel: Clientknoteninformationen auf bestimmte Banddatenträger exportieren

Vom Server Clientknoteninformationen auf die Banddatenträger TAPE01, TAPE02 und TAPE03 exportieren. Angeben, dass diese Banddatenträger von einer Einheit verwendet werden, die der Einheitenklasse MENU1 zugeordnet ist.

```
export node devclass=menu1 volumenames=tape01,tape02,tape03
```

## Beispiel: Clientknoteninformationen unter Verwendung der FSID exportieren

Verwenden Sie auf dem Server die FSID, um aktive Sicherungsversionen der Dateidaten für Clientknoten JOE auf den Banddatenträger TAPE01 zu exportieren. Um die FSID zu bestimmen, geben Sie zuerst einen Befehl QUERY FILESPACE aus.

- Um die FSID zu bestimmen, geben Sie einen Befehl QUERY FILESPACE aus.

```
query filespace joe
```

```
Knotenname Dateibe- FSID Platt- Dateibe- Ist Kapazi- %  
reichsname form reichstyp Dateiber. tät (MB) Ausl.
```

|     |           |   |       |      | Unicode? |         |      |
|-----|-----------|---|-------|------|----------|---------|------|
| JOE | \\joe\c\$ | 1 | WinNT | NTFS | Yes      | 2.502,3 | 75,2 |
| JOE | \\joe\d\$ | 2 | WinNT | NTFS | Yes      | 6.173,4 | 59,6 |

- Exportieren Sie die aktiven Sicherungsversionen der Dateidaten und geben Sie an, dass der Banddatenträger von einer Einheit verwendet wird, die der Einheitenklasse MENU1 zugeordnet ist.

```
export node joe fsid=1,2 filedata=backupactive devclass=menu1
volumenames=tape01
```

## Beispiel: Clientknoteninformationen auf Banddatenträger exportieren, die in einer Datei aufgelistet sind

Vom Server die Clientknoteninformationen auf Banddatenträger exportieren, die in der folgenden Datei aufgelistet sind:

-  Linux-BetriebssystemeTAPEVOL
-  Windows-BetriebssystemeTAPEVOL.DATA


Die Datei enthält die folgenden Zeilen:

```
TAPE01
TAPE02
TAPE03
```

Angeben, dass die Banddatenträger von einer Einheit verwendet werden, die der Einheitenklasse MENU1 zugeordnet ist. Geben Sie den folgenden Befehl aus:

 Linux-Betriebssysteme

```
export node devclass=menu1 volumenames=file:tapevol
```

 Windows-Betriebssysteme

```
export node devclass=menu1 volumenames=file:tapevol.data
```

## EXPORT NODE (Knotendefinitionen oder Dateidaten direkt auf einen anderen Server exportieren)

Mit diesem Befehl können Clientknotendefinitionen oder Dateidaten für den sofortigen Import direkt auf einen anderen Server exportiert werden.

Wichtig: Knoten des Typs NAS können nicht exportiert werden. Die Exportverarbeitung schließt diese Knoten aus.

Sie können eine Exportoperation zwischen Servern, die einen anderen Wert als NONE für FILEDATA hat, aussetzen und erneut starten. Der Server sichert den Status der Exportoperation, sodass die Exportoperation an dem Punkt erneut gestartet werden kann, an dem sie fehlgeschlagen ist oder ausgesetzt wurde. Die Exportoperation kann zu einem späteren Zeitpunkt erneut gestartet werden, indem der Befehl RESTART EXPORT ausgegeben wird.

Wichtig: Eine Exportoperation wird ausgesetzt, wenn eine der folgenden Bedingungen festgestellt wird:

- Ein Befehl SUSPEND EXPORT wird für die aktive Exportoperation ausgegeben
- Segmentvorableerung - die Datei, die für den Export gelesen wird, wird von einem anderen Prozess gelöscht
- Übertragungsfehler bei einem Export zwischen Servern
- Keine verfügbaren Mountpunkte
- Erforderliche Datenträger sind nicht verfügbar
- E/A-Fehler wurden festgestellt

Mit dem Befehl QUERY EXPORT können Informationen zu allen aktiven und ausgesetzten Exportoperationen angezeigt werden.

Die Exportoperation kann nicht erneut gestartet werden, wenn die Exportoperation fehlschlägt, bevor die auswählbaren Knoten- und Dateibereichsdefinitionen auf den Zielservers übertragen werden. Sie müssen den Befehl erneut eingeben, um eine neue Exportoperation zu beginnen.

Sie können einen Befehl QUERY PROCESS auf dem Zielservers ausgeben, um den Fortschritt der Importoperation zu überwachen. Geben Sie den Befehl QUERY EXPORT aus, um alle wiederanlaufähigen Exportoperationen zwischen Servern aufzulisten. In EXPORT ADMIN (Administratorinformationen exportieren) finden Sie eine Liste der Einschränkungen, die für die Exportfunktion gelten.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
.-*-----.  
>>-EXPort Node-----+----->  
      '-Knotenname-'  
  
>+-----+----->  
      '-FILESpace----Dateibereichsname-'  
  
>+-----+----->  
      '-FSID----Dateibereichs-ID-'  
  
>+-----+----->  
      '-UNIFILESpace----Dateibereichsname-'  
  
>+-----+----->  
      '-DObains----Domänennamen-'  
  
      .-FILEData----None-----.  
>+-----+----->  
      '-FILEData----+All-----+'  
                +-None-----+  
                +-ARchive-----+  
                +-Backup-----+  
                +-BACKUPActive+  
                +-ALLActive----+  
                '-SPacemanaged-'  
  
>+-----+----->  
      |                .-FROMTime----00:00:00-. |  
      '-FROMDate----Datum-----+-----+  
                '-FROMTime----Zeit-----'  
  
>+-----+----->  
      |                .-TOTime----23:59:59-. |  
      '-TODate----Datum-----+-----+  
                '-TOTime----Zeit-----'  
  
>+-----+----->  
      '-EXPORTIDentifier----Export-ID-'  
  
                .-PREVIEWImport----No-----.  
>+-----+-----+----->  
      '-TOServer----Servername- ' '-PREVIEWImport----+No--+-'  
                '-Yes-'  
  
      .-MERGEfilespace----No-----.  
>+-----+-----+----->  
      '-MERGEfilespace----+No--+-'  
                '-Yes-'  
  
      .-Replacedefs----No-----.  
>+-----+-----+----->  
      '-Replacedefs----+No--+-'  
                '-Yes-'  
  
      .-PROXynodeassoc----No-----.  
>+-----+-----+----->  
      '-PROXynodeassoc----+No--+-'  
                '-Yes-'  
  
      .-ENCryptionstrength----AES-----.  
>+-----+-----+----->  
      '-ENCryptionstrength----+AES--+-'  
                '-DES-'  
  
      .-ALLOWSHREddable----No-----.  
>+-----+-----+----->  
      '-ALLOWSHREddable----+No--+-'  
                '-Yes-'
```

## Parameter

#### Knotenname

Gibt die Namen der Clientknoten an, für die Informationen exportiert werden sollen. Dieser Parameter ist wahlfrei. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Für jeden eingegebenen Knoten werden alle Dateibereiche in den Dateibereichs-, FSID- und Unicode-aktivierten Listen durchsucht.

Einschränkung: Wenn Sie eine Liste der Knotennamen oder Knotenmuster angeben, meldet der Server keine Knotennamen oder Knotenmuster zurück, die nicht mit Einträgen in der Datenbank übereinstimmen. Überprüfen Sie die zusammenfassende Statistik im Aktivitätenprotokoll, um sicherzustellen, dass der Server alle gewünschten Knoten exportiert hat.

#### FILESpace

Gibt die Dateibereiche an, für die Daten exportiert werden sollen. Dieser Parameter ist wahlfrei. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.

Einschränkung: Wenn ein Dateibereich angegeben wird, werden keine Unicode-fähigen Dateibereiche exportiert.

#### FSID

Gibt die Dateibereiche an, indem ihre Dateibereichs-IDs (File Space IDs = FSIDs) verwendet werden. Der Server verwendet die FSIDs zum Lokalisieren der Dateibereiche, die exportiert werden sollen. Zum Lokalisieren der FSID eines Dateibereichs verwenden Sie den Befehl QUERY FILESPACE. Mehrere Dateibereichs-IDs müssen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Dieser Parameter ist wahlfrei.

#### UNIFILESpace

Gibt die Dateibereiche an, die dem Server als Unicode-aktiviert bekannt sind. Der Server konvertiert die Namen, die Sie eingeben, aus der Zeichenumsetztabelle des Servers in die Zeichenumsetztabelle UTF-8, um die Dateibereiche zu lokalisieren, die exportiert werden sollen. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es kann ein Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Dieser Parameter ist wahlfrei.

#### Domains

Gibt die Maßnahmendomänen an, aus denen Knoten exportiert werden. Dieser Parameter ist wahlfrei. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Wenn Sie Domänen angeben, exportiert IBM Spectrum Protect einen Knoten nur dann, wenn er zu einer der angegebenen Domänen gehört. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.

#### FILEData

Gibt den Typ der Dateien an, die für alle Knoten exportiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NONE.

Anmerkung: Wenn Sie einen Knoten exportieren, der über Gruppendaten verfügt, werden möglicherweise Daten exportiert, die nicht Teil der Zielobjekte sind. Beispiele für Gruppendaten sind Daten virtueller Maschinen und Systemstattsicherungsdaten. Wird beispielsweise bei FILEDATA=BACKUPACTIVE der Parameter FROMDATE oder TODATE angegeben, ist es möglich, dass inaktive Sicherungsdaten eingeschlossen werden. Die Teilsicherungsverarbeitung für die Daten kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden.

Wenn der Export auf sequenzielle Datenträger erfolgt, wird die von den Dateidaten verwendete Einheitenklasse durch die Einheitenklasse des Speicherpools bestimmt. Wenn es sich um dieselbe Einheitenklasse wie in diesem Befehl handelt, benötigt IBM Spectrum Protect zwei Laufwerke zum Exportieren von Knoteninformationen. Das Mountlimit für die Einheitenklasse muss mindestens 2 betragen.

Wichtig: Wenn Sie Clientknoten exportieren, die als TYPE=SERVER registriert sind, geben Sie ALL, ARCHIVE oder ALLACTIVE an. In den folgenden Beschreibungen werden *aktive* und *inaktive* Versionen von Sicherungsdateien erwähnt. Eine aktive Version einer Sicherungsdatei ist die aktuellste Sicherungsversion für eine Datei, die noch auf der Client-Workstation vorhanden ist. Alle anderen Versionen der Sicherungsdatei werden als inaktive Kopien bezeichnet. Folgende Werte sind verfügbar:

#### ALL

Der Server exportiert alle Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert werden.

#### None

Der Server exportiert keine Dateien, nur Knotendefinitionen.

#### ARchive

Der Server exportiert nur archivierte Dateien.

#### Backup

Der Server exportiert nur Sicherungsversionen, unabhängig davon, ob sie aktiv oder inaktiv sind.

#### BACKUPActive

Der Server exportiert nur aktive Sicherungsversionen. Diese aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl EXPORT ausgegeben wird.

#### ALLActive

Der Server exportiert alle aktiven Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden. Die aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl EXPORT ausgegeben wird.

#### SPAcemanaged

Der Server exportiert nur Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

## FROMDate

Gibt das früheste Datum an, für das Dateien, die exportiert werden sollen, auf dem Server gespeichert wurden. Dateien, die vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter FROMDATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Verzeichnisverarbeitung: Der Parameter FROMDATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.

Wichtig: Befinden sich Gruppdaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Gruppdaten auf dem Knoten sind beispielsweise Daten virtueller Maschinen oder Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 09/15/1998   |
| TODAY                          | Das aktuelle Datum   | TODAY  |
| TODAY-Tage oder -Tage          | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY -3 oder -3.  |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

Wird dieser Parameter nicht angegeben, exportiert IBM Spectrum Protect alle Objekte, die vor dem Datum im Parameter TODATE gespeichert wurden und die durch den Parameter FILEDATA qualifiziert sind. Wird kein Parameter TODATE angegeben, werden alle Daten exportiert, die durch den Parameter FILEDATA qualifiziert sind.

Wenn eine Exportoperation zwischen Servern ein relatives FROMDATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird FROMDATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und zehn Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

## TODate

Gibt das späteste Datum für Dateien an, die vom Server exportiert werden sollen. Dateien, die auf dem Server an einem späteren Datum als dem für TODATE angegebenen Datum gespeichert werden, werden nicht exportiert. TODATE gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen.

- IBM Spectrum Protect ignoriert den Parameter TODATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.
- Wenn ein Parameter TODATE ohne einen Parameter TOTIME angegeben wird, exportiert der Server alle Objekte, die an oder vor dem durch den Parameter TODATE angegebenen Tag eingefügt wurden.
- Wurde der Parameter FROMDATE angegeben, muss der Wert von TODATE größer-gleich dem Wert von FROMDATE sein. Sind TODATE und FROMDATE gleich, muss der Wert für den Parameter TOTIME größer als der Wert für den Parameter FROMTIME sein.
- Der Parameter TODATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.

Wichtig: Befinden sich Gruppdaten auf dem Knoten, den Sie exportieren, können Daten, die nach dem Datum oder der Zeit im Parameter TODATE oder TOTIME gesichert wurden, exportiert werden. Beispiele für Gruppdaten sind Daten virtueller

Maschinen und Systemstatussicherungsdaten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 10/15/2006   |
| TODAY                          | Das aktuelle Datum   | TODAY  |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY -3 <b>oder</b> -3.   |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

Wenn eine Exportoperation zwischen Servern ein relatives TODATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird TODATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und 10 Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

#### FROMTime

Gibt die früheste Uhrzeit an, für die Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Geben Sie FROMTIME an, müssen Sie auch den Parameter FROMDATE verwenden. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. Objekte, die vor der angegebenen Uhrzeit und vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. IBM Spectrum Protect ignoriert den Parameter FROMTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Wichtig: Befinden sich Gruppensicherungsdaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Beispiele für Gruppensicherungsdaten auf dem Knoten sind Daten virtueller Maschinen und Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Bei Verwendung mit dem Parameter FROMDATE lautet der Standardwert für diesen Parameter Mitternacht (00:00:00).

Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

| Wert                         | Beschreibung  | Beispiel  |
|------------------------------|---|---|
| HH:MM:SS                     | Eine bestimmte Uhrzeit  | 10:30:08  |
| NOW                          | Die aktuelle Uhrzeit  | NOW   |
| NOW+HH:MM <b>oder</b> +HH:MM | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.FROMTIME+ kann nur mit einem FROMDATE vor heute verwendet werden. | NOW+02:00 <b>oder</b> +02:00.<br>Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW+02:00 oder FROMTIME=+02:00 ausgegeben, enthält die Exportoperation nur Dateien, die nach 7:00 Uhr an dem angegebenen FROMDATE auf den Server gestellt wurden. |



| Wert                         | Beschreibung   | Beispiel   |
|------------------------------|--|--|
| NOW-HH:MM <b>oder</b> -HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten | NOW -02:00 <b>oder</b> -02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW-02:00 oder FROMTIME=-2:00 ausgegeben, enthält der Export Dateien, die nach 3:00 Uhr auf den Server gestellt wurden. |

#### TOTime

Gibt den spätesten Zeitpunkt an, an dem Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Sie müssen den Parameter TODATE angeben, um den Parameter TOTIME verwenden zu können. TOTIME gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter TOTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Bei Verwendung mit dem Parameter TODATE lautet der Standardwert für diesen Parameter Mitternacht minus eine Sekunde (23:59:59).

Wichtig: Die Werte für die Parameter TOTIME und TODATE müssen größer als die Werte für die Parameter FROMDATE und FROMTIME sein.

Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

| Wert                         | Beschreibung  | Beispiel  |
|------------------------------|---|---|
| HH:MM:SS                     | Eine bestimmte Uhrzeit  | 10:30:08  |
| NOW+HH:MM <b>oder</b> +HH:MM | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.  | NOW+02:00 <b>oder</b> +02:00.<br><br>Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW+02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 7 Uhr gespeichert wurden. |
| NOW-HH:MM <b>oder</b> -HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten. | NOW-02:00 <b>oder</b> -02:00.<br><br>Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW-02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 3 Uhr gespeichert wurden. |

#### TOServer

Gibt den Namen eines Servers an, an den die Exportdaten direkt über das Netz für den sofortigen Import gesendet werden.

Wichtig: Der Zielservers muss mit dem Befehl DEFINE SERVER auf dem Ursprungsserver definiert werden. Der Administrator, der den Exportbefehl ausgibt, muss mit demselben Administratorknamen und demselben Kennwort definiert werden und muss auf dem Zielservers über die Systemberechtigung verfügen.

Wenn Sie TOSERVER angeben, können Sie nicht die Parameter DEVCLASS, VOLUMENAMES, SCRATCH, USEDVOLUMELIST und PREVIEW angeben.

#### PREVIEWImport

Gibt an, ob der Umfang der zu übertragenden Daten angezeigt werden soll, ohne die Daten tatsächlich zu versetzen. Mit diesen Informationen kann bestimmt werden, welcher Speicherpoolbereich auf dem Zielservers benötigt wird. Der Standardwert ist NO. Gültige Werte sind:

Yes

Gibt an, dass die Ergebnisse der Importoperation auf dem Zielservers vorangezeigt werden sollen, ohne dass die Daten importiert werden. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet.

No

Gibt an, dass die Daten in den Zielservers importiert werden sollen, ohne dass die Ergebnisse vorangezeigt werden.

#### MERGEfilespace

Gibt an, ob IBM Spectrum Protect Clientdateien in vorhandene Dateibereiche auf dem Zielservers mischt (sofern sie vorhanden sind) oder ob IBM Spectrum Protect neue Dateibereichsnamen generiert. Der Standardwert ist NO.

Gültige Werte sind:

Yes

Gibt an, dass importierte Daten auf dem Zielservers in den vorhandenen Dateibereich gemischt werden, wenn ein Dateibereich mit demselben Namen auf dem Zielservers vorhanden ist.

No

Gibt an, dass IBM Spectrum Protect einen neuen Dateibereichsnamen für importierte Daten auf dem Zielserver generiert, wenn Dateibereiche mit demselben Namen vorhanden sind.

#### Replacedefs

Gibt an, ob Definitionen (nicht Dateidaten) auf dem Server ersetzt werden sollen. Der Standardwert ist NO.

Gültige Werte sind:

Yes

Gibt an, dass Definitionen auf dem Server ersetzt werden, wenn Definitionen mit demselben Namen wie die zu importierenden Definitionen auf dem Zielserver vorhanden sind.

No

Gibt an, dass importierte Definitionen übersprungen werden, wenn ihre Namen mit Definitionen in Konflikt stehen, die bereits auf dem Zielserver definiert sind.

#### PROXynodeassoc

Gibt an, ob Proxyknotenzuordnungen exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

#### ENCryptionstrength

Gibt an, welcher Algorithmus für die Verschlüsselung von Kennwörtern verwendet werden soll, wenn Verwaltungs- und Knotensätze exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist AES. Erfolgt der Export auf einen Server, der AES nicht unterstützt, geben Sie DES an. Sie können einen der folgenden Werte angeben:

AES

Gibt den Advanced Encryption Standard an.

DES

Gibt den Data Encryption Standard an.

#### ALLOWSHREDDable

Gibt an, ob Daten aus einem Speicherpool, der das Schreddern erzwingt, exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, dass der Server keine Daten aus einem Speicherpool exportiert, der das Schreddern erzwingt.

Yes

Gibt an, dass der Server Daten aus einem Speicherpool exportiert, der das Schreddern erzwingt. Die Daten auf den Exportdatenträgern werden nicht geschreddert.

Einschränkung: Nachdem eine Exportoperation die Identifizierung von Dateien für den Export beendet hat, werden alle Änderungen des Werts ALLOWSHREDABLE für den Speicherpool ignoriert. Eine Exportoperation, die ausgesetzt ist, behält während der gesamten Operation den ursprünglichen Wert für ALLOWSHREDABLE. Möglicherweise möchten Sie Ihre Exportoperation abbrechen, wenn Änderungen des Werts ALLOWSHREDABLE für den Speicherpool die Operation gefährden. Sie können den Exportbefehl nach einer erforderlichen Bereinigung erneut ausgeben.

#### EXPORTIDentifier

Dieser optionale Parameter gibt den Namen an, den Sie zum Identifizieren dieser Exportoperation auswählen. Geben Sie keine ID an, wird vom Server eine ID generiert. Die Export-ID darf 64 Zeichen nicht überschreiten, darf keine Platzhalterzeichen enthalten und ist nicht von der Groß-/Kleinschreibung abhängig. Mit dieser ID können Sie auf Exportoperationen in den Befehlen QUERY EXPORT, SUSPEND EXPORT, RESTART EXPORT oder CANCEL EXPORT verweisen.

Einschränkung: Sie müssen den Parameter TOSERVER angeben, wenn Sie den Parameter EXPORTIDENTIFIER angeben.

EXPORTIDENTIFIER wird bei FILEDATA=NONE ignoriert.

## Beispiel: Clientknoteninformationen und alle Clientdateien exportieren

---

Um Clientknoteninformationen und alle Clientdateien für NODE1 direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus:

```
export node node1 filedata=all toserver=serverb
```

## Beispiel: Clientknoteninformationen und alle Clientdateien für einen bestimmten Datumsbereich exportieren

---

Um Clientknoteninformationen und alle Clientdateien für NODE1 zwischen dem 1. Februar 2009 und heute direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus.

```
export node node1 filedata=all toserver=serverb  
fromdate=02/01/2009 todate=today
```

## Beispiel: Clientknoteninformationen und alle Clientdateien für einen bestimmten Datums- und Zeitbereich exportieren

---

Um Clientknoteninformationen und alle Clientdateien für NODE1 zwischen dem 1. Februar 2009 um 8 Uhr bis heute um 8 Uhr direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus:

```
export node node1 filedata=all toserver=serverb
fromdate=02/01/2009 fromtime=08:00:00
todate=today totime=08:00:00
```

## Beispiel: Clientknoteninformationen und alle Clientdateien für die letzten drei Tage exportieren

Um Clientknoteninformationen und alle Clientdateien für NODE1 für die letzten drei Tage direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus:

```
export node node1 filedata=all toserver=serverb
fromdate=today -3
```

## EXPORT POLICY (Maßnahmeninformationen exportieren)

Mit diesem Befehl können Maßnahmeninformationen von einem IBM Spectrum Protect-Server auf sequenzielle Datenträger oder für den sofortigen Import direkt auf einen anderen Server exportiert werden. Wenn eine Maßnahme mit dem Befehl EXPORT POLICY exportiert wird, werden die aktiven Datenpoolinformationen in der Domäne nicht exportiert.

Der Server exportiert folgende Maßnahmeninformationen:

- Maßnahmendomänendefinitionen
- Maßnahmengruppendefinitionen, einschließlich der aktiven Maßnahmengruppe
- Verwaltungsklassendefinitionen, einschließlich der Standardverwaltungsklasse
- Sicherungskopiergruppen- und Archivierungskopiergruppendefinitionen
- Zeitplandefinitionen für jede Maßnahmendomäne
- Client-Knotenzuordnungen, wenn der Client-Knoten auf dem Ziel-Server vorhanden ist

Mit dem Befehl QUERY ACTLOG kann der Status der Exportoperation angezeigt werden. Diese Informationen können auch über die Serverkonsole angezeigt werden.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn Sie Maßnahmeninformationen auf sequenzielle Datenträger exportieren und der Hintergrundprozess abgebrochen wird, sind die sequenziellen Datenträger, auf denen sich die exportierten Daten befinden, unvollständig und dürfen nicht zum Importieren von Daten verwendet werden. Wird ein Hintergrundprozess abgebrochen, bei dem Daten von einem Server auf einen anderen Server exportiert werden, kann dies zu einem Teilimport von Daten führen. Werten Sie alle importierten Daten auf dem Zielsystem aus, um zu bestimmen, ob die importierten Daten behalten oder gelöscht werden sollen. Überprüfen Sie die Importnachrichten auf Details. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Die folgenden Einschränkungen gelten für die Exportfunktion:

- Exportoperationen aus einer höheren Version und einem höheren Release in eine frühere Version und ein früheres Release werden nicht unterstützt.
- Exportoperationen zwischen Servern, die dieselbe Version und dasselbe Release, aber verschiedene Fixpacks aufweisen, können fehlschlagen. Beispielsweise können Sie keinen Export von einem Server der Version 7.1.3 auf einen Server der Version 7.1.1 oder einen früheren Server ausführen.
- Exportierte Daten von einem Server mit aktiviertem Aufbewahrungsschutz sind nicht durch Aufbewahrung geschützt, wenn sie auf einen anderen Server importiert werden.
- Die Exportverarbeitung schließt Knoten des Typs NAS (Network-attached Storage) aus.
- Das Exportieren von Daten in eine Centera-Einheitenklasse oder das Importieren von Daten aus einer Centera-Einheitenklasse wird nicht unterstützt. Dateien, die in Centera-Speicherpools gespeichert werden, können jedoch exportiert werden, und Dateien, die importiert werden müssen, können auf einer Centera-Speichereinheit gespeichert werden.

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

Der Befehl EXPORT POLICY hat zwei Formen: Zum Exportieren von Daten direkt auf einen anderen Server in dem Netz oder zum Exportieren von Daten auf sequenzielle Datenträger. Syntax und Parameter der jeweiligen Form werden separat definiert.



Anmerkungen:

1. Wenn PREVIEW=NO gilt, muss eine Einheitenklasse angegeben werden.
2. Wenn PREVIEW=NO und SCRATCH=NO gilt, müssen Datenträger angegeben werden.

## Parameter

---

### Domänenname

Gibt die Maßnahmendomänen an, für die Informationen exportiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Maßnahmendomänen. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

### Preview

Gibt an, ob die Ergebnisse der Exportoperation vorangezeigt werden sollen, ohne die Informationen zu exportieren. Mit diesem Parameter kann der Umfang der zu übertragenden Daten (Byte) vorangezeigt werden, um zu bestimmen, wie viele Datenträger benötigt werden. Dieser Parameter unterstützt die folgenden Werte:

#### No

Gibt an, dass die Maßnahmeninformationen exportiert werden sollen. Wird dieser Wert angegeben, muss auch eine Einheitenklasse angegeben werden.

#### Yes

Gibt an, dass die Operation vorangezeigt, aber nicht ausgeführt wird. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet. Wird dieser Wert angegeben, muss keine Einheitenklasse angegeben werden.

Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

### DEVclass

Gibt die Einheitenklasse an, in die die Exportdaten geschrieben werden sollen. Dieser Parameter ist erforderlich, wenn Sie PREVIEW=NO angeben.

Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Exports aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, um ein Laufwerk verfügbar zu machen.

Tipp: Daten können in einen Speicherpool auf einem anderen Server exportiert werden, indem eine Einheitenklasse mit dem Einheitentyp SERVER angegeben wird.

### Scratch

Gibt an, ob Arbeitsdatenträger verwendet werden können. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

#### Yes

Gibt an, dass Arbeitsdatenträger zum Exportieren verwendet werden können. Wird auch eine Liste mit Datenträgern angegeben, werden Arbeitsdatenträger nur verwendet, wenn auf den angegebenen Datenträgern nicht genügend Speicherbereich vorhanden ist.

#### No

Gibt an, dass keine Arbeitsdatenträger zum Exportieren verwendet werden können. Um zu bestimmen, wie viele Datenträger benötigt werden, können Sie den Befehl mit der Angabe PREVIEW=YES ausführen.

### VOLumentnames

Gibt die Datenträger an, die zum Speichern der exportierten Daten verwendet werden sollen. Dieser Parameter ist wahlfrei, es sei denn, es wird SCRATCH=NO und PREVIEW=NO angegeben. Wird kein Datenträgername angegeben, werden Arbeitsdatenträger verwendet.

Sie können einen der folgenden Werte angeben:

#### Datenträgername

Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

#### FILE: Dateiname

Gibt den Namen einer Datei an, die eine Liste mit Datenträgern enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

Folgende Namenskonventionen bei der Angabe von Datenträgern verwenden, die folgenden Einheitentypen zugeordnet sind:

| Für Einheit | Angeben                        |
|-------------|--------------------------------|
| Band        | 1 - 6 alphanumerische Zeichen. |

| Für Einheit               | Angeben  |
|---------------------------|--|
| FILE                      | Beliebige, vollständig qualifizierte Dateinamenzeichenfolge. Beispiel:<br>Linux-Betriebssysteme/imdata/mt1.<br>Windows-Betriebssystemed:\Programmdateien\tivoli\tsm\data1.dsm. |
| <br><br><br>REMOVABLEFILE | Windows-Betriebssysteme1 - 6 alphanumerische Zeichen.  |
| SERVER                    | 1 - 250 alphanumerische Zeichen.   |

#### USEDVolumelist

Gibt die Datei an, in der eine Liste der Datenträger gespeichert wird, die in der Exportoperation verwendet werden. Dieser Parameter ist wahlfrei.

Diese Datei kann für die Importoperation verwendet werden. Diese Datei enthält Kommentarzeilen mit dem Exportdatum und der Exportuhrzeit sowie dem Befehl, der zum Erstellen des Exports ausgegeben wurde.

Achtung: Wird eine vorhandene Datei angegeben, wird die Datei überschrieben.

## Beispiel: Maßnahmeninformationen auf bestimmte Banddatenträger exportieren

Vom Server Maßnahmeninformationen auf die Banddatenträger TAPE01, TAPE02 und TAPE03 exportieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist.

```
export policy devclass=menu1
volumenames=tape01,tape02,tape03
```

## Beispiel: Maßnahmeninformationen auf Banddatenträger exportieren, die in einer Datei aufgelistet sind

Vom Server die Maßnahmeninformationen auf Banddatenträger exportieren, die in der folgenden Datei aufgelistet sind:

- Linux-BetriebssystemeTAPEVOL
- TAPEVOL.DATA

Diese Datei enthält die folgenden Zeilen:

```
TAPE01
TAPE02
TAPE03
```

Angeben, dass diese Banddatenträger von einer Einheit verwendet werden, die der Einheitenklasse MENU1 zugeordnet ist. Geben Sie den folgenden Befehl aus: Linux-Betriebssysteme

```
export policy devclass=menu1 volumenames=file:tapevol
```

```
export policy devclass=menu1 volumenames=file:tapevol.data
```

## EXPORT POLICY (Eine Maßnahme direkt auf einen anderen Server exportieren)

Mit diesem Befehl können Maßnahmeninformationen direkt auf einen anderen Server in dem Netz exportiert werden. Dies hat einen sofortigen Import auf den Zielserver zur Folge.

Sie können einen Befehl QUERY PROCESS auf dem Zielserver ausgeben, um den Fortschritt der Importoperation zu überwachen. In EXPORT ADMIN (Administratorinformationen exportieren) finden Sie eine Liste der Einschränkungen, die für die Exportfunktion gelten.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax



Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten importiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls IMPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.

Sie haben auch die Option, eine Exportoperation direkt auf einem anderen Server in dem Netz zu verarbeiten. Dies hat einen sofortigen Importprozess zur Folge, ohne dass kompatible sequenzielle Einheitentypen zwischen den beiden Servern verwendet werden müssen.

Sie können die folgenden Typen von Serverinformationen exportieren, indem Sie den Befehl EXPORT SERVER ausgeben:

- Maßnahmendomänendefinitionen
- Maßnahmengruppendefinitionen
- Verwaltungsklassen- und Kopiergruppendefinitionen
- Zeitpläne, die für jede Maßnahmendomäne definiert sind
- Administratordefinitionen
- Clientknotendefinitionen

Sie können wahlweise die folgenden Typen von Daten exportieren:

- Dateibereichsdefinitionen
- Zugriffsberechtigungsinformationen zu den exportierten Dateibereichen
- Gesicherte Dateien, archivierte Dateien und Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn Sie Serverinformationen auf sequenzielle Datenträger exportieren und der Hintergrundprozess abgebrochen wird, sind die sequenziellen Datenträger, auf denen sich die exportierten Daten befinden, unvollständig und dürfen nicht zum Importieren von Daten verwendet werden. Wird ein Hintergrundprozess abgebrochen, bei dem Daten von einem Server auf einen anderen Server exportiert werden, kann dies zu einem Teilimport von Daten führen. Werten Sie alle importierten Daten auf dem Zielsystem aus, um zu bestimmen, ob die importierten Daten behalten oder gelöscht werden sollen. Überprüfen Sie die Importnachrichten auf Details.

Geben Sie den Befehl QUERY PROCESS auf dem Zielsystem aus, um den Fortschritt der Importoperation zu überwachen. Geben Sie den Befehl QUERY EXPORT aus, um alle aktiven oder ausgesetzten Exportoperationen zwischen Servern aufzulisten (die einen anderen Wert für FILEDATA als NONE haben).

Mit dem Befehl QUERY ACTLOG können die tatsächlichen Statusinformationen angezeigt werden, die Auskunft über die Größe und den Erfolg oder das Fehlschlagen der Exportoperation geben.

Die folgenden Einschränkungen gelten für die Exportfunktion:

- Exportoperationen aus einer höheren Version und einem höheren Release in eine frühere Version und ein früheres Release werden nicht unterstützt.
- Exportoperationen zwischen Servern, die dieselbe Version und dasselbe Release, aber verschiedene Fixpacks aufweisen, können fehlschlagen. Beispielsweise können Sie keinen Export von einem Server der Version 7.1.3 auf einen Server der Version 7.1.1 oder einen früheren Server ausführen.
- Exportierte Daten von einem Server mit aktiviertem Aufbewahrungsschutz sind nicht durch Aufbewahrung geschützt, wenn sie auf einen anderen Server importiert werden.
- Die Exportverarbeitung schließt Knoten des Typs NAS (Network-attached Storage) aus.
- Das Exportieren von Daten in eine Centera-Einheitenklasse oder das Importieren von Daten aus einer Centera-Einheitenklasse wird nicht unterstützt. Dateien, die in Centera-Speicherpools gespeichert werden, können jedoch exportiert werden, und Dateien, die importiert werden müssen, können auf einer Centera-Speichereinheit gespeichert werden.
- Mit den Befehlen EXPORT NODE und EXPORT SERVER werden keine Daten aus einem Schredderpool exportiert, es sei denn, dies wird explizit zugelassen, indem der Parameter ALLOWSHREDDABLE auf YES gesetzt wird. Wenn dieser Wert angegeben wird und die exportierten Daten Daten aus Schredderpools einschließen, können diese Daten nicht geschreddert werden. Es wird keine Warnung ausgegeben, wenn die Exportoperation Daten aus Schredderpools einschließt.
- Das inkrementelle Exportieren oder Importieren der folgenden Typen von Clientdaten auf einen anderen IBM Spectrum Protect-Server wird nicht unterstützt:
  - VMware-Sicherungen, bei denen Gesamt- und Teilsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen
  - Sicherungsgruppen, bei denen Gesamt- und Differenzsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen
  - Windows-Systemstatusdaten, die periodisch, inkrementell auf einen anderen Server übertragen werden

Der vollständige Export oder Import dieser Daten in ein neues Dateisystem auf dem Ziel wird unterstützt, indem der gesamte Dateibereich, der die Daten enthält, exportiert wird. Bei dem Export darf nicht der Parameter FILEDATA=ALLACTIVE, FROMDATE,



TODATE oder MERGEFILESPPACES verwendet werden.

Die Verwendung der Knotenreplikation zur inkrementellen Übertragung dieses Typs von Clientdaten zwischen zwei Servern ist optimal.

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

Der Befehl EXPORT SERVER hat zwei Formen: Zum Exportieren von Daten direkt auf einen anderen Server in dem Netz oder zum Exportieren von Daten auf sequenzielle Datenträger. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für EXPORT SERVER

| Befehl            | Beschreibung  |
|-------------------|---|
| CANCEL EXPORT     | Löscht eine ausgesetzte Exportoperation.  |
| CANCEL PROCESS    | Bricht einen Serverhintergrundprozess ab.   |
| COPY ACTIVATEDATA | Kopiert aktive Sicherungsdaten.   |
| EXPORT ADMIN      | Kopiert Verwaltungsdaten auf externe Datenträger oder direkt auf einen anderen Server.          |
| EXPORT NODE       | Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server. |
| EXPORT POLICY     | Kopiert Maßnahmeninformationen auf externe Datenträger oder direkt auf einen anderen Server.    |
| IMPORT SERVER     | Schreibt den gesamten Server oder einen Teil davon von externen Datenträgern zurück.            |
| QUERY ACTLOG      | Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.  |
| QUERY EXPORT      | Zeigt die Exportoperationen an, die gerade aktiv oder ausgesetzt sind.                          |
| QUERY PROCESS     | Zeigt Informationen über Hintergrundprozesse an.  |
| RESTART EXPORT    | Startet eine ausgesetzte Exportoperation erneut.  |
| SUSPEND EXPORT    | Setzt eine aktive Exportoperation aus.  |

- EXPORT SERVER (Server auf sequenzielle Datenträger exportieren)  
Sie können die Serversteuerungsinformationen und Clientdateidaten vollständig oder teilweise von einem Server auf sequenzielle Datenträger exportieren, sodass diese Informationen auf einen anderen Server importiert werden können.
- EXPORT SERVER (Serversteuerungsinformationen und Clientdateidaten auf einen anderen Server exportieren)  
Mit diesem Befehl können die Serversteuerungsinformationen und Clientdateidaten vollständig oder teilweise direkt auf einen anderen Server in dem Netz exportiert werden. Dies hat einen sofortigen Import auf den Zielservers zur Folge.

## EXPORT SERVER (Server auf sequenzielle Datenträger exportieren)

Sie können die Serversteuerungsinformationen und Clientdateidaten vollständig oder teilweise von einem Server auf sequenzielle Datenträger exportieren, sodass diese Informationen auf einen anderen Server importiert werden können.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
.-FILEData----None-----  
>>-EXPoRT Server--+----->  
'-FILEData----+All-----'
```

```

+-None-----+
+-ARchive-----+
+-Backup-----+
+-BACKUPActive+
+-ALLActive-----+
'-SPacemanaged-'

.-Preview---No-----+
>+-----+
|          (1) (2) |
|'-Preview-----+No--+-'|
|          '-Yes-' |

>+-----+
|          (1) |
|'-DEVclass-----Einheitenklassenname-'|

.-Scratch---Yes-----+
>+-----+
|          (2) |
|'-Scratch-----+Yes--+-'|
|          '-No--' |

>+-----+
|          (2)          .,-----+ |
|          V          | |
|'-VOLumenames-----+Datenträgername+--+-'|
|          '-FILE:--Dateiname----' |

>+-----+
|          '-USEDVolumelist---Dateiname-'|

>+-----+
|          .-FROMTime---00:00:00-. |
|'-FROMDate---Datum--+-----+-'|
|          '-FROMTime---Zeit-----' |

>+-----+
|          .-TOTime---23:59:59-. |
|'-TODate---Datum--+-----+-'|
|          '-TOTime---Zeit-----' |

.-ENCryptionstrength---AES-----+
>+-----+
|'-ENCryptionstrength---+AES--+-'|
|          '-DES-' |

.-ALLOWSHREDDable---No-----+
>+-----+
|'-ALLOWSHREDDable---+No--+-'|
|          '-Yes-' |

```

#### Anmerkungen:

1. Wenn PREVIEW=NO gilt, muss eine Einheitenklasse angegeben werden.
2. Wenn PREVIEW=NO und SCRATCH=NO gilt, müssen Datenträger angegeben werden.

## Parameter

### FILEData

Gibt den Typ der Dateien an, die für alle Knoten exportiert werden, die für den Server definiert sind. Dieser Parameter ist wahlfrei. Der Standardwert ist NONE.

Beim Export auf sequenzielle Datenträger wird die für den Zugriff auf die Dateidaten verwendete Einheitenklasse durch die Einheitenklasse für den Speicherpool bestimmt. Handelt es sich um dieselbe Einheitenklasse wie in diesem Befehl, werden zum Exportieren von Serverinformationen zwei Laufwerke benötigt. Der Grenzwert für Ladeanforderungen der Einheitenklasse muss mindestens auf 2 gesetzt werden.

In den folgenden Beschreibungen werden *aktive* und *inaktive* Versionen von Sicherungsdateien erwähnt. Eine aktive Version einer Sicherungsdatei ist die aktuellste Sicherungsversion für eine Datei, die noch auf der Client-Workstation vorhanden ist. Alle anderen Versionen der Sicherungsdatei werden als inaktive Kopien bezeichnet. Die folgenden Werte sind verfügbar:

ALL

IBM Spectrum Protect exportiert alle Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

None

IBM Spectrum Protect exportiert keine Dateien, nur Definitionen.

ARchive

IBM Spectrum Protect exportiert nur archivierte Dateien.

Backup

IBM Spectrum Protect exportiert nur Sicherungsversionen, unabhängig davon, ob die Versionen aktiv oder inaktiv sind.

BACKUPActive

IBM Spectrum Protect exportiert nur aktive Sicherungsversionen.

ALLActive

IBM Spectrum Protect exportiert alle aktiven Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

SPAcemanaged

IBM Spectrum Protect exportiert nur Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

Preview

Gibt an, ob die Ergebnisse der Exportoperation vorangezeigt werden sollen, ohne die Informationen zu exportieren. Mit diesem Parameter kann der Umfang der zu übertragenden Daten (Byte) vorangezeigt werden, um zu bestimmen, wie viele Datenträger benötigt werden. Dieser Parameter unterstützt die folgenden Werte:

No

Gibt an, daß die Server-Informationen exportiert werden sollen. Wird dieser Wert angegeben, muss auch eine Einheitenklasse angegeben werden.

Yes

Gibt an, dass die Operation vorangezeigt, aber nicht ausgeführt wird. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet. Wird dieser Wert angegeben, muss keine Einheitenklasse angegeben werden.

Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

DEVclass

Gibt die Einheitenklasse an, in die die Exportdaten geschrieben werden sollen. Dieser Parameter ist erforderlich, wenn Sie PREVIEW=NO angeben.

Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Exports aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, um ein Laufwerk verfügbar zu machen.

Tipp: Daten können in einen Speicherpool auf einem anderen Server exportiert werden, indem eine Einheitenklasse mit dem Einheitentyp SERVER angegeben wird.

Scratch

Gibt an, ob Arbeitsdatenträger verwendet werden können. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

Yes

Gibt an, dass Arbeitsdatenträger zum Exportieren verwendet werden können. Wird auch eine Liste mit Datenträgern angegeben, werden Arbeitsdatenträger nur verwendet, wenn auf den angegebenen Datenträgern nicht genügend Speicherbereich vorhanden ist.

No

Gibt an, dass keine Arbeitsdatenträger zum Exportieren verwendet werden können. Um zu bestimmen, wie viele Datenträger benötigt werden, können Sie den Befehl mit der Angabe PREVIEW=YES ausführen.

VOLumenames

Gibt die Datenträger an, die zum Speichern der exportierten Daten verwendet werden sollen. Dieser Parameter ist wahlfrei, es sei denn, es wird SCRATCH=NO und PREVIEW=NO angegeben. Wird kein Datenträgername angegeben, werden Arbeitsdatenträger verwendet.

Sie können einen der folgenden Werte angeben:


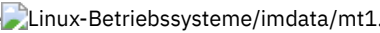
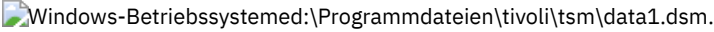


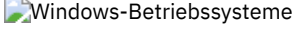

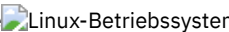
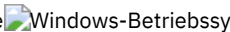
Datenträgername

Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

FILE: Dateiname

Gibt den Namen einer Datei an, die eine Liste mit Datenträgern enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

Folgende Namenskonventionen bei der Angabe von Datenträgern verwenden, die folgenden Einheitentypen zugeordnet sind:

| Für Einheit  | Angeben  |
|--|--|
| Band   | 1 - 6 alphanumerische Zeichen.   |
| FILE   | Beliebige, vollständig qualifizierte Dateinamenzeichenfolge. Beispiel:<br> <br> |
| <br><br><br>REMOVABLEFILE |    1 - 6 alphanumerische Zeichen.  |
| SERVER   | 1 - 250 alphanumerische Zeichen.   |

#### USEDVolumelist

Gibt die Datei an, in der eine Liste der Datenträger gespeichert wird, die in der Exportoperation verwendet werden. Dieser Parameter ist wahlfrei.

Diese Datei kann für die Importoperation verwendet werden. Diese Datei enthält Kommentarzeilen mit dem Exportdatum und der Exportuhrzeit sowie dem Befehl, der zum Erstellen des Exports ausgegeben wurde.

Achtung: Wird eine vorhandene Datei angegeben, wird die Datei überschrieben.

#### FROMDate

Gibt das früheste Datum an, für das Dateien, die exportiert werden sollen, auf dem Server gespeichert wurden. Dateien, die vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter FROMDATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Verzeichnisverarbeitung: Der Parameter FROMDATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.

Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Gruppendaten auf dem Knoten sind beispielsweise Daten virtueller Maschinen oder Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 09/15/1998   |
| TODAY                          | Das aktuelle Datum   | TODAY  |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY -3 <b>oder</b> -3.   |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

Wird dieser Parameter nicht angegeben, exportiert IBM Spectrum Protect alle Objekte, die vor dem Datum im Parameter TODATE gespeichert wurden und die durch den Parameter FILEDATA qualifiziert sind. Wird kein Parameter TODATE angegeben, werden alle Daten exportiert, die durch den Parameter FILEDATA qualifiziert sind.

Wenn eine Exportoperation zwischen Servern ein relatives FROMDATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der

ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird FROMDATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und zehn Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

#### TODate

Gibt das späteste Datum für Dateien an, die vom Server exportiert werden sollen. Dateien, die auf dem Server an einem späteren Datum als dem für TODATE angegebenen Datum gespeichert werden, werden nicht exportiert. TODATE gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen.

- IBM Spectrum Protect ignoriert den Parameter TODATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.
- Wenn ein Parameter TODATE ohne einen Parameter TOTIME angegeben wird, exportiert der Server alle Objekte, die an oder vor dem durch den Parameter TODATE angegebenen Tag eingefügt wurden.
- Wurde der Parameter FROMDATE angegeben, muss der Wert von TODATE größer-gleich dem Wert von FROMDATE sein. Sind TODATE und FROMDATE gleich, muss der Wert für den Parameter TOTIME größer als der Wert für den Parameter FROMTIME sein.
- Der Parameter TODATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.

Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 10/15/2006   |
| TODAY                          | Das aktuelle Datum   | TODAY  |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY -3 <b>oder</b> -3.   |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

Wenn eine Exportoperation zwischen Servern ein relatives TODATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird TODATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und zehn Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

#### FROMTime

Gibt die früheste Uhrzeit an, für die Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Geben Sie FROMTIME an, müssen Sie auch den Parameter FROMDATE verwenden. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. Objekte, die vor der angegebenen Uhrzeit und vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. IBM Spectrum Protect ignoriert den Parameter FROMTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Beispiele für Gruppendaten auf dem Knoten sind Daten virtueller Maschinen und Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Bei Verwendung mit dem Parameter FROMDATE lautet der Standardwert für diesen Parameter Mitternacht (00:00:00).

Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

| Wert                             | Beschreibung   | Beispiel  |
|----------------------------------|--|---|
| HH:MM:SS                         | Eine bestimmte Uhrzeit   | 10:30:08  |
| NOW                              | Die aktuelle Uhrzeit   | NOW   |
| NOW+HH:MM <b>oder</b><br>+HH:MM  | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten. FROMTIME+ kann nur mit einem FROMDATE vor heute verwendet werden. | NOW+02:00 <b>oder</b> +02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW+02:00 oder FROMTIME+=02:00 ausgegeben, enthält die Exportoperation nur Dateien, die nach 7:00 Uhr an dem angegebenen FROMDATE auf den Server gestellt wurden. |
| NOW-HH:MM <b>oder</b> -<br>HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten   | NOW -02:00 <b>oder</b> -02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW-02:00 oder FROMTIME=-2:00 ausgegeben, enthält der Export Dateien, die nach 3:00 Uhr auf den Server gestellt wurden.  |

#### TOTIME

Gibt den spätesten Zeitpunkt an, an dem Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Sie müssen den Parameter TODATE angeben, um den Parameter TOTIME verwenden zu können. TOTIME gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter TOTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Bei Verwendung mit dem Parameter TODATE lautet der Standardwert für diesen Parameter Mitternacht minus eine Sekunde (23:59:59).

Wichtig: Die Werte für die Parameter TOTIME und TODATE müssen größer als die Werte für die Parameter FROMDATE und FROMTIME sein.

Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

| Wert                             | Beschreibung  | Beispiel  |
|----------------------------------|---|---|
| HH:MM:SS                         | Eine bestimmte Uhrzeit  | 10:30:08  |
| NOW+HH:MM <b>oder</b><br>+HH:MM  | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.  | NOW+02:00 <b>oder</b> +02:00.<br><br>Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW+02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 7 Uhr gespeichert wurden. |
| NOW-HH:MM <b>oder</b> -<br>HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten. | NOW-02:00 <b>oder</b> -02:00.<br><br>Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW-02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 3 Uhr gespeichert wurden. |

#### ENCryptionstrength

Gibt an, welcher Algorithmus für die Verschlüsselung von Kennwörtern verwendet werden soll, wenn Verwaltungs- und Knotensätze exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist AES. Erfolgt der Export auf einen Server, der AES nicht unterstützt, geben Sie DES an. Sie können einen der folgenden Werte angeben:

AES

Gibt den Advanced Encryption Standard an.

DES

Gibt den Data Encryption Standard an.

#### ALLOWSHREDdable

Gibt an, ob Daten aus einem Speicherpool, der das Schreddern erzwingt, exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, dass Daten nicht aus einem Speicherpool exportiert werden, der das Schreddern erzwingt.

Yes

Gibt an, dass Daten aus einem Speicherpool exportiert werden können, der das Schreddern erzwingt. Die Daten auf den Exportdatenträgern werden nicht geschreddert.

## Beispiel: Einen Server auf bestimmte Banddatenträger exportieren

---

Vom Server Server-Informationen auf die Banddatenträger TAPE01, TAPE02 und TAPE03 exportieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist.

```
export server devclass=menu1
volumenames=tape01,tape02,tape03
```

## Beispiel: Einen Server auf Banddatenträger exportieren, die in einer Datei aufgelistet sind

---

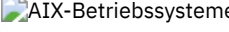
Vom Server die Serverinformationen auf Banddatenträger exportieren, die in der folgenden Datei aufgelistet sind:

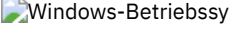
- Linux-BetriebssystemeTAPEVOL
- Windows-BetriebssystemeTAPEVOL.DATA

Die Datei enthält die folgenden Zeilen:

```
TAPE01
TAPE02
TAPE03
```

Angeben, dass die Banddatenträger von einer Einheit verwendet werden, die der Einheitenklasse MENU1 zugeordnet ist. Geben Sie den folgenden Befehl aus:

```
Linux-Betriebssysteme
export server devclass=menu1 volumenames=file:tapevol
```

```
Windows-Betriebssysteme
export server devclass=menu1 volumenames=file:tapevol.data
```

## EXPORT SERVER (Serversteuerungsinformationen und Clientdateidaten auf einen anderen Server exportieren)

---

Mit diesem Befehl können die Serversteuerungsinformationen und Clientdateidaten vollständig oder teilweise direkt auf einen anderen Server in dem Netz exportiert werden. Dies hat einen sofortigen Import auf den Zielserver zur Folge.

Exportoperation zwischen Servern, die einen anderen Wert für FILEDATA als NONE haben, können erneut gestartet werden, nachdem die Operation ausgesetzt wurde. Der Server sichert den Status der Exportoperation, sodass die Exportoperation an dem Punkt erneut gestartet werden kann, an dem sie fehlgeschlagen ist oder an dem sie ausgesetzt wurde. Die Exportoperation kann zu einem späteren Zeitpunkt erneut gestartet werden, indem der Befehl RESTART EXPORT ausgegeben wird. Diese Exportoperationen können manuell ausgesetzt sowie erneut gestartet werden. Schlägt ein Export fehl, wird er daher automatisch ausgesetzt, wenn er die Phase für die Übertragung der Definitionen beendet hat.

Eine Exportoperation wird ausgesetzt, wenn eine der folgenden Bedingungen festgestellt wird:

- Ein Befehl SUSPEND EXPORT wird für die aktive Exportoperation ausgegeben
- Segmentvorableerung - die Datei, die für den Export gelesen wird, wird von einem anderen Prozess gelöscht
- Übertragungsfehler bei einem Export zwischen Servern
- Keine verfügbaren Mountpunkte
- Erforderliche Datenträger sind nicht verfügbar
- E/A-Fehler wurden festgestellt

Die Exportoperation kann nicht erneut gestartet werden, wenn die Exportoperation fehlschlägt, bevor die auswählbaren Knoten- und Dateibereichsdefinitionen auf den Zielserver übertragen werden. Sie müssen den Befehl erneut eingeben, um eine neue Exportoperation zu beginnen.

Geben Sie den Befehl QUERY PROCESS auf dem Zielserver aus, um den Fortschritt der Importoperation zu überwachen. Geben Sie den Befehl QUERY EXPORT aus, um alle aktiven oder ausgesetzten Exportoperationen zwischen Servern aufzulisten (die einen anderen Wert für FILEDATA als NONE haben). In EXPORT ADMIN (Administratorinformationen exportieren) finden Sie eine Liste der Einschränkungen, die für die Exportfunktion gelten.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```

      .-FILEData---None-----
>>-EXPort Server-----+----->
      '-FILEData---+All-----+'
                +-None-----+
                +-ARchive-----+
                +-Backup-----+
                +-BACKUPActive--+
                +-ALLActive-----+
                '-SPacemanaged-'

>+-----+-----+-----+----->
|                                     .-FROMTime---00:00:00- |
'-FROMDate---Datum-----+-----+'
      '-FROMTime---Zeit-----'

>+-----+-----+-----+----->
|                                     .-TOTime---23:59:59- |
'-TODate---Datum-----+-----+'
      '-TOTime---Zeit-----'

>+-----+-----+-----+----->
      '-EXPORTIdentifier---Export-ID-'

      .-PREVIEWImport---No-----
>+-----+-----+-----+----->
      '-TOServer---Servername-'   '-PREVIEWImport---+No--+-'
                                   '-Yes-'

      .-MERGEfilespace---No-----
>+-----+-----+-----+----->
      '-MERGEfilespace---+No--+-'
                                   '-Yes-'

      .-Replacedefs---No-----
>+-----+-----+-----+----->
      '-Replacedefs---+No--+-'
                                   '-Yes-'

      .-PROXynodeassoc---No-----
>+-----+-----+-----+----->
      '-PROXynodeassoc---+No--+-'
                                   '-Yes-'

      .-ENCryptionstrength---AES-----
>+-----+-----+-----+----->
      '-ENCryptionstrength---+AES--+-'
                                   '-DES-'

      .-ALLOWSHREDDable---No-----
>+-----+-----+-----+-----><
      '-ALLOWSHREDDable---+No--+-'
                                   '-Yes-'

```

## Parameter

### FILEData

Gibt den Typ der Dateien an, die für alle Knoten exportiert werden sollen, die für den Server definiert sind. Dieser Parameter ist wahlfrei. Der Standardwert ist NONE.

Export auf sequenzielle Datenträger: Die Einheitenklasse für den Zugriff auf die Dateidaten wird durch die Einheitenklasse des Speicherpools bestimmt. Handelt es sich um dieselbe Einheitenklasse wie in diesem Befehl, benötigt IBM Spectrum Protect zwei Laufwerke zum Exportieren von Serverinformationen. Sie müssen den Grenzwert für Ladeanforderungen für die Einheitenklasse auf mindestens 2 setzen.

In den folgenden Beschreibungen werden aktive und inaktive Versionen von Sicherungsdateien erwähnt. Eine aktive Version einer Sicherungsdatei ist die aktuellste Sicherungsversion für eine Datei, die noch auf der Client-Workstation vorhanden ist. Alle anderen Versionen der Sicherungsdatei werden als inaktive Kopien bezeichnet. Gültige Werte:

#### ALL

IBM Spectrum Protect exportiert alle Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

#### None



IBM Spectrum Protect exportiert keine Dateien, nur Definitionen.

ARchive

IBM Spectrum Protect exportiert nur archivierte Dateien.

Backup

IBM Spectrum Protect exportiert nur Sicherungsversionen, unabhängig davon, ob sie aktiv oder inaktiv sind.

BACKUPActive

IBM Spectrum Protect exportiert nur aktive Sicherungsversionen.

ALLActive

IBM Spectrum Protect exportiert alle aktiven Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

SPacemanaged

IBM Spectrum Protect exportiert nur Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

FROMDate

Gibt das früheste Datum an, für das Dateien, die exportiert werden sollen, auf dem Server gespeichert wurden. Dateien, die vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter FROMDATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Verzeichnisverarbeitung: Der Parameter FROMDATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.

Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Gruppendaten auf dem Knoten sind beispielsweise Daten virtueller Maschinen oder Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 09/15/1998   |
| TODAY                          | Das aktuelle Datum   | TODAY  |
| TODAY-Tage <b>oder</b> - Tage  | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY -3 <b>oder</b> -3.   |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

Wird dieser Parameter nicht angegeben, exportiert IBM Spectrum Protect alle Objekte, die vor dem Datum im Parameter TODATE gespeichert wurden und die durch den Parameter FILEDATA qualifiziert sind. Wird kein Parameter TODATE angegeben, werden alle Daten exportiert, die durch den Parameter FILEDATA qualifiziert sind.

Wenn eine Exportoperation zwischen Servern ein relatives FROMDATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird FROMDATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und zehn Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

TODate

Gibt das späteste Datum für Dateien an, die vom Server exportiert werden sollen. Dateien, die auf dem Server an einem späteren Datum als dem für TODATE angegebenen Datum gespeichert werden, werden nicht exportiert. TODATE gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen.

- IBM Spectrum Protect ignoriert den Parameter TODATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.
- Wenn ein Parameter TODATE ohne einen Parameter TOTIME angegeben wird, exportiert der Server alle Objekte, die an oder vor dem durch den Parameter TODATE angegebenen Tag eingefügt wurden.
- Wurde der Parameter FROMDATE angegeben, muss der Wert von TODATE größer-gleich dem Wert von FROMDATE sein. Sind TODATE und FROMDATE gleich, muss der Wert für den Parameter TOTIME größer als der Wert für den Parameter FROMTIME sein.
- Der Parameter TODATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.

Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 10/15/2006   |
| TODAY                          | Das aktuelle Datum   | TODAY  |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY -3 <b>oder</b> -3.   |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

Wenn eine Exportoperation zwischen Servern ein relatives TODATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird TODATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und zehn Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

#### FROMTime

Gibt die früheste Uhrzeit an, für die Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Geben Sie FROMTIME an, müssen Sie auch den Parameter FROMDATE verwenden. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. Objekte, die vor der angegebenen Uhrzeit und vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. IBM Spectrum Protect ignoriert den Parameter FROMTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Beispiele für Gruppendaten auf dem Knoten sind Daten virtueller Maschinen und Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Bei Verwendung mit dem Parameter FROMDATE lautet der Standardwert für diesen Parameter Mitternacht (00:00:00).

Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

| Wert     | Beschreibung           | Beispiel |
|----------|------------------------|----------|
| HH:MM:SS | Eine bestimmte Uhrzeit | 10:30:08 |
| NOW      | Die aktuelle Uhrzeit   | NOW      |

| Wert                             | Beschreibung  | Beispiel  |
|----------------------------------|---|---|
| NOW+HH:MM <b>oder</b><br>+HH:MM  | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.FROMTIME+ kann nur mit einem FROMDATE vor heute verwendet werden. | NOW+02:00 <b>oder</b> +02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW+02:00 oder FROMTIME=+02:00 ausgegeben, enthält die Exportoperation nur Dateien, die nach 7:00 Uhr an dem angegebenen FROMDATE auf den Server gestellt wurden. |
| NOW-HH:MM <b>oder</b> -<br>HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten  | NOW -02:00 <b>oder</b> -02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW-02:00 oder FROMTIME=-2:00 ausgegeben, enthält der Export Dateien, die nach 3:00 Uhr auf den Server gestellt wurden.  |

#### TOTime

Gibt den spätesten Zeitpunkt an, an dem Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Sie müssen den Parameter TODATE angeben, um den Parameter TOTIME verwenden zu können. TOTIME gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter TOTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Bei Verwendung mit dem Parameter TODATE lautet der Standardwert für diesen Parameter Mitternacht minus eine Sekunde (23:59:59).

Wichtig: Die Werte für die Parameter TOTIME und TODATE müssen größer als die Werte für die Parameter FROMDATE und FROMTIME sein.

Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

| Wert                             | Beschreibung  | Beispiel  |
|----------------------------------|---|---|
| HH:MM:SS                         | Eine bestimmte Uhrzeit  | 10:30:08  |
| NOW+HH:MM <b>oder</b><br>+HH:MM  | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.  | NOW+02:00 <b>oder</b> +02:00.<br><br>Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW+02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 7 Uhr gespeichert wurden. |
| NOW-HH:MM <b>oder</b> -<br>HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten. | NOW-02:00 <b>oder</b> -02:00.<br><br>Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW-02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 3 Uhr gespeichert wurden. |

#### TOServer

Gibt den Namen eines Servers an, an den die Exportdaten direkt über das Netz für den sofortigen Import gesendet werden.

Wichtig: Der Zielservers muss mit dem Befehl DEFINE SERVER auf dem Ursprungsserver definiert werden. Der Administrator, der den Exportbefehl ausgibt, muss mit demselben Administratortnamen und demselben Kennwort definiert werden und muss auf dem Zielservers über die Systemberechtigung verfügen.

Wenn Sie TOSERVER angeben, können Sie nicht die Parameter DEVCLASS, VOLUMENAMES, SCRATCH, USEDVOLUMELIST und PREVIEW angeben.

#### PREVIEWImport

Gibt an, ob der Umfang der zu übertragenden Daten angezeigt werden soll, ohne die Daten tatsächlich zu versetzen. Mit diesen Informationen kann bestimmt werden, welcher Speicherpoolbereich auf dem Zielservers benötigt wird. Der Standardwert ist NO. Gültige Werte sind:

Yes

Gibt an, dass die Ergebnisse der Importoperation auf dem Zielservers vorangezeigt werden sollen, ohne dass die Daten importiert werden. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet.

No

Gibt an, dass die Daten in den Zielservers importiert werden sollen, ohne dass die Ergebnisse vorangezeigt werden.

#### MERGEfilespaces

Gibt an, ob IBM Spectrum Protect Clientdateien in vorhandene Dateibereiche auf dem Zielservers mischt (sofern sie vorhanden sind) oder ob IBM Spectrum Protect neue Dateibereichsnamen generiert. Der Standardwert ist NO.

Gültige Werte sind:

Yes

Gibt an, dass importierte Daten auf dem Zielserver in den vorhandenen Dateibereich gemischt werden, wenn ein Dateibereich mit demselben Namen auf dem Zielserver vorhanden ist.

No

Gibt an, dass IBM Spectrum Protect einen neuen Dateibereichsnamen für importierte Daten auf dem Zielserver generiert, wenn Dateibereiche mit demselben Namen vorhanden sind.

Replacedefs

Gibt an, ob Definitionen (nicht Dateidaten) auf dem Server ersetzt werden sollen. Der Standardwert ist NO.

Gültige Werte sind:

Yes

Gibt an, dass Definitionen auf dem Server ersetzt werden, wenn Definitionen mit demselben Namen wie die zu importierenden Definitionen auf dem Zielserver vorhanden sind.

No

Gibt an, dass importierte Definitionen übersprungen werden, wenn ihre Namen mit Definitionen in Konflikt stehen, die bereits auf dem Zielserver definiert sind.

PROXynodeassoc

Gibt an, ob Proxyknotenzuordnungen exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

ENCryptionstrength

Gibt an, welcher Algorithmus für die Verschlüsselung von Kennwörtern verwendet werden soll, wenn Verwaltungs- und Knotensätze exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist AES. Erfolgt der Export auf einen Server, der AES nicht unterstützt, geben Sie DES an. Sie können einen der folgenden Werte angeben:

AES

Gibt den Advanced Encryption Standard an.

DES

Gibt den Data Encryption Standard an.

ALLOWSHREDdable

Gibt an, ob Daten aus einem Speicherpool, der das Schreddern erzwingt, exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, dass es der Server nicht erlaubt, dass Daten aus einem Speicherpool, der das Schreddern erzwingt, exportiert werden.

Yes

Gibt an, dass es der Server erlaubt, dass Daten aus einem Speicherpool, der das Schreddern erzwingt, exportiert werden. Die Daten auf den Exportdatenträgern werden nicht geschreddert.

Wichtig: Nachdem eine Exportoperation die Identifizierung von Dateien für den Export beendet hat, werden alle Änderungen des Werts ALLOWSHREDABLE für den Speicherpool ignoriert. Eine Exportoperation, die ausgesetzt ist, behält während der gesamten Operation den ursprünglichen ALLOWSHREDABLE-Wert. Möglicherweise möchten Sie Ihre Exportoperation abbrechen, wenn Änderungen des Werts ALLOWSHREDABLE für den Speicherpool die Operation gefährden. Sie können den Exportbefehl nach einer erforderlichen Bereinigung erneut ausgeben.

EXPORTIDentifier

Dieser optionale Parameter gibt den Namen an, den Sie zum Identifizieren dieser Exportoperation ausgewählt haben. Geben Sie keinen Befehlsnamen an, wird vom Server ein Name generiert. Die Export-ID darf 64 Zeichen nicht überschreiten, darf keine Platzhalterzeichen enthalten, und ist nicht von der Groß-/Kleinschreibung abhängig. Mit dieser ID können Sie auf Exportoperationen in den Befehlen QUERY EXPORT, SUSPEND EXPORT, RESTART EXPORT oder CANCEL EXPORT verweisen. EXPORTIDENTIFIER wird bei FILEDATA=NONE oder PREVIEWIMPORT=YES ignoriert.

Geben Sie den Parameter EXPORTIDENTIFIER an, müssen Sie den Parameter TOSERVER angeben.

## Beispiel: Serverinformationen direkt auf einen anderen Server exportieren

---

Um Serverinformationen direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus.

```
export server filedata=all toserver=serverb
```

## Beispiel: Serverinformationen unter Verwendung eines Datumsbereichs direkt auf einen anderen Server exportieren

---

Um Serverinformationen zwischen dem 1. Februar 2009 und heute direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus.

```
export server filedata=all toserver=serverbfromdate=02/01/2009 todate=today
```

## Beispiel: Serverinformationen und Clientdateidaten unter Verwendung eines Datums- und Zeitbereichs direkt auf einen anderen Server exportieren

---

Um Serverinformationen zwischen dem 1. Februar 2009 um 8 Uhr bis heute um 8 Uhr direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus.

```
export server filedata=all toserver=serverbfromdate=02/01/2009 fromtime=08:00:00
todate=today totime=08:00:00
```

## EXTEND DBSPACE (Speicherbereich für die Datenbank erhöhen)

---

Verwenden Sie diesen Befehl, um den Speicherbereich für die Datenbank zu vergrößern, indem Verzeichnisse für die Datenbank hinzugefügt werden.

### Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Wenn Sie den Befehl EXTEND DBSPACE ausgeben, werden der Datenbank Verzeichnisse hinzugefügt. Mit den Standardparametereinstellungen werden Daten auf alle Datenbankverzeichnisse verteilt, und Speicherbereich wird zurückgefordert. Mit dieser Aktion wird die Leistung der parallelen E/A verbessert und der neue Verzeichnisbereich für die sofortige Verwendung zur Verfügung gestellt.

Sollen Daten nicht erneut verteilt werden, wenn Sie neue Verzeichnisse hinzufügen, können Sie RECLAIMSTORAGE=NO angeben. Wenn Sie für diesen Parameter NO angeben, wird der gesamte Speicherbereich in vorhandenen Verzeichnissen gefüllt, bevor neue Verzeichnisse verwendet werden. Sie können später Daten erneut verteilen und Speicherbereich zurückfordern, aber Sie müssen die manuelle Prozedur für diese Task mit DB2-Befehlen ausführen.

Einschränkung: Die Neuverteilung von Daten und die Zurückforderung von Speicherbereich als Teil einer Operation zum Erweitern des Datenbankbereichs funktioniert nur mit DB2-Tabellenbereichen der Version 9.7 oder höher. Die Tabellenbereiche werden erstellt, wenn Sie einen neuen IBM Spectrum Protect-Server der Version 6.2 oder höher formatieren. Wenn Sie für Ihren IBM Spectrum Protect-Server ein Upgrade von Version 6.1 durchgeführt oder Ihren Server aus Version 6.1 zurückgeschrieben haben, können Sie Daten nicht erneut verteilen und Speicherbereich nicht zurückfordern. Sie müssen den Befehl EXTEND DBSPACE mit RECLAIMSTORAGE=NO ausgeben. Wichtig: Bei dem Neuverteilungsprozess werden erhebliche Systemressourcen verwendet. Planen Sie dies ein, wenn der Datenbank Speicherbereich hinzugefügt werden soll. Beachten Sie die folgenden Richtlinien:

- Führen Sie den Prozess aus, wenn der Server keine hohe Arbeitslast verarbeitet.
- Die Zeit, die erforderlich ist, um Daten erneut zu verteilen und Speicherbereich zurückzufordern, kann variieren. Sie wird durch Faktoren beeinflusst, wie z. B. Dateisystemlayout, Verhältnis neuer Pfade zu vorhandenen Speicherpfaden, Server-Hardware und Parallelbetrieb. Um eine grobe Schätzung zu erhalten, können Sie die Operation mit einer kleinen IBM Spectrum Protect-Datenbank auf einem Übungssystem testen. Verwenden Sie Ihre Ergebnisse als Referenz, um die Zeit zu schätzen, die für die Prozedur erforderlich ist.
- Unterbrechen Sie nicht den Neuverteilungsprozess. Wenn Sie versuchen, den Prozess zu stoppen, indem Sie z. B. den Prozess anhalten, der die Arbeit ausführt, müssen Sie den DB2-Server stoppen und erneut starten. Wenn der Server erneut gestartet wird, wechselt er in den Modus für die Wiederherstellung nach einem Systemabsturz. Dies dauert einige Minuten. Danach wird der Neuverteilungsprozess fortgesetzt.

Nachdem eine Operation zum Erweitern des Datenbankbereichs ausgeführt wurde, halten Sie den Server an und starten Sie ihn erneut, um die neuen Verzeichnisse vollständig zu verwenden. Sind die vorhandenen Datenbankverzeichnisse nahezu voll, wenn ein neues Verzeichnis hinzugefügt wird, kann der Server eine Bedingung 'Kein Speicherbereich verfügbar' feststellen (wird in der Datei db2diag.log angegeben). Sie können die Bedingung 'Kein Speicherbereich verfügbar' beseitigen, indem der Server angehalten und erneut gestartet wird.

### Syntax

---

```
      .-,-,-----
      v          |
>>-EXTend DBSpace---DB-Verzeichnis+----->
      .-REclaimstorage---Yes----.  .-Wait----No-----
>+-----+-----+-----><
```


```
'-REclaimstorage-----+No---+'  '-Wait-----+No---+'  
      '-Yes-'                    '-Yes-'
```

## Parameter

---

### DB-Verzeichnis (Erforderlich)

Gibt die Verzeichnisse für den Datenbankspeicher an. Die Verzeichnisse müssen leer sein und auf die Verzeichnisse muss durch die Benutzer-ID des Datenbankmanagers zugegriffen werden können. Ein Verzeichnisname muss ein vollständig qualifizierter Name sein und darf 175 Zeichen nicht überschreiten. Schließen Sie den Namen in Anführungszeichen ein, wenn er eingebettete Leerzeichen, ein Gleichheitszeichen oder andere Sonderzeichen enthält. Wenn Sie eine Verzeichnisliste für den Datenbankspeicher angeben, beträgt die maximale Länge der Liste 1400 Zeichen.

 Windows-BetriebssystemeEinschränkung: Sie können keine Pfade mit allgemeiner Namenskonvention angeben.

Tipp: Geben Sie Verzeichnisse an, die dieselbe Größe wie vorhandene Verzeichnisse haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Sind ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse, reduzieren sie das Potenzial zum optimierten parallelen Vorabesezugriff und zur Verteilung der Datenbank.

### REclaimstorage

Gibt an, ob Daten auf neu erstellte Datenbankverzeichnisse erneut verteilt werden und Speicherbereich aus den alten Speicherpfaden zurückgefordert wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 'Yes'.

Die Operation wird als Hintergrundprozess ausgeführt, wenn nicht `WAIT=YES` angegeben wird.

#### Yes

Gibt an, dass Daten erneut verteilt werden, sodass neue Verzeichnisse für die sofortige Verwendung verfügbar sind. Wichtig: Bei dem Neuverteilungsprozess werden erhebliche Systemressourcen verwendet. Planen Sie dies im Voraus ein.

Nach dem Starten des Prozesses werden Nachrichten ausgegeben, die den Fortschritt angeben. Sie können den Befehl `QUERY PROCESS` verwenden, um die Operation zu überwachen. Um den Prozess abzubrechen, können Sie den Befehl `CANCEL PROCESS` verwenden. Ist jedoch eine Operation zur Neuverteilung von Daten aktiv, wird sie beendet, bevor der Prozess gestoppt wird.

#### No

Gibt an, dass Daten nicht auf Datenbankverzeichnisse erneut verteilt werden und Speicherbereich nicht zurückgefordert wird, wenn Speicherbereich für die Datenbank hinzugefügt wird.

### Wait

Gibt an, ob dieser Befehl im Hintergrund oder Vordergrund verarbeitet wird.

#### No

Gibt die Hintergrundverarbeitung an. Der Standardwert ist NO.

#### Yes

Gibt die Vordergrundverarbeitung an.

 AIX-Betriebssysteme  Linux-BetriebssystemeYES kann nicht von der Server-Konsole aus angegeben werden.

 AIX-Betriebssysteme  Linux-Betriebssysteme

## Beispiel: Verzeichnisse zum Speicherbereich für die Datenbank hinzufügen, Daten erneut verteilen und Speicher zurückfordern

---

Zwei Verzeichnisse (/tsm\_db/stg1 und tsm\_db/stg2) unter dem Verzeichnis /tsm\_db zum Speicherbereich für die Datenbank hinzufügen. Den folgenden Befehl ausgeben:

```
extend dbspace /tsm_db/stg1,/tsm_db/stg2
```

 Windows-Betriebssysteme

## Beispiel: Laufwerke zum Speicherbereich für die Datenbank hinzufügen, Daten erneut verteilen und Speicher zurückfordern

---

Die Laufwerke D und E zum Speicherbereich der Datenbank hinzufügen. Den folgenden Befehl ausgeben:

```
extend dbspace D:,E:
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für EXTEND DBSPACE




| Befehl                 | Beschreibung   |
|------------------------|--|
| DSMSERV EXTEND DBSPACE | Fügt Verzeichnisse hinzu, um den Speicherbereich für die Verwendung durch die Datenbank zu vergrößern. |
| QUERY DB               | Zeigt Zuordnungsinformationen zu der Datenbank an.   |
| QUERY DBSPACE          | Zeigt Informationen zum Speicherplatz an, der für die Datenbank definiert ist.                         |

**Zugehörige Tasks:**

Bestandskapazität verwalten

## GENERATE-Befehle

Verwenden Sie die GENERATE-Befehle für Sicherungsgruppen für einen ausgewählten Dateibereich oder Clientknoten.

- GENERATE BACKUPSET (Sicherungsgruppe mit Daten des Clients für Sichern/Archivieren generieren)
- GENERATE BACKUPSETTOC (Inhaltsverzeichnis für eine Sicherungsgruppe generieren)
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme GENERATE DEDUPSTATS (Dateneduplizierungsstatistikdaten generieren)

## GENERATE BACKUPSET (Sicherungsgruppe mit Daten des Clients für Sichern/Archivieren generieren)

Verwenden Sie diesen Befehl, um eine Sicherungsgruppe für einen Knoten des Clients für Sichern/Archivieren zu generieren. Eine *Sicherungsgruppe* ist eine Sammlung der aktiven gesicherten Daten eines Clients für Sichern/Archivieren, die als ein einzelnes Objekt auf bestimmten Datenträgern im Serverspeicher gespeichert und verwaltet wird. Obwohl Sie eine Sicherungsgruppe für jeden Clientknoten erstellen können, kann eine Sicherungsgruppe nur von einem Client für Sichern/Archivieren verwendet werden.

Einschränkung: Eine Sicherungsgruppe im "Deduplizierungsformat" trägt diese Bezeichnung infolge eines Befehls GENERATE BACKUPSET mit mindestens einer der folgenden Spezifikationen:

- Schließt einen Knoten des Clients für Sichern/Archivieren mit Version 6.1.x ein (mindestens Version 6.1.0, aber niedriger als Version 6.2.0).
- Schließt einen Knoten ein, der über einen oder mehrere Knoten verfügt, die berechtigt sind, als Proxy zu agieren. Mindestens einer dieser Proxy-Knoten hat die Version 6.1.x des Clients für Sichern/Archivieren.

Sicherungsgruppen im Deduplizierungsformat können nur von dem Client für Sichern/Archivieren mit Version 6.1.2 oder höher zurückgeschrieben werden. Clients für Sichern/Archivieren vor Version 6.1.2 können keine Zurückschreibung aus einer Sicherungsgruppe ausführen, die das Deduplizierungsformat hat.

Eine Sicherungsgruppe im "verteilten Deduplizierungsformat" trägt diese Bezeichnung infolge eines Befehls GENERATE BACKUPSET mit mindestens einer der folgenden Spezifikationen:

- Schließt einen Knoten des Clients für Sichern/Archivieren mit Version 6.2.0 oder höher ein.
- Schließt einen Knoten ein, der über einen oder mehrere Knoten verfügt, die berechtigt sind, als Proxy zu agieren. Mindestens einer dieser Proxy-Knoten hat die Version 6.2.0 des Clients für Sichern/Archivieren.

Sicherungsgruppen im verteilten Deduplizierungsformat können nur von dem Client für Sichern/Archivieren mit Version 6.2.0 oder höher zurückgeschrieben werden.

Einschränkung: Sie können keine Sicherungsgruppe mit Dateien generieren, die unter Verwendung von NDMP in IBM Spectrum Protect gesichert wurden. Sie können jedoch eine Sicherungsgruppe mit Dateien erstellen, die unter Verwendung der NetApp-Momentaufnahme-Differenz gesichert wurden.

Der Server erstellt Kopien von aktiven Versionen der gesicherten Objekte eines Clients, die sich innerhalb eines oder mehrerer Dateibereiche befinden, die mit diesem Befehl angegeben werden. Der Server fasst diese Kopien dann auf sequenziellen Datenträgern zusammen. Gegenwärtig umfassen die für Sicherungsgruppen unterstützten Sicherungsobjekttypen nur Verzeichnisse und Dateien.

Der Knoten des Clients für Sichern/Archivieren kann die Sicherungsgruppe von dem Server und von den Datenträgern zurückschreiben, auf die die Sicherungsgruppe geschrieben wurde.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wird der durch diesen Befehl erstellte Hintergrundprozess abgebrochen, enthalten die Datenträger möglicherweise keine vollständige Sicherungsgruppe. Mit dem Befehl QUERY PROCESS können Informationen zu dem Hintergrundprozess angezeigt werden, der durch diesen Befehl erstellt wird.

Tipp: Wenn IBM Spectrum Protect eine Sicherungsgruppe generiert, können Sie die Leistung verbessern, wenn die primären Speicherpools, die die Clientdaten enthalten, zusammengefasst werden. Wird ein primärer Speicherpool zusammengefasst, befinden sich die Clientknotendaten wahrscheinlich auf weniger Banddatenträger als dies der Fall wäre, wenn der Speicherpool nicht zusammengefasst würde. Mit der Kollokation wird weniger Zeit für die Suche nach Datenbankeinträgen benötigt, und es sind weniger Ladeoperationen erforderlich.

## Berechtigungsklasse

Um diesen Befehl ausgeben zu können, müssen Benutzer die Systemberechtigung oder Maßnahmenberechtigung für die Domäne haben, der der Client-Knoten zugeordnet ist.

## Syntax

```

      .-,------.
      v          |
>>-GENerate BACKUPSET-----+Knotenname-----+----->
      '-Knotengruppenname-'

>>--Präfix_des_Sicherungsgruppennamens----->

      .-*------.
>+-----+-----+----->
| .-,------. |
| v          | |
|'---Dateibereichsname---+'

>>--DEVclass-----Einheitenklassenname-----+----->
      '-SCRatch-----+Yes-----'
      '-SCRatch-----+Yes---+'
      '-No---'

>+-----+-----+----->
| .-,------. |
| v          | |
|'VOLUMes-----Datenträgernamen---+'

      .-RETention-----365-----.
>+-----+-----+----->
|'RETention-----+Tage---+'
|'NOLimit-'

>+-----+-----+----->
      .-Wait-----No-----.
|'DEScRiption-----Beschreibung-' |'Wait-----+No---+'
|'Yes-'

      .-NAMEType-----SERVER-----.
>+-----+-----+----->
|'NAMEType-----+SERVER---+'
|'Unicode+'
|'FSID----'

      .-CODEType-----BOTH-----.
>+-----+-----+----->
|'CODEType-----+Unicode---+'
|'NONUnicode+'
|'BOTH-----'

      .-PITDate-----aktuelles_Datum-.
>+-----+-----+----->
|'PITDate-----Datum-----'

      .-PITTime-----aktuelle_Uhrzeit-.
>+-----+-----+----->
|'PITTime-----Zeit-----'

      .-DATAType-----FILE------. .-TOC-----Preferred-----.
>+-----+-----+-----+----->
| .-,------. | |'TOC-----+No-----+'
| v          | | |'Preferred+'
|'DATAType-----+FILE---+' |'Yes-----'
|'IMAGE+'
|'ALL---'

```



```

>----->
' -TOCMGmtclass---Klassenname-'

.-ALLOWSHREddable---No-----
>-----<
' -ALLOWSHREddable---+No--+-'
                               '-Yes-'

```

## Parameter

### Knotenname oder Knotengruppenname (Erforderlich)

Gibt den Namen des Clientknotens und der Knotengruppe an, dessen bzw. deren Daten in der Sicherungsgruppe enthalten sind. Sollen mehrere Knotennamen und Knotengruppenamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Sie können Platzhalterzeichen für Knotennamen, aber nicht für Knotengruppenamen verwenden. Werden mehrere Knotennamen angegeben, generiert der Server eine Sicherungsgruppe für jeden Knoten und stellt alle Sicherungsgruppen in eine einzelne Gruppe von Ausgabedatenträgern.

### Präfix\_des\_Sicherungsgruppennamens (Erforderlich)

Gibt den Namen der Sicherungsgruppe für den Client-Knoten an. Die maximale Länge des Namens beträgt 30 Zeichen.

Wird ein Name ausgewählt, fügt IBM Spectrum Protect ein Suffix hinzu, um den Sicherungsgruppenamen zu erstellen. Wird die Sicherungsgruppe beispielsweise *mybackupset* genannt, fügt IBM Spectrum Protect eine eindeutige Zahl wie beispielsweise 3099 zum Namen hinzu. Der Sicherungsgruppenname wird dann für IBM Spectrum Protect als *mybackupset.3099* identifiziert. Sollen später Informationen zu dieser Sicherungsgruppe angezeigt werden, kann in dem Namen ein Platzhalterzeichen wie beispielsweise *mybackupset.\** eingefügt oder der vollständig qualifizierte Name wie beispielsweise *mybackupset.3099* angegeben werden.

Werden mehrere Knotennamen oder Knotengruppenamen angegeben, generiert der Server eine Sicherungsgruppe für jeden Knoten oder für jede Knotengruppe und stellt alle Sicherungsgruppen in eine einzelne Gruppe von Ausgabedatenträgern. Jeder Sicherungsgruppe wird derselbe vollständig qualifizierte Name zugeordnet, der aus dem *Präfix\_des\_Sicherungsgruppennamens* und einem Suffix besteht, das vom Server bestimmt wird.

### Dateibereichsname

Gibt die Namen der Dateibereiche an, die die Daten enthalten, die in der Sicherungsgruppe berücksichtigt werden sollen. Dieser Parameter ist wahlfrei. Der angegebene Dateibereichsname kann Platzhalterzeichen enthalten. Es können mehrere Dateibereiche angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird kein Dateibereich angegeben, werden Daten aus allen gesicherten und aktiven Dateibereichen der Clientknoten in der Sicherungsgruppe berücksichtigt.

Für einen Server, der über Clients mit Unterstützung für Unicode-fähige Dateibereiche verfügt, können Sie entweder einen Dateibereichsnamen oder eine Dateibereichs-ID (FSID) eingeben. Wird ein Dateibereichsname eingegeben, muss der Server möglicherweise den eingegebenen Dateibereichsnamen konvertieren. Beispielsweise muss der Server gegebenenfalls den Namen, den Sie eingeben, aus der Zeichenumsetzungstabelle des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich unter dem Parameter NAMETYPE. Geben Sie keinen Dateibereichsnamen an oder geben Sie nur ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter CODETYPE verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

### DEVclass (Erforderlich)

Gibt den Namen der Einheitenklasse für die Datenträger an, auf die die Sicherungsgruppe geschrieben wird. Die maximale Länge des Namens beträgt 30 Zeichen.

Einschränkung: Sie können keine Einheitenklasse mit dem Einheitentyp NAS oder CENTERA angeben.

### SCRatch

Gibt an, ob Arbeitsdatenträger für die Sicherungsgruppe verwendet werden sollen. Wird im Parameter VOLUMES eine Datenträgerliste angegeben, werden Arbeitsdatenträger von dem Server nur verwendet, wenn die Daten nicht auf die angegebenen Datenträger passen. Der Standardwert ist SCRATCH=YES. Gültige Werte:

YES

Gibt an, dass Arbeitsdatenträger für die Sicherungsgruppe verwendet werden sollen.

NO

Gibt an, dass keine Arbeitsdatenträger für die Sicherungsgruppe verwendet werden sollen.

### VOLUMes

Gibt die Namen der Datenträger an, die die Sicherungsgruppe enthalten sollen. Dieser Parameter ist wahlfrei. Es können mehrere Datenträger angegeben werden, die ohne Leerzeichen durch ein Komma voneinander getrennt werden.

Wird dieser Parameter nicht angegeben, werden Arbeitsdatenträger für die Sicherungsgruppe verwendet.

### RETention

Gibt die Anzahl der Tage an, die die Sicherungsgruppe auf dem Server aufbewahrt werden soll. Sie können eine ganze Zahl von 0 bis 30000 angeben. Der Standardwert ist 365 Tage. Gültige Werte:

**Tage**

Gibt die Anzahl der Tage an, die die Sicherungsgruppe auf dem Server aufbewahrt werden soll.

**NOLimit**

Gibt an, dass die Sicherungsgruppe auf dem Server unbegrenzt aufbewahrt werden soll.

Wird NOLIMIT angegeben, werden die Datenträger mit der Sicherungsgruppe vom Server unbegrenzt aufbewahrt, es sei denn, ein Benutzer oder Administrator löscht die Datenträger aus dem Serverspeicher.

**DESCRiption**

Gibt die Beschreibung an, die der Sicherungsgruppe zugeordnet werden soll. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

**Wait**

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

**Yes**

Gibt an, dass der Befehl im Vordergrund verarbeitet wird. Erstellte Nachrichten werden erst angezeigt, wenn die Verarbeitung des Befehls beendet ist. Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

**No**

Gibt an, dass der Befehl im Hintergrund verarbeitet wird. Mit dem Befehl QUERY PROCESS kann die Hintergrundverarbeitung dieses Befehls überwacht werden.

**NAMEType**

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unterstützung für Unicode-aktivierte Dateibereiche verfügt. Sie können diesen Parameter für IBM Spectrum Protect-Clients angeben, die die Betriebssysteme Windows, NetWare oder Macintosh OS X verwenden.

Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen eingeben. Der Standardwert lautet SERVER. Gültige Werte:

**SERVER**

Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren.

**UNICODE**

Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server Probleme beim Zugriff auf die Systemkonvertierungsroutinen hat.

**FSID**

Der Server interpretiert die Dateibereichsnamen als ihre Dateibereichs-IDs (FSIDs).

Wichtig: Gehen Sie bei der Angabe dieses Parameters mit Vorsicht vor, wenn auch mehrere Knotennamen angegeben werden. Verschiedene Knoten können dieselbe Dateibereichs-ID für verschiedene Dateibereiche verwenden oder können verschiedene Dateibereichs-IDs für denselben Dateibereichsnamen verwenden. Wird daher eine Dateibereichs-ID als Dateibereichsname angegeben, kann dies zur Folge haben, dass für einige Knoten die falschen Daten in die Sicherungsgruppe geschrieben werden.

**CODEType**

Angaben, welche Art von Dateibereichen in der Operation berücksichtigt werden soll. Der Standardwert lautet BOTH. Dieser Standardwert bedeutet, dass Dateibereiche unabhängig vom Typ der Codepage eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben oder wenn Sie keine Dateibereichsnamen angeben. Gültige Werte:

**UNICODE**

Nur Dateibereiche einschließen, die in Unicode sind.

**NONUNICODE**

Nur Dateibereiche einschließen, die nicht in Unicode sind.

**BOTH**

Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen.

**PITDate**

Gibt an, dass Dateien, die an dem angegebenen Datum aktiv waren und die noch auf dem IBM Spectrum Protect-Server gespeichert sind, in die Sicherungsgruppe eingeschlossen werden sollen, auch wenn sie zum Zeitpunkt der Befehlsausgabe

inaktiv sind. Dieser Parameter ist wahlfrei. Der Standardwert ist das Datum, an dem der Befehl GENERATE BACKUPSET ausgeführt wird. Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                           | Beschreibung   | Beispiel  |
|--------------------------------|--|---|
| MM/TT/JJJJ                     | Ein bestimmtes Datum                                     | 09/15/1998  |
| TODAY                          | Das aktuelle Datum                                       | TODAY   |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage | TODAY-7 oder -7.<br>Um Dateien einzuschließen, die vor einer Woche aktiv waren, geben Sie PITDATE=TODAY-7 oder PITDATE=-7 an. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.                            | EOLM  |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.      | EOLM-1<br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.                                |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.                      | BOTM  |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage. | BOTM+9<br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.                                     |

#### PITTime

Gibt an, dass Dateien, die zu der angegebenen Uhrzeit aktiv waren und die noch auf dem IBM Spectrum Protect-Server gespeichert sind, in die Sicherungsgruppe eingeschlossen werden sollen, auch wenn sie zum Zeitpunkt der Befehlsausgabe inaktiv sind. Dieser Parameter ist wahlfrei. Wurde ein PITDate angegeben, ist der Standardwert Mitternacht (00:00:00); andernfalls ist der Standardwert die Uhrzeit, zu der der Befehl GENERATE BACKUPSET gestartet wird. Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert                  | Beschreibung   | Beispiel   |
|-----------------------|--|--|
| HH:MM:SS              | Eine bestimmte Uhrzeit am angegebenen PIT-Datum                            | 12:33:28   |
| NOW                   | Die aktuelle Uhrzeit am angegebenen PIT-Datum                              | NOW  |
| NOW+HH:MM oder +HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen PIT-Datum | NOW+03:00 oder +03:00<br>Wird dieser Befehl um 9:00 Uhr mit der Angabe PITTIME=NOW+03:00 oder PITTIME=+03:00 ausgegeben, schließt IBM Spectrum Protect Dateien ein, die um 12:00 Uhr am angegebenen PIT-Datum aktiv waren. |

#### DATATYPE

Gibt an, dass Sicherungsgruppen mit den angegebenen Typen von Daten generiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist, dass Sicherungsgruppen auf Dateiebene generiert werden sollen. Bei der Angabe mehrerer Datentypen müssen die Datentypen durch Kommas und ohne Leerzeichen voneinander getrennt werden.

Der Server generiert eine Sicherungsgruppe für jeden Datentyp und stellt alle Sicherungsgruppen in eine einzelne Gruppe von Ausgabedatenträgern. Jeder Sicherungsgruppe wird derselbe vollständig qualifizierte Name zugeordnet, der aus dem *Präfix\_des\_Sicherungsgruppennamens* und einem Suffix besteht, das vom Server bestimmt wird. Jede Sicherungsgruppe hat jedoch einen anderen Datentyp, wie vom Befehl QUERY BACKUPSET angezeigt wird. Gültige Werte:

#### ALL

Gibt an, dass Sicherungsgruppen für alle Typen von Daten (Dateiebene, Image und Anwendung), die auf dem Server gesichert wurden, generiert werden sollen.

#### FILE

Gibt an, dass eine Sicherungsgruppe auf Dateiebene generiert werden soll. Sicherungsgruppen auf Dateiebene enthalten Dateien und Verzeichnisse, die vom Sicherungsclient gesichert werden. Wurden keine Dateien oder Verzeichnisse vom Sicherungsclient gesichert, wird keine Sicherungsgruppe auf Dateiebene generiert. Dies ist der Standardwert.

#### IMAGE

Gibt an, dass eine Imagesicherungsgruppe generiert werden soll. Imagesicherungsgruppen enthalten Images, die mit dem Befehl BACKUP IMAGE des Sicherungsclients erstellt werden. Imagesicherungsgruppen werden nur generiert, wenn ein Image vom Sicherungsclient gesichert wurde.

## TOC

Gibt an, ob für jede Sicherungsgruppe auf Dateiebene ein Inhaltsverzeichnis gesichert wird. Inhaltsverzeichnisse werden immer für Sicherungsgruppen gesichert, die Image- oder Anwendungsdaten enthalten. Der Parameter TOC wird ignoriert, wenn Image- und Anwendungssicherungsgruppen generiert werden. Ein Inhaltsverzeichnis wird immer für Image- und Anwendungssicherungsgruppen generiert.

Sie sollten bei der Festlegung, ob ein Inhaltsverzeichnis gesichert werden soll, Folgendes berücksichtigen:

- Wird ein Inhaltsverzeichnis für eine Sicherungsgruppe gesichert, können Sie den IBM Spectrum Protect-Webclient für Sichern/Archivieren verwenden, um die gesamte Dateisystemstruktur zu untersuchen und Dateien und Verzeichnisse zum Zurückschreiben auszuwählen. Für die Erstellung eines Inhaltsverzeichnisses müssen Sie das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die Verwaltungsklasse definieren, die mit dem Parameter TOCMGMTCLASS angegeben wird. Die Erstellung eines Inhaltsverzeichnisses erfordert zusätzliche Verarbeitung, zusätzlichen Speicherpoolplatz und möglicherweise einen Mountpunkt während der Sicherungsgruppenoperation.
- Wird ein Inhaltsverzeichnis für eine Sicherungsgruppe nicht gesichert, können Sie dennoch einzelne Dateien oder Verzeichnisstrukturen mit dem Befehl RESTORE BACKUPSET des Clients für Sichern/Archivieren zurückschreiben, wenn Sie den vollständig qualifizierten Namen jeder Datei oder jedes Verzeichnisses kennen, die bzw. das zurückgeschrieben werden soll.

Um den Inhalt von Sicherungsgruppen anzuzeigen, können Sie auch den Befehl QUERY BACKUPSETCONTENTS verwenden.

Dieser Parameter ist wahlfrei. Gültige Werte:

No

Gibt an, dass keine Inhaltsverzeichnisinformationen für Sicherungsgruppen auf Dateiebene gesichert werden.

Preferred

Gibt an, dass Inhaltsverzeichnisinformationen für Sicherungsgruppen auf Dateiebene gesichert werden sollen. Dies ist der Standardwert. Eine Sicherungsgruppe ist jedoch nicht fehlerhaft, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt.

Yes

Gibt an, dass Inhaltsverzeichnisinformationen für jede Sicherungsgruppe auf Dateiebene gesichert werden müssen. Eine Sicherungsgruppe ist fehlerhaft, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt.

## TOCMgmtclass

Gibt den Namen der Verwaltungsklasse an, an die das Inhaltsverzeichnis gebunden werden soll. Wird keine Verwaltungsklasse angegeben, wird das Inhaltsverzeichnis an die Standardverwaltungsklasse für die Maßnahmendomäne gebunden, der der Knoten zugeordnet ist. In diesem Fall müssen Sie für die Erstellung des Inhaltsverzeichnisses das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die angegebene Verwaltungsklasse definieren.

## ALLOWSHREDDable

Gibt an, ob Daten aus einem Speicherpool, der das Schreddern erzwingt, in die Sicherungsgruppe eingeschlossen werden sollen. Dieser Parameter ist wahlfrei. Gültige Werte:

No

Gibt an, dass Daten aus einem Speicherpool, der das Schreddern erzwingt, nicht in die Sicherungsgruppe eingeschlossen werden. Dies ist der Standardwert.

Yes

Gibt an, dass Daten aus einem Speicherpool, der das Schreddern erzwingt, in die Sicherungsgruppe eingeschlossen werden können. Die Daten auf dem Sicherungsgruppendatenträger werden nicht geschreddert.

## Beispiel: Eine Sicherungsgruppe für einen Dateibereich generieren

---

Eine Sicherungsgruppe von dem Dateibereich /srvr generieren, der zu dem Clientknoten JANE gehört. Der Sicherungsgruppe den Namen PERS\_DATA zuordnen und die Sicherungsgruppe 75 Tage aufbewahren. Angeben, dass die Datenträger VOL1 und VOL2 die Daten der Sicherungsgruppe enthalten. Die Datenträger sollen von einer Einheit gelesen werden, die der Einheitenklasse AGADM zugeordnet ist. Eine Beschreibung einschließen.

```
generate backupset jane pers_data /srvr devclass=agadm
retention=75 volumes=voll,vol2 description="Basisimage Bereich 51"
```

## Beispiel: Eine Sicherungsgruppe von einem Unicode-fähigen Dateibereich generieren

---

Eine Sicherungsgruppe von dem Unicode-fähigen Dateibereich \\joe\c\$ generieren, der zum Clientknoten JOE gehört. Der Sicherungsgruppe den Namen JOES\_DATA zuordnen. Angeben, dass der Datenträger VOL1 die Daten der Sicherungsgruppe enthält. Der Datenträger soll von einer Einheit gelesen werden, die der Einheitenklasse AGADM zugeordnet ist. Der Server soll den Dateibereichsnamen \\joe\c\$ aus der Server-Codepage in die Codepage UTF-8 konvertieren.

```
generate backupset joe joes_data \\joe\c$ devclass=agadm
volumes=voll nametype=unicode
```

Tabelle 1. Zugehörige Befehle für GENERATE BACKUPSET

| Befehl                  | Beschreibung  |
|-------------------------|---|
| CANCEL PROCESS          | Bricht einen Serverhintergrundprozess ab.   |
| COPY ACTIVATEDATA       | Kopiert aktive Sicherungsdaten.   |
| DEFINE COPYGROUP        | Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse. |
| DEFINE NODEGROUP        | Definiert eine Gruppe von Knoten.   |
| DEFINE NODEGROUPMEMBER  | Fügt einer Knotengruppe einen Clientknoten hinzu.   |
| DEFINE BACKUPSET        | Definiert eine zuvor generierte Sicherungsgruppe für einen Server.  |
| DELETE BACKUPSET        | Löscht eine Sicherungsgruppe.   |
| DELETE NODEGROUP        | Löscht eine Knotengruppe.   |
| DELETE NODEGROUPMEMBER  | Löscht einen Clientknoten aus einer Knotengruppe.   |
| QUERY BACKUPSET         | Zeigt Sicherungsgruppen an.   |
| GENERATE BACKUPSETTOC   | Generiert ein Inhaltsverzeichnis für eine Sicherungsgruppe.   |
| QUERY NODEGROUP         | Zeigt Informationen zu Knotengruppen an.  |
| QUERY BACKUPSETCONTENTS | Zeigt den Inhalt in Sicherungsgruppen an.   |
| UPDATE BACKUPSET        | Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.   |
| UPDATE COPYGROUP        | Ändert ein oder mehrere Attribute einer Kopiengruppe.   |
| UPDATE NODEGROUP        | Aktualisiert die Beschreibung einer Knotengruppe.   |

## GENERATE BACKUPSETTOC (Inhaltsverzeichnis für eine Sicherungsgruppe generieren)

Verwenden Sie diesen Befehl, um ein Inhaltsverzeichnis für eine Sicherungsgruppe zu generieren, die noch nicht über ein Inhaltsverzeichnis verfügt. Der Client für Sichern/Archivieren verwendet das Inhaltsverzeichnis, um die Sicherungsgruppe anzuzeigen. Damit wird es Benutzern ermöglicht, einzelne Dateien zum Zurückschreiben aus der Sicherungsgruppe auszuwählen.

Die Erstellung eines Inhaltsverzeichnisses für eine Sicherungsgruppe erfordert Speicherbereich im Speicherpool und möglicherweise einen oder mehrere Mountpunkte während der Erstellungsoperation.

### Berechtigungsklasse

Um diesen Befehl ausgeben zu können, müssen Benutzer die Systemberechtigung oder Maßnahmenberechtigung für die Domäne haben, der der Client-Knoten zugeordnet ist.

### Syntax

```
>>-GENerate BACKUPSETTOC--Knotenname--Sicherungsgruppenname----->  
  
.-DATAType---ALL-----  
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->  
|           .-,-----|. |  
|           v           | |  
|'-DATAType---FILE---+-' |  
|           'IMAGE-'     | |  
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|----->  
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----><  
|'-TOCMgmtclass---Klassename-'
```

### Parameter

Knotenname (Erforderlich)

Gibt den Namen des Clientknotens an, dessen Daten in der Sicherungsgruppe enthalten sind. Es können keine Platzhalterzeichen verwendet werden, um einen Namen anzugeben, und es kann keine Liste mit Clientknotenamen angegeben werden.

Sicherungsgruppenname (Erforderlich)

Gibt den Namen der Sicherungsgruppe für den Client-Knoten an. Es können keine Platzhalterzeichen verwendet werden, um einen Namen anzugeben, und es kann keine Liste mit Sicherungsgruppennamen angegeben werden.

DATATYPE

Gibt den Datentyp an, der im Inhaltsverzeichnis enthalten sein soll. Dieser Parameter ist wahlfrei. Standardmäßig werden alle Daten eingeschlossen. Bei der Angabe mehrerer Datentypen müssen die Datentypen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Gültige Werte:

ALL

Gibt an, dass das Inhaltsverzeichnis alle Typen von Daten (Dateiebene, Image und Anwendung) enthält, die in der Sicherungsgruppe gespeichert sind. Dies ist der Standardwert.

FILE

Gibt an, dass das Inhaltsverzeichnis nur Daten auf Dateiebene enthält. Daten auf Dateiebene bestehen aus Dateien und Verzeichnissen, die vom Client für Sichern/Archivieren gesichert wurden. Enthält die Sicherungsgruppe keine Dateien oder Verzeichnisse, wird das Inhaltsverzeichnis nicht generiert.

IMAGE

Gibt an, dass das Inhaltsverzeichnis nur Imagesicherungen enthält. Imagesicherungen bestehen aus Dateisystemimages, die mit dem Befehl BACKUP IMAGE des Sicherungsclients erstellt wurden. Enthält die Sicherungsgruppe keine Imagesicherungen, wird das Inhaltsverzeichnis nicht generiert.

TOCMgmtclass

Gibt den Namen der Verwaltungsklasse an, an die das Inhaltsverzeichnis gebunden werden soll. Wird keine Verwaltungsklasse angegeben, wird das Inhaltsverzeichnis an die Standardverwaltungsklasse für die Maßnahmendomäne gebunden, der der Knoten zugeordnet ist. Wird ein Inhaltsverzeichnis erstellt, müssen Sie das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die angegebene Verwaltungsklasse definieren.

## Beispiel: Ein Inhaltsverzeichnis generieren

Ein Inhaltsverzeichnis für die Sicherungsgruppe PROJX\_DATA generieren, die Daten für den Clientknoten GARY enthält. Das Inhaltsverzeichnis soll an die Standardverwaltungsklasse gebunden werden.



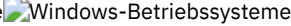
```
generate backupsettoc gary projx_data
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für GENERATE BACKUPSETTOC

| Befehl                  | Beschreibung  |
|-------------------------|---|
| COPY ACTIVE DATA        | Kopiert aktive Sicherungsdaten.   |
| DEFINE COPYGROUP        | Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse. |
| DEFINE NODEGROUP        | Definiert eine Gruppe von Knoten.   |
| DEFINE NODEGROUPMEMBER  | Fügt einer Knotengruppe einen Clientknoten hinzu.   |
| DEFINE BACKUPSET        | Definiert eine zuvor generierte Sicherungsgruppe für einen Server.  |
| DELETE BACKUPSET        | Löscht eine Sicherungsgruppe.   |
| DELETE NODEGROUP        | Löscht eine Knotengruppe.   |
| DELETE NODEGROUPMEMBER  | Löscht einen Clientknoten aus einer Knotengruppe.   |
| GENERATE BACKUPSET      | Generiert eine Sicherungsgruppe mit den Daten eines Clients.  |
| QUERY BACKUPSET         | Zeigt Sicherungsgruppen an.   |
| QUERY NODEGROUP         | Zeigt Informationen zu Knotengruppen an.  |
| QUERY BACKUPSETCONTENTS | Zeigt den Inhalt in Sicherungsgruppen an.   |
| UPDATE BACKUPSET        | Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.   |
| UPDATE COPYGROUP        | Ändert ein oder mehrere Attribute einer Kopiengruppe.   |

| Befehl           | Beschreibung                                      |
|------------------|---|
| UPDATE NODEGROUP | Aktualisiert die Beschreibung einer Knotengruppe. |

## GENERATE DEDUPSTATS (Dateneduplizierungsstatistikdaten generieren)

Verwenden Sie diesen Befehl, um Dateneduplizierungsstatistikdaten für einen Verzeichniscontainerspeicherpool oder einen Cloud-Containerspeicherpool zu generieren, um die Dateneduplizierungsleistung zu bestimmen.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool erforderlich.

### Syntax

```
>>-GENERate DEDUPStats--Poolname----->
. ,-----
V | .-*-----
>-----+Knotenname-----+----->
  '-Knotengruppenname-' | . ,-----
                        | V |
                        +---Dateibereichsname---+
                        | . ,-----
                        | V |
                        '-FSID-----'

.-CODEType----BOTH----- .-MAXPRocess----4-----
>-----+-----+----->
  '-CODEType----+UNICODE----+' '-MAXPRocess----Anzahl-'
      +NONUNICODE-+
      '-BOTH-----'

.-NAMEType----SERVER----- .-Wait----No-----
>-----+-----+----->
  '-NAMEType----+SERVER--+-' '-Wait----+No--+-'
      +UNICODE-+           '-Yes-'
      '-FSID-----'
```

### Parameter

#### Poolname (Erforderlich)

Gibt den Namen des Speicherpools an, der in den Dateneduplizierungsstatistikdaten aufgelistet wird. Für den Speicherpoolnamen können bis zu 30 Zeichen angegeben werden. Wenn Sie mehr als 30 Zeichen angeben, schlägt der Befehl fehl.

Einschränkung: Sie können nur Verzeichniscontainerspeicherpools oder Cloudspeicherpools angeben.

#### Knotenname oder Knotengruppenname (Erforderlich)

Gibt den Namen des Clientknotens oder der definierten Gruppe von Clientknoten an, der bzw. die in den Dateneduplizierungsstatistikdaten aufgelistet wird. Sie können auch eine Kombination von Clientknotenname und Clientknotengruppenname angeben. Sollen mehrere Clientknotenname oder Clientknotengruppenname angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Sie können Platzhalterzeichen für Clientknotenname, aber nicht für Clientknotengruppenname verwenden.

#### Dateibereichsname oder FSID

Gibt die Namen der Dateibereiche in den Dateneduplizierungsstatistikdaten an. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Der Standardwert ist ein Stern. Geben Sie einen der folgenden Werte an:

\*

Geben Sie einen Stern (\*) an, um alle Dateibereiche oder IDs anzuzeigen.

#### Dateibereichsname

Gibt den Namen des Dateibereichs an. Geben Sie mehrere Dateibereiche an, indem Sie die Namen durch Kommas ohne Zwischenleerschritte voneinander trennen. FSID gibt eine Dateibereichs-ID an. Dieser Parameter ist für Clients mit Dateibereichen in Unicode-Format gültig. Geben Sie mehrere Dateibereiche an, indem Sie die Namen durch Kommas ohne Zwischenleerschritte voneinander trennen.

Für Clients mit Dateibereichen in Unicode-Format können Sie entweder einen Dateibereichsnamen oder eine Dateibereichs-ID (FSID) eingeben. Wenn Sie einen Dateibereichsnamen eingeben, muss der Server möglicherweise den eingegebenen Dateibereichsnamen konvertieren. Beispielsweise muss der Server gegebenenfalls den Namen, den Sie eingeben, aus der Codepage des Servers in Unicode konvertieren.

Einschränkungen: Die folgenden Einschränkungen gelten für Dateibereichsnamen und FSIDs:

- Ein Knotenname muss angegeben werden, wenn ein Dateibereichsname angegeben wird.
- In demselben Befehl dürfen nicht gleichzeitig Dateibereichsnamen und Dateibereichs-IDs (FSIDs) angegeben werden.

#### CODEType

Gibt an, welcher Typ von Dateibereichen in den Satz eingeschlossen werden soll. Der Standardwert lautet BOTH. Dieser Standardwert gibt an, dass Dateibereiche unabhängig vom Typ der Codepage eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie einen Stern zum Anzeigen von Informationen zu allen Dateibereichen eingeben. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

##### UNICODE

Dateibereiche einschließen, die ein Unicode-Format haben.

##### NONUNICODE

Dateibereiche einschließen, die kein Unicode-Format haben.

##### BOTH

Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen. Dies ist der Standardwert.

#### MAXProcess

Gibt die maximale Anzahl paralleler Prozesse für die Generierung von Statistikdaten für einen Container in einem Verzeichniscontainer- oder Cloud-Containerspeicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert im Bereich von 1 bis 99 ein. Der Standardwert ist 4.

#### NAMETYPE

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Verwenden Sie diesen Parameter, wenn IBM Spectrum Protect-Clients über Dateibereiche in Unicode-Format verfügen und die Clients unter dem Betriebssystem Windows, NetWare oder Macintosh OS X ausgeführt werden. Dieser Parameter ist wahlfrei.

Dieser Parameter ist erforderlich, wenn Sie einen Knotennamen und einen Dateibereichsnamen bzw. eine Dateibereichs-ID (FSID) angeben.

Einschränkung: Wenn Sie diesen Parameter angeben, darf der Dateibereichsname keinen Stern enthalten.

Geben Sie einen der folgenden Werte an:

##### SERVER

Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren. Dies ist der Standardwert.

##### UNICODE

Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab.

Tipp: Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

##### FSID

Der Server interpretiert die Dateibereichsnamen als ihre FSIDs.

#### Wait

Gibt an, ob die Datenduplizierungsstatistikdaten im Vordergrund oder im Hintergrund generiert werden. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

##### No

Gibt an, dass die Operation im Hintergrund ausgeführt wird. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden. Dies ist der Standardwert.

##### Yes

Gibt an, dass die Operation im Vordergrund ausgeführt wird. Die Ausführung der Operation nimmt unter Umständen viel Zeit in Anspruch. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.

Einschränkung: Sie können den Parameter WAIT=YES nicht an der Serverkonsole angeben.

## Beispiel: Datenduplizierungsstatistikdaten für einen Dateibereich generieren

Datenduplizierungsstatistikdaten für einen Dateibereich mit dem Namen /srvr generieren, der zum Verzeichniscontainerspeicherpool POOL1 gehört, der auf dem Clientknoten NODE1 gespeichert ist.



```
generate dedupstats pool1 node1 /srvr
```




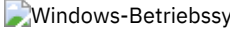
## Beispiel: Dateneduplizierungsstatistikdaten für einen Unicode-fähigen Dateibereich generieren

Dateneduplizierungsstatistikdaten für einen Unicode-fähigen Dateibereich mit dem Namen \\abc\c\$ generieren, der zum Clientknoten NODE2 gehört. Der Dateibereichsname \\abc\c\$ wird aus der Server-Codepage in die Codepage UTF-8 konvertiert.

```
generate dedupstats node2 \\abc\c$ nametype=unicode
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für GENERATE DEDUPSTATS

| Befehl   | Beschreibung                                |
|--|---|
|  <br> DELETE DEDUPSTATS | Löscht Dateneduplizierungsstatistikdaten.   |
|  <br> QUERY DEDUPSTATS  | Zeigt Dateneduplizierungsstatistikdaten an. |

## GRANT-Befehle

Verwenden Sie den Befehl GRANT, um entsprechende Berechtigungen oder entsprechenden Zugriff zu erteilen.

- GRANT AUTHORITY (Administratorberechtigung hinzufügen)
- GRANT PROXYNODE (Proxyberechtigung einem Clientknoten erteilen)

## GRANT AUTHORITY (Administratorberechtigung hinzufügen)

Mit diesem Befehl können einem Administrator Verwaltungsberechtigungsklassen und die Berechtigung für den Zugriff auf Client-Knoten erteilt werden.

Einem uneingeschränkten Maßnahmen- oder Speicheradministrator kann keine eingeschränkte Berechtigung erteilt werden. Hierfür muss dem Administrator die uneingeschränkte Berechtigung mit dem Befehl REVOKE AUTHORITY entzogen und dann mit diesem Befehl die eingeschränkte Berechtigung erteilt werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-GRant AUTHority--Administratorname----->
      .-,------.
      (1)  V      |
>--Classes-----+SYstem-----+----->
              +-Policy-----+
              +-STorage-----+
              +-Operator-----+
              '-Node--| A |- '
>+-----+-----+----->
|          .-,------. |
|          V      | |
| '-D0mains-----Domänenname+-- '
>+-----+-----+-----<
|          .-,------. |
|          (1)  V      | |
| '-STGpools-----Poolname+-- '
A
      .-AUTHority---Access-----
|-----+-----+-----+-----|
| '-AUTHority---+Access+-- '   '-NOde-----Knotenname-----'
```

Anmerkungen:

1. Mindestens einer dieser Parameter muss angegeben werden.

## Parameter

---

Administratorname (Erforderlich)

Gibt den Namen des Administrators an, dem eine Verwaltungsberechtigungsklasse erteilt wird.

Classes

Gibt eine oder mehrere Berechtigungsklassen an, die einem Administrator erteilt werden sollen. Dieser Parameter ist erforderlich, es sei denn, es wird der Parameter STGPOLLS angegeben. Es können mehrere Berechtigungsklassen angegeben werden, wobei die einzelnen Namen durch Komma voneinander getrennt werden müssen. Gültige Klassen sind:

System

Gibt an, dass einem Administrator die Systemberechtigung erteilt werden soll. Ein Systemadministrator verfügt über die höchste Berechtigungsstufe in IBM Spectrum Protect. Ein Systemadministrator kann alle Verwaltungsbefehle ausgeben und hat die Berechtigung, alle Maßnahmendomänen und alle Speicherpools zu verwalten. Wenn einem Administrator die Systemberechtigung erteilt wird, dürfen keine weiteren Berechtigungsklassen oder die Parameter DOMAINS und STGPOLLS angegeben werden. Nur ein Systemadministrator kann anderen Administratoren Berechtigungen erteilen.

Policy

Gibt an, dass einem Administrator die Maßnahmenberechtigung erteilt werden soll. Wird der Parameter DOMAINS nicht angegeben, wird uneingeschränkte Maßnahmenberechtigung erteilt. Ein Administrator mit uneingeschränkter Maßnahmenberechtigung kann Befehle ausgeben, die alle vorhandenen Maßnahmendomänen sowie alle Maßnahmendomänen betreffen, die in Zukunft definiert werden. Ein Administrator mit uneingeschränkter Maßnahmenberechtigung kann keine Maßnahmendomänen definieren, löschen oder kopieren. Verwenden Sie den Befehl GRANT AUTHORITY mit CLASSES=POLICY und ohne den Parameter DOMAINS, um die eingeschränkte Maßnahmenberechtigung für einen Administrator in die uneingeschränkte Maßnahmenberechtigung zu erweitern.

STorage

Gibt an, dass einem Administrator die Speicherberechtigung erteilt werden soll. Wenn der Parameter STGPOLLS nicht angegeben wird, wird uneingeschränkte Speicherberechtigung erteilt. Ein Administrator mit uneingeschränkter Speicherberechtigung kann alle Befehle ausgeben, die Speicherressourcen für den Server zuordnen und steuern. Ein Administrator mit uneingeschränkter Speicherberechtigung kann Befehle ausgeben, die alle vorhandenen Speicherpools sowie alle Speicherpools betreffen, die in Zukunft definiert werden. Ein Administrator mit uneingeschränkter Speicherberechtigung kann Speicherpools nicht definieren oder löschen. Verwenden Sie den Befehl GRANT AUTHORITY mit CLASSES=STORAGE und ohne den Parameter STGPOLLS, um die eingeschränkte Speicherberechtigung für einen Administrator in die uneingeschränkte Speicherberechtigung zu erweitern.

Operator

Gibt an, dass einem Administrator die Bedienerberechtigung erteilt werden soll. Ein Administrator mit Bedienerberechtigung kann Befehle ausgeben, die den direkten Betrieb des Servers und die Verfügbarkeit von Speicherdatenträgern steuern.

Node

Gibt an, dass einem Benutzer eine Knotenberechtigung erteilt werden soll. Ein Benutzer mit Clientknotenberechtigung kann mit einer Benutzer-ID mit Administratorberechtigung und einem Kennwort von einem fernen System aus auf einen Web-Client für Sichern/Archivieren zugreifen, wenn der Benutzer über die Eignerberechtigung (Owner) oder Zugriffsberechtigung (Access) verfügt. Die Zugriffsberechtigung (Access) ist der Standardwert für eine Knotenberechtigungsklasse. Achtung: Wird die Knotenberechtigungsklasse angegeben, muss auch der Parameter DOMAIN oder der Parameter NODE angegeben werden, jedoch nicht beide Parameter.

AUTHority

Gibt die Berechtigungsstufe eines Benutzers mit Knotenberechtigung an. Dieser Parameter ist wahlfrei.

Hat ein Administrator bereits die System- oder Maßnahmenberechtigung für die Maßnahmendomäne, zu der der Knoten gehört, wird mit diesem Befehl die Berechtigung des Administrators nicht geändert.

Gültige Berechtigungsstufen sind:

Access

Gibt an, dass einem Benutzer mit der Knotenberechtigungsklasse die Clientzugriffsberechtigung erteilt werden soll. Dies ist der Standardwert, wenn CLASSES=NODE angegeben wird. Ein Benutzer mit Clientzugriffsberechtigung kann auf einen Web-Client für Sichern/Archivieren zugreifen und Sicherungs- und Zurückschreibungsaktionen auf diesem Client ausführen.

Achtung: Ein Benutzer mit Clientzugriffsberechtigung kann nicht auf diesen Client von einem anderen System aus zugreifen, indem der Parameter -NODENAME oder -VIRTUALNODENAME verwendet wird.

Ein Clientknoten kann die Option REVOKEREMOTEACCESS definieren, um zu verhindern, dass ein Benutzer, der über die Knotenberechtigung mit Clientzugriffsberechtigung verfügt, auf eine Clientdatenstation zugreift, auf der ein Web-Client ausgeführt wird. Diese Option gilt nicht für Administratoren mit Clienteignerberechtigung, Systemberechtigung oder Maßnahmenberechtigung für die Maßnahmendomäne, zu der der Knoten gehört.

#### Owner

Gibt an, dass einem Benutzer mit der Knotenberechtigungskategorie die Clienteignerberechtigung erteilt werden soll. Ein Benutzer mit Clienteignerberechtigung kann über die Web-Client-Schnittstelle auf einen Web-Client für Sichern/Archivieren und außerdem auf die Daten von einem anderen Client aus zugreifen, indem der Parameter -NODENAME oder -VIRTUALNODENAME verwendet wird.

#### Domains

Gibt an, dass dem Administrator Clientzugriffsberechtigung oder Clienteignerberechtigung für alle Clients in der angegebenen Maßnahmendomäne erteilt werden soll. Dieser Parameter kann nicht zusammen mit dem Parameter NODE verwendet werden.

#### NOde

Gibt an, dass dem Administrator Clientzugriffsberechtigung oder Clienteignerberechtigung für den Knoten erteilt werden soll. Dieser Parameter kann nicht zusammen mit dem Parameter DOMAIN verwendet werden.

#### Domains

Gibt bei Verwendung mit CLASSES=POLICY an, dass einem Administrator die eingeschränkte Maßnahmenberechtigung erteilt werden soll.

Mit der eingeschränkten Maßnahmenberechtigung kann ein Administrator einen Teil der Maßnahmenbefehle für die Domänen ausgeben, für die der Administrator eine Berechtigung hat. Mit diesem Parameter kann einem Administrator mit eingeschränkter Maßnahmenberechtigung zusätzliche Maßnahmendomänenberechtigung erteilt werden. Dieser Parameter ist wahlfrei. Es können mehrere Maßnahmendomänen angegeben werden, wobei die einzelnen Namen durch ein Komma getrennt werden müssen.

Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Es wird die Berechtigung für alle übereinstimmenden Maßnahmendomänen erteilt.

#### STGpools

Gibt an, dass einem Administrator die eingeschränkte Speicherberechtigung erteilt werden soll. Wenn der Parameter STGPools angegeben wird, ist CLASSES=STORAGE wahlfrei.

Mit der eingeschränkten Speicherberechtigung kann ein Administrator einen Teil der Speicherbefehle für die Speicherpools ausgeben, für die der Administrator eine Berechtigung hat. Mit diesem Parameter kann einem Administrator mit eingeschränkter Speicherberechtigung zusätzliche Speicherpoolberechtigung erteilt werden. Dieser Parameter ist wahlfrei. Es können mehrere Speicherpools angegeben werden, wobei die einzelnen Namen durch ein Komma voneinander getrennt werden müssen.

Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Für alle übereinstimmenden Speicherpools wird die Berechtigung erteilt.

## Beispiel: Einem Administrator die Systemberechtigung erteilen

---

Administrator Larry die Systemberechtigung erteilen.

```
grant authority larry classes=system
```

## Beispiel: Zugriff auf zusätzliche Maßnahmendomänen erteilen

---

Zusätzliche Maßnahmendomänen angeben, die der Administrator CLAUDIA mit eingeschränkter Maßnahmenberechtigung verwalten kann.

```
grant authority claudia domains=employee_records,progl
```

## Beispiel: Einem Administrator die uneingeschränkte Speicherberechtigung und die eingeschränkte Maßnahmenberechtigung erteilen

---

Administrator TOM die uneingeschränkte Speicherberechtigung und die eingeschränkte Maßnahmenberechtigung für die Domänen erteilen, deren Namen mit EMP beginnen.

```
grant authority tom classes=storage domains=emp*
```

## Beispiel: Einem Administrator Berechtigung erteilen, die auf einen bestimmten Knoten beschränkt ist

---

Dem Benutzer HELP Knotenberechtigung erteilen, damit die Help-Desk-Mitarbeiter den Clientknoten LABCLIENT beim Sichern oder Zurückschreiben von Daten unterstützen können, ohne über andere IBM Spectrum Protect-Berechtigungen auf höherer Ebene zu verfügen.

```
grant authority help classes=node node=labclient
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für GRANT AUTHORITY

| Befehl           | Beschreibung   |
|------------------|--|
| QUERY ADMIN      | Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.                                 |
| REVOKE AUTHORITY | Widerruft eine oder mehrere Berechtigungsklassen oder schränkt den Zugriff auf Maßnahmendomänen und Speicherpools ein. |

## GRANT PROXYNODE (Proxyberechtigung einem Clientknoten erteilen)

Verwenden Sie diesen Befehl, um einem Clientknoten auf dem IBM Spectrum Protect-Server Proxyberechtigung zu erteilen.

Zielclientknoten sind Eigner der Daten und Agentenknoten arbeiten für die Zielknoten. Wurde die Proxyberechtigung für einen Zielclientknoten erteilt, kann ein Agentenknoten Sicherungs- und Zurückschreibungsoperationen für den Zielknoten ausführen. Daten, die vom Agentenknoten für den Zielknoten gespeichert werden, werden unter dem Namen des Zielknotens im Serverspeicher gespeichert.

## Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Systemberechtigung
- Uneingeschränkte Maßnahmenberechtigung

## Syntax

```
>>-GRant PROXynode TArget-----Zielknotenname----->  
>--AGent-----Agentenknotenname-----<
```

## Parameter

TArget (Erforderlich)

Gibt den Namen des Knotens an, der Eigner der Daten ist. Namen mit Platzhalterzeichen können zur Angabe des Zielknotennamens nicht verwendet werden.

AGent (Erforderlich)

Gibt den Namen des Knotens an, der Operationen für den Zielknoten ausführt. Der Agentenknoten muss sich nicht in derselben Domäne wie der Zielknoten befinden. Platzhalterzeichen und durch Kommas getrennte Listen mit Knotennamen sind zulässig.

## Beispiel: Einem Clientknoten Proxy-Berechtigung erteilen

Angenommen, MOE und JOE sind Agentenknoten in einem NAS-Cluster und werden zum Sichern und Zurückschreiben gemeinsam genutzter NAS-Daten verwendet. Um eine Proxy-Berechtigungsbeziehung für den Zielknoten NASCLUSTER zu erstellen, geben Sie den folgenden Befehl aus:

```
grant proxynode target=nascluster agent=moe,joe
```

Geben Sie den folgenden Befehl auf dem Agentenknoten MOE zum Sichern von NAS-Clusterdaten aus, die auf dem Laufwerk E: gespeichert sind. Der Name des Zielknotens ist NASCLUSTER.

```
dsmc -asnode=nascluster incremental e:
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für GRANT PROXYNODE

| Befehl           | Beschreibung   |
|------------------|--|
| QUERY PROXYNODE  | Zeigt die Knoten an, die die Berechtigung als Proxyknoten haben. |
| REVOKE PROXYNODE | Entzieht einem Agentenknoten die Proxyberechtigung.              |

## HALT (Server abschalten)

Mit diesem Befehl kann der Server abgeschaltet werden. Der Befehl HALT erzwingt ein sofortiges Abschalten, wobei alle Verwaltungs- und Clientknotensitzungen abgebrochen werden, auch wenn sie noch nicht beendet sind.

Alle laufenden Transaktionen, die durch den Befehl HALT unterbrochen werden, werden beim Neustart des Servers rückgängig gemacht. Der Befehl HALT darf nur verwendet werden, wenn die Verwaltungs- und Clientknotensitzungen abgeschlossen oder abgebrochen wurden. Um den Server abzuschalten, ohne die Verwaltungs- und Client-Knotensitzungen stark zu beeinträchtigen, folgende Schritte ausführen:

1. Mit dem Befehl DISABLE SESSIONS verhindern, dass neue Clientknotensitzungen gestartet werden.
2. Mit dem Befehl QUERY SESSIONS alle vorhandenen Verwaltungs- und Clientknotensitzungen identifizieren.
3. Alle vorhandenen Verwaltungs- und Clientknotensitzungen über das geplante Abschalten des Servers informieren (außerhalb von IBM Spectrum Protect).
4. Mit dem Befehl CANCEL SESSIONS alle vorhandenen Verwaltungs- und Clientknotensitzungen abrechnen.
5. Mit dem Befehl HALT den Server abschalten und alle Verwaltungs- und Clientknotensitzungen stoppen.

Tipp:

Der Befehl HALT kann mit der Serveroption ALIASHALT repliziert werden. Verwenden Sie die Serveroption, um einen anderen Term als HALT zu definieren, mit dem dieselbe Funktion ausgeführt wird. Der Befehl HALT behält jedoch seine normale Funktion, die Serveroption bietet eine zusätzliche Methode zur Ausgabe des Befehls HALT. Für zusätzliche Informationen siehe ALIASHALT.

## Berechtigungsklasse

Für diesen Befehl ist die System- oder Bedienerberechtigung erforderlich.

## Syntax

```
>>-HALT----->>
```

## Parameter

Keine.

## Beispiel: Den Server abschalten

Den Server über die Serverkonsole oder über einen Verwaltungsclient abschalten. Alle Benutzeraktivitäten werden sofort gestoppt und neue Aktivitäten können nicht gestartet werden.

```
halt
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für HALT

| Befehl           | Beschreibung   |
|------------------|--|
| CANCEL PROCESS   | Bricht einen Serverhintergrundprozess ab.  |
| CANCEL SESSION   | Bricht aktive Sitzungen mit dem Server ab.   |
| DISABLE SESSIONS | Verhindert, dass neue Sitzungen auf IBM Spectrum Protect zugreifen, lässt jedoch zu, dass bestehende Sitzungen fortgesetzt werden. |
| ENABLE SESSIONS  | Nimmt die Serveraktivität nach einem Befehl DISABLE oder ACCEPT DATE wieder auf.   |
| QUERY PROCESS    | Zeigt Informationen über Hintergrundprozesse an.   |

| Befehl        | Beschreibung   |
|---------------|--|
| QUERY SESSION | Zeigt Informationen zu allen aktiven Administrator- und Clientsitzungen mit IBM Spectrum Protect an. |

## HELP (Hilfe für Befehle und Fehlernachrichten anfordern)

Mit diesem Befehl können Verwaltungsbefehle und Fehlernachrichten angezeigt werden. Der Befehl kann von einem Verwaltungsbefehlszeilenclient ausgegeben werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Help-----<<
+-Numer_des_Hilfethemas-----+
|                               |
|                               |
|                               |
|                               |
+-Befehlsname-----+-----+
|                               |
|                               |
+-Nachrichtnummer-----+-----+
+-Serveroptionsname-----+-----+
+-Dienstprogrammname-----+-----+
```

### Parameter

#### Numer\_des\_Hilfethemas

Gibt die Nummer Ihrer Auswahl aus den Hilfethemen an. Dieser Parameter ist wahlfrei.

Die Nummern der Hilfethemen werden im Inhaltsverzeichnis angezeigt. Beispiel:

```
3.0 Verwaltungsbefehle
...
3.13.10 DEFINE DEVCLASS (Einheitenklasse definieren)
  3.13.10.1 DEFINE DEVCLASS (Einheitenklasse 3590 definieren)
  3.13.10.2 DEFINE DEVCLASS (Einheitenklasse 3592 definieren)
...
```

Die Nummer des Hilfethemas für den Befehl DEFINE DEVCLASS für die Einheitenklasse 3592 ist 3.13.10.2.

#### Befehlsname

Gibt den Namen des Verwaltungsbefehls an, der angezeigt werden soll. Dieser Parameter ist wahlfrei.

#### Unterbefehlsname

Gibt bis zu zwei der Unterbefehlsnamen an, die dem Namen des Verwaltungsbefehls zugeordnet sind, der angezeigt werden soll. Dieser Parameter ist wahlfrei.

#### Nachrichtnummer

Gibt die Nummer der Nachricht an, für die Informationen angezeigt werden sollen. Dieser Parameter ist wahlfrei. Es können Hilfeinformationen für Servernachrichten (Präfix ANR) und Clientnachrichten (Präfix ANE oder ANS) angefordert werden. Das Präfix und den Bewertungscode nicht angeben, wenn die Nummer einer Fehlernachricht angegeben wird.

#### Serveroptionsname

Gibt den Namen der Serveroption an, für die Informationen angezeigt werden sollen. Dieser Parameter ist wahlfrei.

#### Dienstprogrammname

Gibt den Namen des Serverdienstprogramms an, für das Informationen angezeigt werden sollen. Dieser Parameter ist wahlfrei.

### Beispiel: Die Hilfethemen anzeigen

Die Hilfethemen für die Befehlszeilenschnittstelle anzeigen.

```
Hilfe
```

Teilausgabe:

```
1.0 Server von der Befehlszeile aus verwalten
  1.1 Befehle mit dem Verwaltungsclient ausgeben
```

- 1.1.1 Verwaltungsclient starten und stoppen
- 1.1.2 Serveraktivitäten vom Verwaltungsclient aus überwachen

## Beispiel: Ein Hilfethema unter Verwendung der Nummer des Hilfethemas anzeigen

---

Hilfetext unter Verwendung der Nummer des Hilfethemas aufrufen. Die Nummer des Hilfethemas für den Befehl DEFINE DEVCLASS für die Einheitenklasse 3592 ist 3.13.10.2.

```
help 3.13.10.2
```

## Beispiel: Hilfetext für einen Befehl anzeigen

---

Hilfetext für die REMOVE-Befehle anzeigen.

```
help remove
```

3.44 REMOVE-Befehle

Mit den REMOVE-Befehlen kann ein Objekt entfernt werden.

Die folgende Liste enthält die REMOVE-Befehle:

- \* 3.44.1, "REMOVE ADMIN (Administrator löschen)"
- \* 3.44.2, "REMOVE NODE (Knoten oder zugehörigen Maschinenknoten löschen)"

## Beispiel: Hilfetext für eine bestimmte Fehlernachricht anzeigen

---

Hilfetext zu der Fehlernachricht ANR2535E aufrufen.

```
help 2535
```

```
ANR2535E  Befehl: Der Knotenname kann nicht entfernt oder umbenannt
werden,          da ihm eine Einheit zum Versetzen von Daten zugeordnet ist.
Erläuterung: Sie haben versucht, einen Knoten zu entfernen oder
umzubenennen, dem eine Einheit zum Versetzen von Daten zugeordnet ist.
Systemaktion: Der Knoten wird vom Server nicht entfernt oder umbenannt.
Benutzeraktion: Um den Knoten zu entfernen oder umzubenennen, löschen
Sie die zugeordnete Einheit zum Versetzen von Daten und geben Sie den
Befehl erneut aus.
```

## Beispiel: Hilfetext für eine bestimmte Option anzeigen

---

Die Beschreibung, die Syntax und ein Beispiel für die Serveroption COMMETHOD anzeigen.

```
help commethod
```

## Beispiel: Hilfetext für ein bestimmtes Dienstprogramm anzeigen

---

Die Beschreibung, die Syntax und ein Beispiel für das Dienstprogramm DSMSERV anzeigen.

```
help dmserv
```

# IDENTIFY DUPLICATES (Doppelte Daten in einem Speicherpool identifizieren)

---

Verwenden Sie diesen Befehl, um Prozesse zu starten oder zu stoppen, die doppelte Daten in einem Speicherpool identifizieren. Sie können die Anzahl der Prozesse zum Identifizieren doppelter Daten und ihre Dauer angeben.

Wenn Sie einen neuen Speicherpool für die Datendeduplizierung erstellen, können Sie 0 - 50 Prozesse zum Identifizieren doppelter Daten angeben. IBM Spectrum Protect startet die angegebene Anzahl Prozesse zum Identifizieren doppelter Daten automatisch, wenn der Server gestartet wird. Wenn Sie die Prozesse nicht stoppen, werden sie unbegrenzt ausgeführt.

Dieser Befehl betrifft nur die serverseitige Deduplizierungsverarbeitung. Bei der clientseitigen Datendeduplizierungsverarbeitung werden Duplikate auf dem Client für Sichern/Archivieren identifiziert.

Mit dem Befehl IDENTIFY DUPLICATES können Sie weitere Prozesse starten, einige oder alle Prozesse stoppen und eine Zeit angeben, die die Änderung wirksam bleibt. Wenn Sie die Anzahl der Prozesse zum Identifizieren doppelter Daten erhöht oder verringert haben, können Sie mit dem Befehl IDENTIFY DUPLICATES die Anzahl der Prozesse auf den in der Speicherpooldefinition angegebenen Wert zurücksetzen.

Haben Sie keine Prozesse zum Identifizieren doppelter Daten in der Speicherpooldefinition angegeben, können Sie mit dem Befehl IDENTIFY DUPLICATES alle Prozesse manuell starten und stoppen.

Mit diesem Befehl werden ein oder mehrere Hintergrundprozesse gestartet oder gestoppt, die Sie mit dem Befehl CANCEL PROCESS abbrechen können. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Wichtig:

- Sie können auch die Anzahl der Prozesse zum Identifizieren doppelter Daten ändern, indem Sie mit dem Befehl UPDATE STGPOOL die Speicherpooldefinition aktualisieren. Wenn Sie eine Speicherpooldefinition aktualisieren, können Sie jedoch keine Dauer angeben. Die Prozesse, die Sie in der Speicherpooldefinition angeben, werden unbegrenzt ausgeführt oder bis Sie den Befehl IDENTIFY DUPLICATES ausgeben, die Speicherpooldefinition erneut aktualisieren oder einen Prozess abbrechen.

Bei der Ausgabe des Befehls IDENTIFY DUPLICATES wird nicht die Einstellung für die Anzahl der Prozesse zum Identifizieren doppelter Daten in der Speicherpooldefinition geändert.

- Prozesse zum Identifizieren doppelter Daten können entweder aktiv oder inaktiv sein. Prozesse, die gegenwärtig eine Deduplizierung ausführen, sind aktiv. Prozesse, die auf Dateien warten, die dedupliziert werden sollen, sind inaktiv. Prozesse bleiben inaktiv, bis Datenträger mit Daten, die dedupliziert werden sollen, verfügbar werden. Prozesse werden nur gestoppt, wenn sie abgebrochen werden oder wenn Sie die Anzahl der Prozesse zum Identifizieren doppelter Daten für den Speicherpool durch einen Wert ersetzen, der kleiner als der angegebene Wert ist. Bevor ein Prozess zum Identifizieren doppelter Daten stoppt, muss er die Datei, für die gegenwärtig eine Deduplizierung ausgeführt wird, fertig stellen.

Die Ausgabe des Befehls QUERY PROCESS für einen Prozess zum Identifizieren doppelter Daten umfasst die Gesamtzahl Byte und Dateien, die seit dem ersten Start des Prozesses verarbeitet wurden. Wenn beispielsweise ein Prozess zum Identifizieren doppelter Daten vier Dateien verarbeitet, dann inaktiv ist und anschließend fünf weitere Dateien verarbeitet, beträgt die Gesamtzahl der verarbeiteten Dateien neun.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-IDentify DUPLicates--Speicherpoolname----->
>--+-----+--+-----+-----<
  '-NUMPRocess----Anzahl-'  '-DURation----Minuten-'
```

## Parameter

---

Speicherpoolname (Erforderlich)

Gibt den Namen des Speicherpools an, in dem doppelte Daten identifiziert werden sollen. Sie können Platzhalterzeichen verwenden.

NUMPRocess

Gibt die Anzahl der Prozesse zum Identifizieren doppelter Daten an, die nach Beendigung des Befehls ausgeführt werden sollen. Sie können 0 - 50 Prozesse angeben. Der Wert, den Sie für diesen Parameter angeben, überschreibt den in der Speicherpooldefinition angegebenen Wert oder den neuesten Wert, den Sie bei der letzten Ausgabe dieses Befehls angegeben haben. Geben Sie null an, werden alle Prozesse zum Identifizieren doppelter Daten gestoppt.

Dieser Parameter ist wahlfrei. Wenn Sie keinen Wert angeben, startet oder stoppt der Server Prozesse zum Identifizieren doppelter Daten, so dass die Anzahl der Prozesse mit der in der Speicherpooldefinition angegebenen Anzahl identisch ist.

Beispiel: Angenommen, Sie definieren einen neuen Speicherpool und geben zwei Prozesse zum Identifizieren doppelter Daten an. Später geben Sie den Befehl IDENTIFY DUPLICATES aus, um die Anzahl der Prozesse auf vier zu erhöhen. Geben Sie den Befehl IDENTIFY DUPLICATES erneut aus, ohne einen Wert für den Parameter NUMPROCESS anzugeben, stoppt der Server zwei Prozesse zum Identifizieren doppelter Daten.

Haben Sie bei der Definition der Speicherpooldefinition null Prozesse angegeben und geben Sie IDENTIFY DUPLICATES ohne einen Wert für NUMPROCESS aus, werden alle gegenwärtig ausgeführten Prozesse zum Identifizieren doppelter Daten gestoppt, und der Server startet keine neuen Prozesse.

Hinweis: Wenn Sie IDENTIFY DUPLICATES ohne einen Wert für NUMPROCESS ausgeben, ist der Parameter DURATION nicht verfügbar. Die in der Speicherpooldefinition angegebenen Prozesse zum Identifizieren doppelter Daten werden unbegrenzt ausgeführt oder bis Sie den Befehl IDENTIFY DUPLICATES erneut ausgeben, die Speicherpooldefinition aktualisieren oder einen Prozess abbrechen.



Wenn der Server einen Prozess zum Identifizieren doppelter Daten stoppt, stellt der Prozess die aktuelle physische Datei fertig, und wird dann gestoppt. Daher kann es einige Minuten dauern, bis die Anzahl der Prozesse zum Identifizieren doppelter Daten erreicht ist, die Sie als Wert für diesen Parameter angegeben haben.

#### DURation

Gibt die maximale Anzahl Minuten (1 - 9999) an, die dieser Befehl wirksam bleibt. Nach Ablauf der angegebenen Zeit startet oder stoppt der Server Prozesse zum Identifizieren doppelter Daten, so dass die Anzahl der Prozesse mit der in der Speicherpooldefinition angegebenen Anzahl identisch ist.

Dieser Parameter ist wahlfrei. Wird kein Wert angegeben, werden die Prozesse, die nach Ausgabe des Befehls ausgeführt werden, unbegrenzt ausgeführt. Sie werden nur beendet, wenn Sie den Befehl IDENTIFY DUPLICATES erneut ausgeben, die Speicherpooldefinition aktualisieren oder einen Prozess abbrechen.

Beispiel: Wenn Sie einen Speicherpool mit zwei Prozessen zum Identifizieren doppelter Daten definieren und den Befehl IDENTIFY DUPLICATES mit `DURATION=60` und `NUMPROCESS=4` ausgeben, startet der Server zwei weitere Prozesse zum Identifizieren doppelter Daten, die 60 Minuten ausgeführt werden. Nach Ablauf dieser Zeit stellen zwei Prozesse die Dateien fertig, die gerade bearbeitet werden, und werden gestoppt. Die beiden Prozesse, die gestoppt werden, sind möglicherweise nicht die beiden Prozesse, die durch Ausgabe dieses Befehls gestartet wurden.

Der Server stoppt inaktive Prozesse zuerst. Müssen nach dem Stoppen aller inaktiven Prozesse weitere Prozesse gestoppt werden, informiert der Server aktive Prozesse darüber, dass sie gestoppt werden.

Wenn der Server einen Prozess zum Identifizieren doppelter Daten stoppt, stellt der Prozess die aktuelle physische Datei fertig, und wird dann gestoppt. Daher kann es einige Minuten dauern, bis die Zeit erreicht wird, die Sie als Wert für diesen Parameter angegeben haben.

## Beispiel: Die Anzahl und Dauer der Prozesse zum Identifizieren doppelter Daten steuern

In diesem Beispiel haben Sie drei Prozesse zum Identifizieren doppelter Daten in der Speicherpooldefinition angegeben. Sie verwenden den Befehl IDENTIFY DUPLICATES, um die Prozessanzahl zu ändern und um die Zeit anzugeben, die die Änderung wirksam bleiben soll.

Tabelle 1. Prozesse zum Identifizieren doppelter Daten manuell steuern

| In der Speicherpooldefinition sind drei Prozesse zum Identifizieren doppelter Daten angegeben. Mit dem Befehl IDENTIFY DUPLICATES geben Sie... | ...und eine Dauer von... | Das Ergebnis ist...  |
|--|--------------------------|--|
| 2 Prozesse zum Identifizieren doppelter Daten an.  | Keine angegeben          | Ein Prozess zum Identifizieren doppelter Daten beendet die Datei, die gerade bearbeitet wird (falls vorhanden), und wird dann gestoppt. Zwei Prozesse werden unbegrenzt ausgeführt oder bis Sie den Befehl IDENTIFY DUPLICATES erneut ausgeben, die Speicherpooldefinition aktualisieren oder einen Prozess abbrechen.                               |
|  | 60 Minuten               | Ein Prozess zum Identifizieren doppelter Daten beendet die Datei, die gerade bearbeitet wird (falls vorhanden), und wird dann gestoppt. Nach 60 Minuten startet der Server einen Prozess, so dass drei Prozesse ausgeführt werden.   |
| 4 Prozesse zum Identifizieren doppelter Daten an.  | Keine angegeben          | Der Server startet einen Prozess zum Identifizieren doppelter Daten. Vier Prozesse werden unbegrenzt ausgeführt oder bis Sie den Befehl IDENTIFY DUPLICATES erneut ausgeben, die Speicherpooldefinition aktualisieren oder einen Prozess abbrechen.  |
|  | 60 Minuten               | Der Server startet einen Prozess zum Identifizieren doppelter Daten. Nach Ablauf von 60 Minuten beendet ein Prozess die Datei, die gerade bearbeitet wird (falls vorhanden), und wird dann gestoppt. Der zusätzliche Prozess, der durch diesen Befehl gestartet wird, ist möglicherweise nicht der Prozess, der nach Ablauf der Dauer gestoppt wird. |

| In der Speicherpooldefinition sind drei Prozesse zum Identifizieren doppelter Daten angegeben. Mit dem Befehl IDENTIFY DUPLICATES geben Sie... | ...und eine Dauer von... | Das Ergebnis ist...   |
|--|--------------------------|---|
| 0 Prozesse zum Identifizieren doppelter Daten an.  | Keine angegeben          | Alle Prozesse zum Identifizieren doppelter Daten beenden die Dateien, die gerade bearbeitet werden (falls vorhanden), und werden dann gestoppt. Diese Änderung bleibt unbegrenzt erhalten oder bis Sie den Befehl IDENTIFY DUPLICATES erneut ausgeben, die Speicherpooldefinition aktualisieren oder einen Prozess abbrechen. |
|  | 60 Minuten               | Alle Prozesse zum Identifizieren doppelter Daten beenden die Dateien, die gerade bearbeitet werden (falls vorhanden), und werden dann gestoppt. Nach Ablauf von 60 Minuten startet der Server drei Prozesse.  |
| Keine angegeben  | Nicht verfügbar          | Die Anzahl der Prozesse zum Identifizieren doppelter Daten wird auf die in der Speicherpooldefinition angegebene Prozessanzahl zurückgesetzt. Diese Änderung bleibt unbegrenzt erhalten oder bis Sie den Befehl IDENTIFY DUPLICATES erneut ausgeben, die Speicherpooldefinition aktualisieren oder einen Prozess abbrechen.   |

## Beispiel: Duplikate in einem Speicherpool identifizieren

Duplikate in dem Speicherpool STGPOOLA unter Verwendung von drei Prozessen zum Identifizieren doppelter Daten identifizieren. Angeben, dass diese Änderung 60 Minuten wirksam bleiben soll.

```
identify duplicates stgpoola duration=60 numprocess=3
```

## Zugehörige Befehle

Tabelle 2. Zugehörige Befehle für IDENTIFY DUPLICATES

| Befehl         | Beschreibung   |
|----------------|--|
| CANCEL PROCESS | Bricht einen Serverhintergrundprozess ab.  |
| DEFINE STGPOOL | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern. |
| QUERY CONTENT  | Zeigt Informationen über Dateien in einem Speicherpooldatenträger an.              |
| QUERY PROCESS  | Zeigt Informationen über Hintergrundprozesse an.                                   |
| QUERY STGPOOL  | Zeigt Informationen zu Speicherpools an.   |
| UPDATE STGPOOL | Ändert die Attribute eines Speicherpools.  |

## Befehle IMPORT

Mit den IMPORT-Befehlen können Informationen von Exportdatenträgern auf einen IBM Spectrum Protect-Server importiert werden.

Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten importiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls IMPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.

- IMPORT ADMIN (Administratorinformationen importieren)
- IMPORT NODE (Clientknoteninformationen importieren)
- IMPORT POLICY (Maßnahmeninformationen importieren)
- IMPORT SERVER (Serverinformationen importieren)

## IMPORT ADMIN (Administratorinformationen importieren)

Mit diesem Befehl können Administrator- und Berechtigungsdefinitionen von Administratoren von Exportdatenträgern in den IBM Spectrum Protect-Server importiert werden.

Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten importiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls IMPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.

Mit dem Befehl QUERY ACTLOG kann der Status der Importoperation angezeigt werden.

Diese Informationen können auch über die Serverkonsole angezeigt werden.

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn ein Hintergrundprozess des Befehls IMPORT ADMIN abgebrochen wird, wurden einige der Daten bereits importiert. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Einschränkung:

- Sind die Versionen des Zielservers und Quellenservers nicht kompatibel, kann die Operation möglicherweise nicht ausgeführt werden.
- Wenn die Administratordefinition, die importiert wird, Analytikerberechtigung enthält, wird die Administratordefinition importiert, aber nicht die Analytikerberechtigung. Die Analytikerberechtigung ist für Server mit V6.1 oder höher nicht gültig.
- Das Importieren von Daten aus einer CENTERA-Einheitenklasse wird nicht unterstützt. Dateien, die importiert werden, können jedoch auf einer CENTERA-Speichereinheit gespeichert werden.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
.-*------.
>>-Import Admin--+-----+----->
| .-,------. |
| V              | |
'---Administratorname---+'

.-Preview----No-----.
>>+-----+---DEVclass----Einheitenklassenname--->
'-Preview----+No---+'
'-Yes-'

.-,------.
V              |
>>-VOLumentname---+---Datenträgername--+-----+----->
'-FILE:--Dateiname----'

.-Replacedefs----No-----.
>>+-----+----->
'-Replacedefs----+No---+'
'-Yes-'
```

## Parameter

---

### Administratorname

Gibt die Administratoren an, für die Informationen importiert werden sollen. Dieser Parameter ist wahlfrei. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

### Preview

Gibt an, ob die Ergebnisse der Importoperation vorangezeigt werden sollen, ohne die Administratorinformationen zu importieren. Dieser Parameter ist wahlfrei. Die folgenden Parameterwerte werden unterstützt:

No

Gibt an, dass die Informationen importiert werden sollen.

Yes

Gibt an, dass die Operation vorangezeigt, aber nicht ausgeführt wird. Informationen über die Anzahl und den Typ der importierten Objekte sowie die Anzahl der übertragenen Byte werden an der Serverkonsole und im Aktivitätenprotokoll aufgelistet.

Der Standardwert ist NO. Wird für den Wert YES angegeben, müssen Sie die Exportdatenträger laden.

DEVclass (Erforderlich)

Gibt die Einheitenklasse an, aus der die Importdaten gelesen werden sollen.

Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Imports aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, wie beispielsweise Wiederherstellungsoperationen, um ein Laufwerk verfügbar zu machen.

VOLUMENAME (Erforderlich)

Gibt die Datenträger an, die für die Importoperation verwendet werden sollen. Die Datenträger müssen in derselben Reihenfolge importiert werden, in der sie exportiert wurden. Die folgenden Parameterwerte werden unterstützt:










Datenträgername

Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

FILE: Dateiname

Gibt den Namen einer Datei an, die eine Liste der Datenträger enthält, die für die importierten Daten verwendet werden. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

Verwenden Sie die folgenden Namenskonventionen bei der Angabe von Datenträgern, die den folgenden Einheitentypen zugeordnet sind:

| Für Einheit  | Angeben  |
|--|--|
| Band   | 1 – 6 alphanumerische Zeichen.   |
| FILE   | Beliebige, vollständig qualifizierte Dateinamenzeichenfolge. Beispiel:<br> AIX-Betriebssysteme  Linux-Betriebssysteme/imdata/mt1.<br> Windows-Betriebssysteme<br>d:\Programmdateien\tivoli\tsm\data1.dsm. |
|  AIX-Betriebssysteme  Linux-Betriebssysteme<br> Windows-Betriebssysteme REMOVABLEFILE |  AIX-Betriebssysteme  Linux-Betriebssysteme<br> Windows-Betriebssysteme 1 – 6 alphanumerische Zeichen.  |
| SERVER   | 1 – 250 alphanumerische Zeichen.   |

Replacedefs

Gibt an, ob Administratordefinitionen auf dem Zielsever ersetzt werden sollen. Die folgenden Parameterwerte werden unterstützt:

No

Gibt an, dass Definitionen nicht ersetzt werden sollen.

Yes

Gibt an, dass Definitionen ersetzt werden sollen.

Der Standardwert ist NO.

## Beispiel: Administratorinformationen von bestimmten Banddatenträgern importieren

Vom Server aus die Informationen für alle definierten Administratoren von den Banddatenträgern TAPE01, TAPE02 und TAPE03 importieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist. Den folgenden Befehl ausgeben:

```
import admin devclass=menu1
volumenames=tape01,tape02,tape03
```

## Beispiel: Administratorinformationen von Banddatenträgern importieren, die in einer Datei aufgelistet sind

Vom Server die Informationen für alle definierten Administratoren von den Banddatenträgern importieren, die in der folgenden Datei aufgelistet sind:

- Linux-BetriebssystemeTAPEVOL
- TAPEVOL.DATA

Diese Datei enthält diese Zeilen:

```
TAPE01  
TAPE02  
TAPE03
```

Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist. Den folgenden Befehl ausgeben:

Linux-Betriebssysteme

```
import admin devclass=menu1 volumenames=file:tapevol
```

Windows-Betriebssysteme

```
import admin devclass=menu1 volumenames=file:tapevol.data
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für IMPORT ADMIN

| Befehl         | Beschreibung   |
|----------------|--|
| CANCEL PROCESS | Bricht einen Serverhintergrundprozess ab.  |
| EXPORT ADMIN   | Kopiert Verwaltungsdaten auf externe Datenträger oder direkt auf einen anderen Server. |
| IMPORT NODE    | Schreibt Clientknotendaten von externen Datenträgern zurück.                           |
| IMPORT POLICY  | Schreibt Maßnahmendaten von externen Datenträgern zurück.                              |
| IMPORT SERVER  | Schreibt den gesamten Server oder einen Teil davon von externen Datenträgern zurück.   |
| QUERY ACTLOG   | Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.                               |
| QUERY PROCESS  | Zeigt Informationen über Hintergrundprozesse an.                                       |

## IMPORT NODE (Clientknoteninformationen importieren)

Mit diesem Befehl können Clientknotendefinitionen von einem Server oder von sequenziellen Datenträgern in einen IBM Spectrum Protect-Zielservers importiert werden.


**Wichtig:** Bei Befehlen, mit denen Administratoren oder Knoten importiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls IMPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.

Wenn Sie eine Domäne auf dem Quellenserver angeben und diese Maßnahmendomäne auch auf dem Zielservers vorhanden ist, werden die importierten Knoten derselben Maßnahmendomäne auf dem Zielservers zugeordnet. Andernfalls werden importierte Knoten der Maßnahmendomäne STANDARD auf dem Zielservers zugeordnet.

IBM Spectrum Protect-Server mit aktiviertem Aufbewahrungsschutz erlauben keine Importoperationen.

Einschränkungen:

1. Sind die Versionen des Zielservers und Quellenservers nicht kompatibel, kann die Operation möglicherweise nicht ausgeführt werden.
2. Das Importieren von Daten aus einer CENTERA-Einheitenklasse wird nicht unterstützt. Dateien, die importiert werden, können jedoch auf einer CENTERA-Speichereinheit gespeichert werden.
3. Wenn Sie einen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden, müssen alle Zielservers für LDAP-Kennwörter konfiguriert werden. Auf Daten, die von einem Knoten importiert werden, der sich mit einem LDAP-Verzeichnisservers authentifiziert, kann nicht zugegriffen werden, wenn der Zielservers nicht korrekt konfiguriert ist. Ist Ihr Zielservers nicht konfiguriert, können importierte Daten von einem LDAP-Knoten dennoch auf dem Zielservers gespeichert werden. Der Zielservers muss jedoch für die Verwendung von LDAP konfiguriert werden, damit Sie auf die importierten Daten zugreifen können.

4. Sind die Versionen des Zielservers und Quellenservers nicht kompatibel, kann die Operation möglicherweise nicht ausgeführt werden.
5. Sie können eine Einheitenklasse CENTERA nicht als Zielmedium für einen Exportbefehl oder als Quellenmedium für einen Importbefehl verwenden.
6. Das inkrementelle Exportieren/Importieren der folgenden Typen von Clientdaten auf einen anderen IBM Spectrum Protect-Server wird nicht unterstützt:
  - o VMware-Sicherungen, bei denen Gesamt- und Teilsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen.
  - o Sicherungsgruppen, bei denen Gesamt- und Differenzsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen.
  - o  Windows-Betriebssysteme Windows-Systemstatusdaten, die periodisch, inkrementell auf einen anderen Server übertragen werden.

Der vollständige Export/Import dieser Daten in ein neues Dateisystem auf dem Ziel wird unterstützt, indem der gesamte Dateibereich, der die Daten enthält, exportiert wird. In anderen Worten, bei dem Export darf nicht die Option *FILEDATA=ALLACTIVE, FROMDATE, TODATE* oder *MERGEFILESPPACES* verwendet werden.

Das bewährte Verfahren für die inkrementelle Übertragung dieses Typs von Daten zwischen zwei Servern ist die Verwendung der Knotenreplikation.

Mit dem Befehl *QUERY ACTLOG* kann der Status der Importoperation angezeigt werden. Diese Informationen können auch über die Serverkonsole angezeigt werden.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl *CANCEL PROCESS* abgebrochen werden kann. Wenn ein Hintergrundprozess des Befehls *IMPORT NODE* abgebrochen wird, wurden möglicherweise einige der Daten bereits importiert. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl *QUERY PROCESS*.

Bei einem Server, der über Clients mit Unterstützung für Unicode verfügt, kann der Server den eingegebenen Dateibereichsnamen konvertieren oder Sie können die folgenden Parameter verwenden:

- *HEXFILESPPACE*
- *UNIFILESPPACE*

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen *UPDATE*. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```

>>-Import Node-----+----->
| .-,----- . |
| v | |
|'---Knotenname-+-'|

>+-----+----->
| .-,----- . |
| v | |
|'-FILESpace-----Dateibereichsname-+-'|

>+-----+----->
| .-,----- . |
| v | |
|'-HEXFILESPPace-----Dateibereichsname-+-'|

>+-----+----->
| .-,----- . |
| v | |
|'-UNIFILESPPace-----Dateibereichsname-+-'|

```



Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.

#### FILEData

Gibt den Typ der Dateien an, die für alle angegebenen Knoten importiert werden können und auf dem Exportdatenträger gefunden werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NONE.

Werden Daten von sequenziellen Datenträgern importiert, wird die von den Dateidaten verwendete Einheitenklasse durch die Einheitenklasse des Speicherpools bestimmt. Handelt es sich um dieselbe Einheitenklasse wie in diesem Befehl, werden zum Importieren der Knoteninformationen zwei Laufwerke benötigt. Der Grenzwert für Ladeanforderungen der Einheitenklasse muss mindestens 2 betragen.

In den folgenden Beschreibungen werden *aktive* und *inaktive* Sicherungsdateikopien erwähnt. Eine aktive Sicherungsdateikopie ist die aktuellste Sicherungskopie einer Datei, die auf der Clientdatenstation noch vorhanden ist. Alle anderen Sicherungsdateikopien werden als inaktive Kopien bezeichnet. Der Parameter unterstützt die folgenden Werte:

#### ALL

Der Server importiert alle Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden. Die eingeschlossenen Dateibereiche sind Unicode- und Nicht-Unicode-Dateibereiche.

#### None

Nur Knotendefinitionen werden importiert. Der Server importiert keine Dateien.

#### ARchive

Der Server importiert nur archivierte Dateien.

#### Backup

Der Server importiert nur Sicherungsversionen, unabhängig davon, ob sie aktiv oder inaktiv sind.

#### BACKUPActive

Der Server importiert nur aktive Sicherungsversionen. Diese aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl IMPORT ausgegeben wird.

#### ALLActive

Der Server importiert alle aktiven Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden. Die aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl IMPORT ausgegeben wird.

#### SPacemanaged

Der Server importiert nur Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

#### Preview

Gibt an, ob die Ergebnisse der Importoperation vorangezeigt werden sollen, ohne die Informationen zu importieren. Die Option PREVIEW=YES erfordert das Laden der Exportdatenträger. Die folgenden Werte werden unterstützt:

#### No

Gibt an, dass die Knoteninformationen importiert werden sollen.

#### Yes

Gibt an, dass die Ergebnisse der Importoperation vorangezeigt werden sollen, ohne die Dateien zu importieren. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet.

Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

#### DEVclass (Erforderlich)

Gibt die Einheitenklasse an, aus der die Importdaten gelesen werden sollen. Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Imports aktiv, bricht der Server Operationen mit geringerer Priorität ab, wie beispielsweise die Identifizierung doppelter Daten, um ein Laufwerk verfügbar zu machen.

#### Dates

Gibt an, ob die Daten für die Dateikopien auf dasselbe Datum gesetzt werden, an dem die Dateien exportiert wurden, oder ob die Daten an das Importdatum angepasst werden.

Dieser Parameter unterstützt die folgenden Werte:

#### Absolute

Die Daten für Dateikopien werden auf die Werte gesetzt, die beim Exportieren der Dateien angegeben wurden.

#### Relative

Die Daten für Dateikopien werden an das Importdatum angepasst.

Der Standardwert ist ABSOLUTE.



Wenn der Exportdatenträger einige Zeit nach dem Export inaktiv ist (z. B. über einen Zeitraum von sechs Monaten), sind die ursprünglichen Sicherungs- oder Archivierungsdaten eventuell alt genug, um die sofortige Verfallsverarbeitung für Dateikopien auszulösen, wenn die Daten auf einen Server importiert werden. Wenn für diesen Wert RELATIVE angegeben wird, wird die seit dem Export verstrichene Zeit angepasst, so dass für die Dateikopien nicht sofort eine Verfallsverarbeitung erfolgt.

Beispiel: Angenommen, ein Exportband enthält eine Archivierungsdateikopie, die fünf Tage vor der Exportoperation archiviert wurde. Wenn der Datenträger sechs Monate gesichert und dann importiert wird, wird standardmäßig davon ausgegangen, dass die Archivierungsdatei vor sechs Monaten und fünf Tagen eingefügt wurde (DATES=ABSOLUTE). Abhängig vom Aufbewahrungszeitraum, der in der Verwaltungsklasse der Datei angegeben ist, wird für die Datei möglicherweise sofort eine Verfallsverarbeitung durchgeführt. Durch die Angabe von DATES=RELATIVE wird das Archivierungsdatum der Datei während des Imports wieder auf "vor fünf Tagen" zurückgesetzt. Auf diese Weise passt der Parameter DATES=RELATIVE die seit dem Export verstrichene Zeit für Dateisicherungs- und -archivierungsdaten an.

#### VOLumenames (Erforderlich)

Gibt die Datenträger an, die für die Importoperation verwendet werden sollen. Die Datenträger müssen in derselben Reihenfolge importiert werden, in der sie exportiert wurden. Der Parameter unterstützt die folgenden Werte:










##### Datenträgername

Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

##### FILE:Dateiname

Gibt den Namen einer Datei an, die eine Liste der Datenträger enthält, die für die importierten Daten verwendet werden. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

Verwenden Sie die folgenden Namenskonventionen bei der Angabe von Datenträgern, die den folgenden Einheitentypen zugeordnet sind:

| Für Einheit  | Angeben  |
|--|--|
| Band   | 1 – 6 alphanumerische Zeichen.   |
| FILE   |   Beliebige, vollständig qualifizierte Dateinamenzeichenfolge. Ein Beispiel ist /imdata/mt1.<br><br> Beliebige, vollständig qualifizierte Dateinamenzeichenfolge. Beispiel:<br>d:\Programmdateien\tivoli\tsm\data1.dsm. |
|  <br> REMOVABLEFILE |  <br> 1 – 6 alphanumerische Zeichen.  |
| SERVER   | 1 – 250 alphanumerische Zeichen.   |

#### Replacedefs

Gibt an, ob Definitionen auf dem Zielsystem ersetzt werden sollen. Der Standardwert ist NO. Der Parameter unterstützt die folgenden Werte:

No

Objekte sollen nicht ersetzt werden.

Yes

Objekte sollen ersetzt werden.

#### HEXFILESpace

Gibt die hexadezimale Darstellung der Dateibereichsnamen im UTF-8-Format an. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Dieser Parameter ist wahlfrei.

Soll die hexadezimale Darstellung eines Dateibereichsnamens angezeigt werden, können Sie den Befehl QUERY FILESPACE mit FORMAT=DETAILED verwenden.

#### UNIFILESpace

Gibt an, dass die Dateibereiche, die dem Server bekannt sind, Unicode-fähig sind. Der Server konvertiert die Namen, die Sie eingeben, aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8, um die Dateibereiche zu lokalisieren, die importiert werden sollen. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es kann ein Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Dieser Parameter ist wahlfrei.

#### MERGEfilespaces

Gibt an, ob IBM Spectrum Protect Clientdateien in vorhandene Dateibereiche auf dem Zielsystem mischt (sofern sie vorhanden sind) oder ob IBM Spectrum Protect neue Dateibereichsnamen generiert. Der Standardwert ist NO.

Gültige Werte sind:

Yes

Gibt an, dass importierte Daten auf dem Zielsystem in den vorhandenen Dateibereich gemischt werden, wenn ein Dateibereich mit demselben Namen auf dem Zielsystem vorhanden ist.

No

Gibt an, dass IBM Spectrum Protect einen neuen Dateibereichsnamen für importierte Daten auf dem Zielsystem generiert, wenn Dateibereiche mit demselben Namen vorhanden sind.

PROXynodeassoc


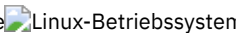
Gibt an, ob Proxyknoten-zuordnungen importiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.


## Beispiel: Clientknoteninformationen von Bändern importieren

Vom Server aus Clientknoteninformationen von den Banddatenträgern TAPE01, TAPE02 und TAPE03 importieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist.

```
import node devclass=menu1 volumenames=tape01,tape02,tape03
```

## Beispiel: Clientknoteninformationen von Bändern importieren, die in einer Datei aufgelistet sind

  Vom Server die Clientknoteninformationen von den Banddatenträgern importieren, die in der Datei TAPEVOL aufgelistet sind.

 Vom Server die Clientknoteninformationen von den Banddatenträgern importieren, die in der Datei TAPEVOL.DATA aufgelistet sind.

Diese Datei enthält diese Zeilen:

```
TAPE01  
TAPE02  
TAPE03
```

Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist.

```
import node devclass=menu1 volumenames=file:tapevol
```



```
import node devclass=menu1 volumenames=file:tapevol.data
```

## Beispiel: Die aktive Sicherung für einen Clientknoten importieren

Importieren Sie vom Server die aktiven Sicherungsversionen der Dateidaten für Clientknoten JOE vom Banddatenträger TAPE01. Der Dateibereich ist Unicode.

```
import node joe unificspace=\\joe\c$ filedata=backupactive devclass=menu1  
volumenames=tape01
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für IMPORT NODE

| Befehl            | Beschreibung  |
|-------------------|---|
| CANCEL PROCESS    | Bricht einen Serverhintergrundprozess ab.   |
| COPY ACTIVATEDATA | Kopiert aktive Sicherungsdaten.   |
| EXPORT NODE       | Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server. |
| IMPORT ADMIN      | Schreibt Verwaltungsdaten von externen Datenträgern zurück.                                     |
| IMPORT POLICY     | Schreibt Maßnahmen von externen Datenträgern zurück.  |
| IMPORT SERVER     | Schreibt den gesamten Server oder einen Teil davon von externen Datenträgern zurück.            |
| QUERY ACTLOG      | Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.  |
| QUERY PROCESS     | Zeigt Informationen über Hintergrundprozesse an.  |

## IMPORT POLICY (Maßnahmeninformationen importieren)

Mit diesem Befehl können Informationen zu Maßnahmendomänen von sequenziellen Exportdatenträgern in den IBM Spectrum Protect-Server importiert werden. IBM Spectrum Protect-Server mit aktiviertem Aufbewahrungsschutz erlauben keine Importoperationen.

IBM Spectrum Protect-Clientdaten können mit der Export- und Importverarbeitung zwischen Servern versetzt werden, wenn auf beiden Plattformen derselbe austauschbare Datenträgertyp unterstützt wird.

Einschränkung:

1. Sind die Versionen des Zielservers und des Quellenservers nicht kompatibel, kann die Importoperation möglicherweise nicht ausgeführt werden.
2. Das Importieren von Daten aus einer CENTERA-Einheitenklasse wird nicht unterstützt. Dateien, die importiert werden, können jedoch auf einer CENTERA-Speichereinheit gespeichert werden.

Mit dem Befehl QUERY ACTLOG kann der Status der Importoperation angezeigt werden. Diese Informationen können auch über die Serverkonsole angezeigt werden.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn ein Hintergrundprozess des Befehls IMPORT POLICY abgebrochen wird, wurden einige der Daten bereits importiert. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Import Policy-+-----+----->
| .-,-,-----|
| V           |
|'---Domänenname-+'

.-Preview-----No-----
>+-----+-----DEVclass-----Einheitenklassenname----->
|'-Preview-----+No--+-'
|'-Yes-'

.-,-,-----
V           |
>--VOLumenames-----+---Datenträgername-+----->
|'-FILE:--Dateiname----'

.-Replacedefs-----No-----
>+-----+-----<
|'-Replacedefs-----+No--+-'
|'-Yes-'
```

## Parameter

Domänennamen

Gibt die Maßnahmendomänen an, für die Informationen importiert werden sollen. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Der Standardwert (\*) lautet alle Domänen.

Preview

Gibt an, ob die Ergebnisse der Importoperation vorangezeigt werden sollen, ohne die Informationen zu importieren. Dieser Parameter unterstützt die folgenden Werte:

No

Gibt an, dass die Informationen importiert werden sollen.

Yes

Gibt an, dass die Operation vorangezeigt, aber nicht ausgeführt wird. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet.

Die Option PREVIEW=YES erfordert das Laden der Exportdatenträger. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.  
DEVclass (Erforderlich)

Gibt die Einheitenklasse an, aus der die Importdaten gelesen werden sollen. Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Imports aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, wie beispielsweise Wiederherstellungsoperationen, um ein Laufwerk verfügbar zu machen.

VOLumenames (Erforderlich)

Gibt die Datenträger an, die für die Importoperation verwendet werden sollen. Die Datenträger müssen in derselben Reihenfolge importiert werden, in der sie exportiert wurden. Dieser Parameter unterstützt die folgenden Werte:







Datenträgername

Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

FILE:Dateiname

Gibt den Namen einer Datei an, die eine Liste mit Datenträgern enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

Verwenden Sie die folgenden Namenskonventionen bei der Angabe von Datenträgern, die den folgenden Einheitentypen zugeordnet sind:

| Für Einheit  | Angeben   |
|--|---|
| Band   | 1 – 6 alphanumerische Zeichen.  |
| FILE   | Beliebige, vollständig qualifizierte Dateinamenzeichenfolge. Beispiel: <ul style="list-style-type: none"><li>• Linux-Betriebssysteme/imdata/mt1</li><li>• Windows-Betriebssysteme<br/>d:\Programme\tivoli\tsm\data1.dsm.</li></ul> |
|  Linux-Betriebssysteme<br> REMOVABLEFILE |  Linux-Betriebssysteme<br> 1 – 6 alphanumerische Zeichen.   |
| SERVER   | 1 – 250 alphanumerische Zeichen.  |

Replacedefs

Gibt an, ob Maßnahmendefinitionen auf dem Zielsystem ersetzt werden sollen. Dieser Parameter unterstützt die folgenden Werte:

Yes

Gibt an, dass die Objekte durch importierte Objekte ersetzt werden sollen.

No

Gibt an, dass die Objekte nicht durch importierte Objekte ersetzt werden sollen.

Der Standardwert ist NO.

## Beispiel: Maßnahmeninformationen von bestimmten Banddatenträgern importieren

Vom Server aus die Informationen für alle definierten Maßnahmen von den Banddatenträgern TAPE01, TAPE02 und TAPE03 importieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist.

```
import policy devclass=menu1  
volumenames=tape01,tape02,tape03
```

## Beispiel: Maßnahmeninformationen von Banddatenträgern importieren, die in einer Datei aufgelistet sind

Vom Server die Informationen für alle definierten Maßnahmen von den Banddatenträgern importieren, die in der Datei mit folgendem Namen aufgelistet sind:

- Linux-BetriebssystemeTAPEVOL
- TAPEVOL.DATA

Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist. Die Datei enthält die folgenden Zeilen:

```
TAPE01  
TAPE02  
TAPE03
```

```
import policy devclass=menu1 volumenames=file:tapevol
```



```
import policy devclass=menu1 volumenames=file:tapevol.data
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für IMPORT POLICY

| Befehl         | Beschreibung   |
|----------------|--|
| CANCEL PROCESS | Bricht einen Serverhintergrundprozess ab.  |
| EXPORT POLICY  | Kopiert Maßnahmeninformationen auf externe Datenträger oder direkt auf einen anderen Server. |
| IMPORT ADMIN   | Schreibt Verwaltungsdaten von externen Datenträgern zurück.                                  |
| IMPORT NODE    | Schreibt Clientknotendaten von externen Datenträgern zurück.                                 |
| IMPORT SERVER  | Schreibt den gesamten Server oder einen Teil davon von externen Datenträgern zurück.         |
| QUERY ACTLOG   | Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.                                     |
| QUERY PROCESS  | Zeigt Informationen über Hintergrundprozesse an.   |

## IMPORT SERVER (Serverinformationen importieren)

Mit diesem Befehl können die Serversteuerungsinformationen und die angegebenen Clientdateidaten vollständig oder teilweise von Exportdatenträgern auf den IBM Spectrum Protect-Server kopiert werden.

Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten importiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls IMPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.

IBM Spectrum Protect-Server mit aktiviertem Aufbewahrungsschutz erlauben keine Importoperationen.

Einschränkungen:

- Sind die Versionen des Zielservers und Quellenservers nicht kompatibel, kann die Operation möglicherweise nicht ausgeführt werden.
- Das Importieren von Daten aus einer CENTERA-Einheitenklasse wird nicht unterstützt. Dateien, die importiert werden, können jedoch auf einer CENTERA-Speichereinheit gespeichert werden.
- Wenn Sie einen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden, müssen alle Zielserver für LDAP-Kennwörter konfiguriert werden. Auf Serverdaten, die von einem Knoten exportiert werden, der sich mit einem LDAP-Verzeichnisserver authentifiziert, kann nicht zugegriffen werden, wenn der Zielserver nicht korrekt konfiguriert ist. Ist Ihr Zielserver nicht konfiguriert, können exportierte Daten von einem LDAP-Knoten dennoch auf dem Zielserver gespeichert werden. Der Zielserver muss jedoch für die Verwendung von LDAP konfiguriert werden, damit Sie auf die Daten zugreifen können.
- Das inkrementelle Exportieren oder Importieren der folgenden Typen von Clientdaten auf einen anderen IBM Spectrum Protect-Server wird nicht unterstützt:
  - VMware-Sicherungen, bei denen Gesamt- und Teilsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen
  - Sicherungsgruppen, bei denen Gesamt- und Differenzsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen
  - Windows-Systemstatusdaten, die periodisch, inkrementell auf einen anderen Server übertragen werden

Der vollständige Export oder Import dieser Daten in ein neues Dateisystem auf dem Ziel wird unterstützt, indem der gesamte Dateibereich, der die Daten enthält, exportiert wird. Bei dem Export darf nicht der Parameter FILEDATA=ALLACTIVE, FROMDATE, TODATE oder MERGEFILESPPACES verwendet werden.

Die Verwendung der Knotenreplikation zur inkrementellen Übertragung dieses Typs von Clientdaten zwischen zwei Servern ist optimal.

Sie können einen Import von Serverinformationen und Clientdateidaten auch direkt von dem Ursprungsserver einleiten. Weitere Informationen befinden sich unter den Befehlen EXPORT.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn ein Hintergrundprozess des Befehls IMPORT SERVER abgebrochen wird, wurden einige der Daten bereits importiert. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```

      .-FILEData----None----- .
>>-Import Server-----+----->
      '-FILEData----+All-----+'
                        +-None-----+
                        +-ARchive-----+
                        +-Backup-----+
                        +-BACKUPActive+
                        +-ALLActive----+
                        '-SPacemanaged-'

      .-Preview----No----- .
>>+-----+---DEVclass----Einheitenklassenname--->
      '-Preview----+No--+-'
                        '-Yes-'

      .-Dates----Absolute---- .
>>+-----+----->
      '-Dates----+Absolute+-'
                        '-Relative-'

      .-,----- .
      v |
>>-VOLumenames---+---Datenträgername--+----->
      '-FILE:--Dateiname----'

      .-Replacedefs----No----- .
>>+-----+----->
      '-Replacedefs----+No--+-'
                        '-Yes-'

      .-MERGEfilesppaces----No----- .
>>+-----+----->
      '-MERGEfilesppaces----+No--+-'
                        '-Yes-'

      .-PROXynodeassoc----No----- .
>>+-----+-----><
      '-PROXynodeassoc----+No--+-'
                        '-Yes-'
```

## Parameter

## FILEData

Gibt den Typ der Dateien an, die für alle Knoten importiert werden können, die für den Server definiert sind. Dieser Parameter ist wahlfrei. Der Standardwert ist NONE.

Die Einheitenklasse für den Zugriff auf die Dateidaten wird durch die Einheitenklasse des Speicherpools bestimmt. Handelt es sich um dieselbe Einheitenklasse wie in diesem Befehl, werden zum Importieren der Informationen zwei Laufwerke benötigt. Der Grenzwert für Ladeanforderungen der Einheitenklasse muss mindestens auf 2 gesetzt werden.

In den folgenden Beschreibungen werden aktive und inaktive Sicherungsdateikopien erwähnt. Eine aktive Sicherungsdateikopie ist die aktuellste Sicherungskopie einer Datei, die auf der Clientdatenstation noch vorhanden ist. Alle anderen Dateikopien werden als inaktive Kopien bezeichnet. Dieser Parameter unterstützt die folgenden Werte:

### ALL

IBM Spectrum Protect importiert alle Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

### None

IBM Spectrum Protect importiert keine Dateien, nur Knotendefinitionen.

### ARchive

IBM Spectrum Protect importiert nur archivierte Dateien.

### Backup

IBM Spectrum Protect importiert nur Sicherungsversionen, unabhängig davon, ob die Versionen aktiv oder inaktiv sind.

### BACKUPActive

IBM Spectrum Protect importiert nur aktive Sicherungsversionen. Diese aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl IMPORT ausgegeben wird.

### ALLActive

IBM Spectrum Protect importiert alle aktiven Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden. Die aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl IMPORT ausgegeben wird.

### SPAcemanaged

IBM Spectrum Protect importiert nur Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

## Preview

Gibt an, ob die Ergebnisse der Importoperation vorangezeigt werden sollen, ohne die Informationen zu importieren. Dieser Parameter unterstützt die folgenden Werte:

### No

Gibt an, dass die Serverinformationen importiert werden sollen.

### Yes

Gibt an, dass die Operation vorangezeigt, aber nicht ausgeführt wird. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll übertragen.

Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird die Option PREVIEW=YES angegeben, müssen Sie die Exportdatenträger laden.

## DEVclass (Erforderlich)

Gibt die Einheitenklasse an, aus der die Importdaten gelesen werden sollen. Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Imports aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, wie beispielsweise Wiederherstellungsoperationen, um ein Laufwerk verfügbar zu machen.

## Dates

Gibt an, ob die Daten für die Dateikopien auf dasselbe Datum gesetzt werden, an dem die Dateien exportiert wurden, oder ob die Daten an das Importdatum angepasst werden.

Wenn der Importdatenträger einige Zeit nach dem Export inaktiv ist (z. B. über einen Zeitraum von sechs Monaten), sind die ursprünglichen Sicherungs- oder Archivierungsdaten eventuell alt genug, um die sofortige Verfallsverarbeitung für Dateikopien auszulösen, wenn die Daten auf einen Server importiert werden. Wenn für diesen Wert RELATIVE angegeben wird, wird die seit dem Export verstrichene Zeit angepasst, so dass für die Dateikopien nicht sofort eine Verfallsverarbeitung erfolgt.

Beispiel: Angenommen, ein Importband enthält eine Archivierungsdateikopie, die fünf Tage vor der Exportoperation archiviert wurde. Wenn der Exportdatenträger sechs Monate gesichert und dann importiert wird, wird standardmäßig davon ausgegangen, dass die Archivierungsdatei vor sechs Monaten und fünf Tagen eingefügt wurde (DATES=ABSOLUTE). Abhängig vom Aufbewahrungszeitraum, der in der Verwaltungsklasse der Datei angegeben ist, wird für die Datei möglicherweise sofort eine Verfallsverarbeitung durchgeführt. Durch die Angabe von DATES=RELATIVE wird das Archivierungsdatum der Datei während des

Imports wieder auf "vor fünf Tagen" zurückgesetzt. Auf diese Weise passt der Parameter DATES=RELATIVE die seit dem Export verstrichene Zeit für Dateisicherungs- und -archivierungsdaten an.

Dieser Parameter unterstützt die folgenden Werte:

**Absolute**

Die Daten für Dateikopien werden auf die Werte gesetzt, die beim Exportieren der Dateien angegeben wurden.

**Relative**

Die Daten für Dateikopien werden an das Datum des Imports angepasst.

Der Standardwert ist ABSOLUTE.

**VOLUMENAMES (Erforderlich)**

Gibt die Datenträger an, die für die Importoperation verwendet werden sollen. Die Datenträger müssen in derselben Reihenfolge importiert werden, in der sie exportiert wurden. Dieser Parameter unterstützt die folgenden Werte:

**Datenträgername**

Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

**FILE: Dateiname**

Gibt den Namen einer Datei an, die eine Liste der Datenträger enthält, die für die importierten Daten verwendet werden. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

Verwenden Sie die folgenden Namenskonventionen bei der Angabe von Datenträgern, die den folgenden Einheitentypen zugeordnet sind:

| Für Einheit               | Angeben   |
|---------------------------|---|
| Band                      | 1 – 6 alphanumerische Zeichen.  |
| FILE                      | Beliebige, vollständig qualifizierte Datenträger- oder Dateinamenzeichenfolge. Ein Beispiel ist /imdata/mt1.<br>Beliebige, vollständig qualifizierte Datenträger- oder Dateinamenzeichenfolge. Beispiel: d:\Programmdateien\tivoli\tsm\data1.dsm. |
| <br><br><br>REMOVABLEFILE | 1 – 6 alphanumerische Zeichen.  |
| SERVER                    | 1 – 250 alphanumerische Zeichen.  |

**Replacedefs**

Gibt an, ob Objekte auf dem Server ersetzt werden sollen. Vorhandene Dateibereiche werden nicht ersetzt. Neue Dateibereiche werden erstellt, wenn identische Namen festgestellt werden. Dieser Parameter unterstützt die folgenden Werte:

**No**

Gibt an, dass die Objekte nicht durch importierte Objekte ersetzt werden sollen.

**Yes**

Gibt an, dass die Objekte durch importierte Objekte ersetzt werden sollen.

Der Standardwert ist NO.

**MERGEfilespace**

Gibt an, ob IBM Spectrum Protect Clientdateien in vorhandene Dateibereiche auf dem Zielsystem mischt (sofern sie vorhanden sind) oder ob IBM Spectrum Protect neue Dateibereichsnamen generiert. Nicht-Unicode- und Unicode-Dateibereiche können nicht gemischt werden. Dieser Parameter unterstützt die folgenden Werte:

**No**

Gibt an, dass IBM Spectrum Protect einen neuen Dateibereichsnamen für importierte Daten auf dem Zielsystem generiert, wenn Dateibereiche mit demselben Namen vorhanden sind.

**Yes**

Gibt an, dass importierte Daten auf dem Zielsystem in den vorhandenen Dateibereich gemischt werden, wenn ein Dateibereich mit demselben Namen auf dem Zielsystem vorhanden ist.

Der Standardwert ist NO.

**PROXynodeassoc**

Gibt an, ob Proxyknotenbeziehungen importiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

**Beispiel: Die Informationen für alle definierten Server von bestimmten Bändern importieren**



Vom Server aus die Informationen für alle definierten Server von den Banddatenträgern TAPE01, TAPE02 und TAPE03 importieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist.

```
import server devclass=menu1 volumenames=tape01,tape02,tape03
```

## Beispiel: Informationen für alle definierten Server von bestimmten Bändern importieren und angeben, dass Dateien in vorhandene Dateibereiche gemischt werden

Vom Server aus die Informationen für alle definierten Server von den Banddatenträgern TAPE01, TAPE02 und TAPE03 importieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist, und dass Clientdateien in Dateibereiche auf dem Zielserver gemischt werden sollen, wenn Dateibereiche mit denselben Namen vorhanden sind.

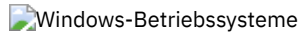
```
import server devclass=menu1 volumenames=tape01,tape02,tape03 mergefilespace=yes
```

## Beispiel: Informationen für alle definierten Server von Bändern importieren, die in einer Datei aufgelistet sind

Vom Server die Informationen für alle definierten Server von den Banddatenträgern importieren, die in der Datei TAPEVOL aufgelistet sind. Angeben, dass die Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist. Die Eingabedatei enthält diese Zeilen:

```
TAPE01  
TAPE02  
TAPE03
```

```
import server devclass=menu1 volumenames=file:tapevol
```



## Beispiel: Informationen für alle definierten Server von Bändern importieren, die in einer Datei aufgelistet sind

Vom Server die Informationen für alle definierten Server von den Banddatenträgern importieren, die in der Datei TAPEVOL.DATA aufgelistet sind. Angeben, dass die Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist. Die Eingabedatei enthält diese Zeilen:

```
TAPE01  
TAPE02  
TAPE03
```

```
import server devclass=menu1 volumenames=file:tapevol.data
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für IMPORT SERVER

| Befehl            | Beschreibung  |
|-------------------|---|
| CANCEL PROCESS    | Bricht einen Serverhintergrundprozess ab.   |
| COPY ACTIVATEDATA | Kopiert aktive Sicherungsdaten.   |
| EXPORT SERVER     | Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server. |
| IMPORT ADMIN      | Schreibt Verwaltungsdaten von externen Datenträgern zurück.   |
| IMPORT NODE       | Schreibt Clientknotendaten von externen Datenträgern zurück.  |
| IMPORT POLICY     | Schreibt Maßnahmen von externen Datenträgern zurück.  |
| QUERY ACTLOG      | Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.  |
| QUERY PROCESS     | Zeigt Informationen über Hintergrundprozesse an.  |

## INSERT MACHINE (Maschinenkenndaten oder Wiederh.-Anweisungen einfügen)

Mit diesem Befehl können vorhandenen Maschineninformationen in der Datenbank Client-Maschinenkenndaten oder Wiederherstellungsanweisungen hinzugefügt werden.

Sie können ein Programm schreiben, um Dateien mit den Informationen zu lesen und die entsprechenden INSERT MACHINE-Befehle zu generieren.

Mit den QUERY-Befehlen können die Informationen abgerufen werden, wenn ein schwerwiegender Fehler auftritt.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-INsert MACHine--Maschinename--Folgenummer----->  
>--+CHARacteristics----Text-----+-----><  
  '-RECOVERYInstructions----Text-'
```

## Parameter

---

Maschinenname (Erforderlich)

Gibt den Namen der Client-Maschine an.

Folgenummer (Erforderlich)

Gibt die Folgenummer für die Textzeile in der Datenbank an.

CHARacteristics

Gibt die Maschinenkenndaten an. Der Benutzer muß die Kenndaten oder die Wiederherstellungsanweisungen angeben, jedoch nicht beides. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält. Der Text kann bis zu 1024 Zeichen umfassen.

RECOVERYInstructions

Gibt die Wiederherstellungsanweisungen an. Der Benutzer muß die Kenndaten oder die Wiederherstellungsanweisungen angeben, jedoch nicht beides. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält. Der Text kann bis zu 1024 Zeichen umfassen.

## Beispiel: Die Informationen einer Maschine aktualisieren

---

Für die Maschine DISTRICT5 den folgenden Kenndatentext in Zeile 1 einfügen: "Machine owner is Mary Smith".

```
insert machine district5 1  
characteristics="Machine owner is Mary Smith"
```


## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für INSERT MACHINE

| Befehl         | Beschreibung                           |
|----------------|--|
| DEFINE MACHINE | Definiert eine Maschine für DRM.       |
| DELETE MACHINE | Löscht eine Maschine.                  |
| QUERY MACHINE  | Zeigt Informationen über Maschinen an. |

### Zugehörige Informationen:

 Informationen zur Servermaschine und zu Clientknotenmaschinen angeben

## ISSUE MESSAGE (Nachricht aus einem Server-Script ausgeben)

---

Diesen Befehl mit Rückkehrcodeverarbeitung in einem Script verwenden, um eine Nachricht aus einem Server-Script auszugeben, mit der die Fehlerquelle bei einem Befehl in dem Script bestimmt wird.

## Berechtigungsklasse

---

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

---

>>-ISSUE MESSAGE--Nachrichtenbewertung--Nachrichtentext----->>

## Parameter

### Nachrichtenbewertung (Erforderlich)

Gibt die Bewertung der Nachricht an. Die Anzeiger für die Nachrichtenbewertung sind:

- I Information. ANR1496I wird im Nachrichtentext angezeigt.
- W Warnung. ANR1497W wird im Nachrichtentext angezeigt.
- E Fehler. ANR1498E wird im Nachrichtentext angezeigt.
- S Schwer wiegender Fehler. ANR1499S wird im Nachrichtentext angezeigt.

### Nachrichtentext (Erforderlich)

Gibt die Beschreibung der Nachricht an.

## Beispiel: Eine Nachricht aus einem Server-Script ausgeben

Angenommen, Sie haben ein Script mit dem Namen backupscript, mit dem die Datenbank eines Clients stillgelegt wird, eine Sicherung dieser Datenbank vorgenommen wird und dann die Datenbank des Clients erneut gestartet wird. Zur Veranschaulichung resultiert das Script in einem Rückkehrcode ungleich Null. Den Befehl ISSUE MESSAGE mit der Nachrichtenbewertung und dem Nachrichtentext verwenden. Das folgende Beispiel ist ein Server-Script, das backupscript auf der Clientmaschine aufruft und Nachrichten auf der Basis des Rückkehrcodes von backupscript ausgibt.

```
issue message i "Starting backup"
define clientaction nodename action=command objects="c:\backupscript" wait=yes
if (101) goto qfail
if (102) goto qwarn
if (103) goto backupf
if (104) goto restartf
issue message i "Backup of database complete"
exit
qfail: issue message e "Quiesce of database failed"
exit
qwarn: issue message w "Quiesce of database failed, taking fuzzy backup"

exit
backupf: issue message e "Backup of database failed"
exit
restartf: issue message s "Database restart failed"
exit
```

### Befehl

```
issue message e "quiesce of database failed"
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für ISSUE MESSAGE

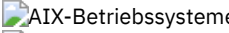
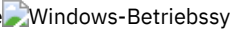
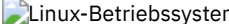
| Befehl        | Beschreibung  |
|---------------|---|
| COPY SCRIPT   | Erstellt eine Kopie einer Prozedur.                           |
| DEFINE SCRIPT | Definiert eine Prozedur für den IBM Spectrum Protect-Server.  |
| DELETE SCRIPT | Löscht eine Prozedur oder einzelne Zeilen aus einer Prozedur. |
| RENAME SCRIPT | Vergibt einen neuen Namen für eine Prozedur.                  |
| RUN           | Führt ein Script aus.   |
| UPDATE SCRIPT | Ändert Zeilen oder fügt Zeilen in einer Prozedur hinzu.       |

## LABEL LIBVOLUME (Datenträger im Kassettenarchiv Kennsatz zuordnen)

Mit diesem Befehl kann Banddatenträgern ein Kennsatz zugeordnet werden; in einem automatisierten Kassettenarchiv wird den Datenträgern automatisch beim Zurückstellen ein Kennsatz zugeordnet. Mit diesem Befehl verwendet der Server den Kennsatz mit vollständiger Länge, mit dem die Datenträger häufig vorgekennzeichnet sind.

Einschränkung: Verwenden Sie diesen Befehl nur für Kassettenarchive des Typs MANUAL, SCSI, ACSLS und 349X. Die Verarbeitung des Befehls wartet nicht darauf, dass ein Laufwerk verfügbar wird, auch wenn sich das Laufwerk nur im Status IDLE befindet. Falls erforderlich, kann ein Kassettenarchivlaufwerk verfügbar gemacht werden, indem der Befehl DISMOUNT VOLUME ausgegeben wird, um den Datenträger in diesem speziellen Laufwerk zu entladen. Wird das Kassettenarchivlaufwerk verfügbar, können Sie den Befehl LABEL LIBVOLUME erneut ausgeben.

Ausführliche und aktuelle Informationen zur Laufwerk- und Speicherarchivunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

-   Supported devices for AIX and Windows
-  Supported devices for Linux

Um den Befehl LABEL LIBVOLUME zu verwenden, muss mindestens ein Laufwerk vorhanden sein, das nicht von einem anderen IBM Spectrum Protect-Prozess verwendet wird. Dies schließt inaktive Datenträger ein, die bereitgestellt werden. Falls erforderlich, verwenden Sie den Befehl DISMOUNT VOLUME zur Aufhebung der Bereitstellung des inaktiven Datenträgers, um dieses Laufwerk verfügbar zu machen.

Standardmäßig überschreibt der Befehl LABEL LIBVOLUME keinen vorhandenen Kennsatz. Soll ein vorhandener Kennsatz jedoch überschrieben werden, können Sie die Option `OVERWRITE=YES` angeben.

Achtung:

- Beim Überschreiben eines Datenträgerkennsatzes werden alle Daten auf dem Datenträger gelöscht. Gehen Sie beim Überschreiben von Datenträgerkennsätzen mit Vorsicht vor, um das Löschen gültiger Daten zu vermeiden.
- Die Kennsätze auf VolSafe-Datenträgern können nur einmal überschrieben werden. Verwenden Sie daher den Befehl LABEL LIBVOLUME nur einmal für VolSafe-Datenträger. Sie können das Überschreiben des Kennsatzes vermeiden, indem Sie die Option `OVERWRITE=NO` mit dem Befehl LABEL LIBVOLUME verwenden.

Wenn Sie den Befehl LABEL LIBVOLUME verwenden, können Sie die Datenträger, die gekennzeichnet werden sollen, auf folgende Art und Weise angeben:


- Benennen Sie explizit einen Datenträger.
- Geben Sie mit dem Parameter `VOLRANGE` einen Bereich von Datenträgern ein.
- Verwenden Sie den Parameter `VOLLIST`, um eine Datei anzugeben, die eine Liste der Datenträgernamen enthält, oder um einen oder mehrere Datenträger explizit zu benennen.

Bei automatisierten Speicherarchiven werden Sie aufgefordert, den Datenträger in den Eingangs-/Ausgangsschacht des Speicherarchivs einzulegen.

Wenn die virtuelle Ein-/Ausgabe (VIO) aktiviert ist, sind Datenträger, die sich in der E/A-Station befinden, nicht mehr in den Eingangs-/Ausgangsanschlüssen. Um sicherzustellen, dass die Datenträger verarbeitet werden können, versetzen Sie die Datenträger aus der E/A-Station in die VIO-Schächte. Ist keine Serviceein-/ausgabestation verfügbar, legen Sie den Datenträger in einen leeren Schacht ein.

Bei manuellen Speicherarchiven werden Sie aufgefordert, den Datenträger direkt in ein Laufwerk zu laden.

Tipp: Um Banddatenträger automatisch zu kennzeichnen, können Sie den Parameter `AUTOLABEL` in den Befehlen `DEFINE LIBRARY` und `UPDATE LIBRARY` verwenden. Wird der Parameter `AUTOLABEL` verwendet, ist es nicht erforderlich, eine Gruppe von Bändern vorab zu kennzeichnen. Diese Methode ist effizienter als die Verwendung des Befehls LABEL LIBVOLUME, der es erfordert, dass Datenträger separat bereitgestellt werden. Wenn Sie den Parameter `AUTOLABEL` mit einem SCSI-Speicherarchiv verwenden, müssen Sie Bänder zurückstellen, indem Sie `CHECKLABEL=BARCODE` im Befehl `CHECKIN LIBVOLUME` angeben. Der Parameter `AUTOLABEL` nimmt für alle Nicht-SCSI-Speicherarchive standardmäßig den Wert `YES` und für SCSI-Speicherarchive den Wert `NO` an.



Um Datenträger mit dem Befehl LABEL LIBVOLUME zu kennzeichnen, geben Sie den Parameter `CHECKIN` an.

Um Banddatenträger in SCSI-Speicherarchiven automatisch zu kennzeichnen, verwenden Sie den Parameter `AUTOLABEL` in den Befehlen `DEFINE LIBRARY` und `UPDATE LIBRARY`. Wird dieser Parameter verwendet, ist es nicht erforderlich, eine Gruppe von Bändern vorab zu kennzeichnen. Diese Methode ist außerdem effizienter als die Verwendung des Befehls LABEL LIBVOLUME, der es erfordert, dass Datenträger separat bereitgestellt werden. Wenn Sie den Parameter `AUTOLABEL` verwenden, müssen Sie Bänder zurückstellen, indem Sie `CHECKLABEL=BARCODE` im Befehl `CHECKIN LIBVOLUME` angeben.

Ein Kennsatz darf keine eingebetteten Leerzeichen oder Punkte enthalten und muss gültig sein, wenn er als Dateiname auf den Datenträgern verwendet wird.

Sie müssen CD-ROM-, Zip- oder Jaz-Datenträger mit den Dienstprogrammen des Einheitenherstellers oder den Windows-Dienstprogrammen kennzeichnen. IBM Spectrum Protect stellt keine Dienstprogramme zum Formatieren oder Kennzeichnen dieser Datenträgertypen bereit. Die Dienstprogramme des Betriebssystems schließen das Plattenverwaltungsprogramm (Disk Administrator) (eine grafische Benutzerschnittstelle) und den Befehl zum Zuordnen von Kennsätzen ein.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax für manuelles Speicherarchiv

```
>>-LABEL LIBVolume--Speicherarchivname----->
. -OVERWRITE----No-----
>-----Datenträgername-----+----->
      '-OVERWRITE----+No--+'
                          '-Yes-'

.-WAITTime----60---
>-----+-----><
      '-WAITTime----Wert-'
```

## Syntax für SCSI-Kassettenarchiv

```
>>-LABEL LIBVolume--Speicherarchivname----->
>----+--Datenträgername-----+----->
      '-SEARCH----+Yes--| A |---+--LABELSource----+Barcode-----+'
                          '-Bulk--| A |-'                          '+Prompt-----+'
                                                                '-Vollist--| B |-'

. -OVERWRITE----No-----
>-----+-----+-----+----->
      '-CHECKIN----+SCRatch-+-'   '-OVERWRITE----+No--+'
                          '-PRiVate-'                          '-Yes-'

.-WAITTime----60---
>-----+-----><
      '-WAITTime----Wert-'
```

A (SEARCH=Yes, SEARCH=Bulk)

```
|---+--VOLRange----+--Datenträgername1,Datenträgername2---+-----|
|          .,-----|
|          V          |
'-VOLList----+--Datenträgername-+-+-----'
      '-FILE:--Dateiname----'
```

B (LABELSource=Vollist)

```
.,-----
V          |
|---VOLList----+--Datenträgername-+-+-----|
      '-FILE:--Dateiname----'
```

## Syntax für 349X-Kassettenarchiv

```
>>-LABEL LIBVolume--Speicherarchivname----->
>----+--Datenträgername-----+----->
      '-SEARCH----Yes----| A |---'

. -OVERWRITE----No-----
>-----+-----+-----+----->
      '-CHECKIN----+SCRatch-+-'   '-OVERWRITE----+No--+'
                          '-PRiVate-'                          '-Yes-'

.-WAITTime----60---
>-----+-----><
```

```

'-WAITTime-----Wert-'
A (SEARCH=Yes)
|---+-VOLRange-----Datenträgername1,Datenträgername2---+-----|
|          .,-----|.          |
|          V          |          |
'-VOLList-----+-Datenträgername-+-+-----|
          '-FILE:--Dateiname-----'

```

## Syntax für ACSLS-Kassettenarchiv

```

>>-LABEL LIBVolume--Speicherarchivname----->
>-----+-Datenträgername-----+----->
          '-SEARCH-----Yes-----| A |---'
.-----+-OVERWRITE-----No-----+----->
'-CHECKIN-----+-SCRatch-+-' '-OVERWRITE-----+-No-+-+'
          '-PRivate-'          '-Yes-'
.-----+-WAITTime-----60---+----->
>-----+-WAITTime-----Wert-+----->
A (SEARCH=Yes)
|---+-VOLRange-----Datenträgername1,Datenträgername2---+-----|
|          .,-----|.          |
|          V          |          |
'-VOLList-----+-Datenträgername-+-+-----|
          '-FILE:--Dateiname-----'

```

## Parameter

### Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das den Speicherdatenträger enthält.

### Datenträgername

Gibt den Namen des Datenträgers an, der gekennzeichnet werden soll.

- Für SCSI-Speicherarchive: Der Server gibt die Anforderung aus, den Datenträger in einen Schacht in dem Speicherarchiv oder, falls verfügbar, in einen Eingangs-/Ausgangsanschluss einzulegen. Der Server identifiziert einen Schacht anhand der Elementadresse des Schachts. Wird ein Datenträger in einem SCSI-Speicherarchiv mit mehreren Eingangs-/Ausgangsanschlüssen gekennzeichnet, wird der Datenträger in dem Schacht mit der niedrigsten Nummer gekennzeichnet.  
Warnung: Wenn Sie einen Datenträgernamen angeben, überschreibt der angegebene Name den Kennsatz, der auf der Kasette gedruckt ist.
- Für Speicherarchive des Typs MANUAL: Der Server gibt die Anforderung aus, den Datenträger in ein Laufwerk einzulegen.
- Für 349X-Kassettenarchive: Der Datenträger befindet sich möglicherweise bereits in dem Kassettenarchiv, oder Sie werden möglicherweise aufgefordert, den Datenträger in die E/A-Station zu stellen.

Hinweis: Ist der angegebene Datenträgername bereits in einem Speicherpool oder in einer Datenträgerhistorydatei definiert, erhält der Datenträger keinen Kennsatz und eine Nachricht wird angezeigt.

### CHECKIN

Gibt an, ob der Server den Datenträger zurückstellt. Dieser Parameter ist wahlfrei. Gültige Werte:

#### SCRatch

Gibt an, dass der Server die Datenträger zurückstellt und die Datenträger dem Arbeitsdatenträgerpool des Kassettenarchivs hinzufügt. Hat ein Datenträger einen Eintrag in der Datenträger-History, können Sie den Datenträger nicht als Arbeitsdatenträger zurückstellen.

#### PRivate

Gibt an, dass der Server die Datenträger zurückstellt und die Datenträger als privat kennzeichnet. Private Datenträger sind nur verfügbar, wenn sie nach Namen angefordert werden.

Wird kein Wert für diesen Parameter angegeben, wird mit dem Befehl der Datenträger gekennzeichnet, aber nicht zurückgestellt. Geben Sie für diesen Parameter keinen Wert ein und soll der Datenträger zurückgestellt werden, müssen Sie den Befehl CHECKIN LIBVOLUME ausgeben.

## SEARCH

Gibt an, dass der Server das Kassettenarchiv nach verwendbaren Datenträgern durchsucht, denen ein Kennsatz zugeordnet werden soll. Dieser Parameter gilt für SCSI-, 349X- und ACSLS-Kassettenarchive.

Die folgenden Werte sind gültig:

### Yes

Gibt an, dass der Server nur den Datenträgern einen Kennsatz zuordnet, die in dem Kassettenarchiv aufbewahrt werden, es sei denn, dem Datenträger wurde bereits ein Kennsatz zugeordnet oder der Barcode des Datenträgers kann nicht gelesen werden.

Wird die Option LABELSOURCE=PROMPT angegeben, wird der Datenträger aus seiner Position in dem Kassettenarchiv oder den Eingangs- und Ausgangsanschlüssen in das Laufwerk versetzt. Der Server fordert den Benutzer auf, den Befehl REPLY auszugeben, der die Kennsatzzeichenfolge enthält, und dieser Kennsatz wird auf das Band geschrieben.

### Bulk

Gibt an, dass der Server die Eingangs-/Ausgangsanschlüsse des Kassettenarchivs nach verwendbaren Datenträgern durchsucht, denen ein Kennsatz zugeordnet werden soll. Diese Option ist nur für SCSI-Kassettenarchive gültig.

Wird LABELSOURCE=BARCODE angegeben, wird der Barcode des Datenträgers gelesen. Anschließend wird das Band aus seiner Position in dem Kassettenarchiv oder in den Eingangs-/Ausgangsanschlüssen in ein Laufwerk versetzt, in dem das Barcodeetikett geschrieben wird. Nachdem das Band mit einem Kennsatz versehen wurde, wird es zurück in seine Position in dem Kassettenarchiv, in die Eingangs-/Ausgangsanschlüsse oder in einen Speicherschacht versetzt, wenn die Option CHECKIN angegeben wurde. Für die korrekte Funktionsweise der Barcodeunterstützung für Kassettenarchive, die von IBM Spectrum Protect unterstützt werden, müssen der IBM Spectrum Protect-Server und der Einheitentreiber dieselbe Stufe aufweisen. Die Barcodeunterstützung ist für Kassettenarchive verfügbar, die von IBM Spectrum Protect unterstützt werden und die den IBM Spectrum Protect-Einheitentreiber oder den IBM® Magstar- oder LTO Ultrium-Einheitentreiber verwenden.

Tipp: Sie können den Parameter VOLRANGE oder VOLLIST verwenden, um die Suche zu begrenzen.

## VOLRange

Gibt einen Bereich von Datenträgernamen an, die durch ein Komma voneinander getrennt sind. Verwenden Sie diesen Parameter, um die Suche nach Datenträgern zu begrenzen, die gekennzeichnet werden sollen, wenn SEARCH=YES (Kassettenarchive 349X, ACSLS und SCSI) oder SEARCH=BULK (nur SCSI-Kassettenarchive) angegeben wird. Sind keine Datenträger in dem Kassettenarchiv vorhanden, die sich in dem angegebenen Bereich befinden, wird der Befehl ohne Fehler beendet.

Es können nur Datenträgernamen angegeben werden, die numerisch erhöht werden können. Neben dem Bereich für den Erhöhungswert kann ein Datenträgername ein alphanumerisches Präfix und ein alphanumerisches Suffix enthalten.

| Parameter              | Beschreibung   |
|------------------------|--|
| volrange=bar110,bar130 | Die folgenden 21 Datenträger werden mit einem Kennsatz versehen: bar110, bar111, bar112,...bar129, bar130. |
| volrange=bar11a,bar13a | Die 3 Datenträger werden wie folgt gekennzeichnet: bar11a, bar12a, bar13a.                                 |
| volrange=123400,123410 | Die 11 Datenträger werden gekennzeichnet: 123400, 123401, ...123409, 123410.                               |

## VOLList

Gibt eine Liste mit Datenträgern an. Verwenden Sie diesen Parameter, um die Suche nach Datenträgern zu begrenzen, die gekennzeichnet werden sollen, wenn SEARCH=YES (Kassettenarchive 349X, ACSLS und SCSI) oder SEARCH=BULK (nur SCSI-Kassettenarchive) angegeben wird. Sind keine Datenträger in dem Kassettenarchiv vorhanden, die sich in der Liste befinden, wird der Befehl ohne Fehler beendet. Der Parameter VOLLIST kann auch die Quelle der Namen sein, die zum Kennzeichnen von Datenträgern verwendet werden sollen, wenn der Parameter LABELSOURCE auf VOLLIST gesetzt ist. Bei LABELSOURCE=VOLLIST müssen Sie den Parameter VOLLIST angeben.

Die folgenden Werte sind gültig:

### Datenträgername

Gibt die Namen der Datenträger an, die für den Befehl verwendet werden. Zum Beispiel: VOLLIST=TAPE01, TAPE02.

### FILE: Dateiname

Gibt den Namen einer Datei an, die eine Liste der Datenträger für den Befehl enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert. Um beispielsweise die Datenträger TAPE01, TAPE02 und TAPE03 zu verwenden, erstellen Sie eine Datei mit dem Namen TAPEVOL, die die folgenden Zeilen enthält:

```
TAPE01
TAPE02
TAPE03
```

Die Datenträger können für den Befehl wie folgt angegeben werden: `VOLLIST=FILE:TAPEVOL`.

Hinweis: Bei dem Dateinamen muss die Groß-/Kleinschreibung beachtet werden.

#### LABELSource

Gibt an, wie oder ob der Server Kennsätze sequenzieller Datenträger liest. Diese Option ist nur für SCSI-Kassettenarchive gültig. Geben Sie diesen Parameter nur bei `SEARCH=YES` oder `SEARCH=BULK` an.

Sie können die folgenden Werte angeben:

##### Prompt

Der Server fordert bei Bedarf zur Eingabe von Datenträgernamen auf.

##### Barcode

Der Server versucht, das Barcode-Etikett zu lesen. Schlägt der Versuch fehl, wird der Datenträger von dem Server nicht mit einem Kennsatz versehen, und es wird eine Nachricht angezeigt.

Wichtig: Für die korrekte Funktionsweise der Barcode-Unterstützung müssen die entsprechenden Einheitentreiber für die Kassettenarchive installiert sein.

##### Vollist

Diese Option gilt nur für SCSI-Kassettenarchive. Der Server versucht, die angegebene Datei oder Dateiliste zu lesen. Schlägt der Versuch fehl, werden die Datenträger von dem Server nicht mit einem Kennsatz versehen, und es wird eine Nachricht angezeigt.

#### OVERWRITE

Gibt an, ob der Server versucht, vorhandene Kennsätze zu überschreiben. Dieser Parameter ist wahlfrei. Der Standardwert ist `NO`. Sie können die folgenden Werte angeben:

##### No

Gibt an, dass der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht. Für StorageTek-VolSafe-Datenträger muss der Wert `NO` lauten.

##### Yes

Gibt an, dass der Server vorhandene Kennsätze nur dann überschreibt, wenn sowohl der vorhandene Kennsatz als auch der angeforderte Kennsatz oder das Barcodeetikett noch nicht in dem Serverspeicherpool oder in der Datenträgerhistoryliste definiert sind.

#### WAITTime

Gibt die Anzahl Minuten an, die der Server auf Ihre Antwort auf eine Anforderung wartet. Geben Sie einen Wert im Bereich 0-9999 an. Möchten Sie vom Server zur Eingabe aufgefordert werden, geben Sie eine Wartezeit größer als Null an. Der Standardwert ist 60 Minuten. Beispiel: Angenommen, Sie werden vom Server aufgefordert, ein Band in den Eingangs-/Ausgangsanschluss eines Kassettenarchivs einzulegen. Haben Sie eine Wartezeit von 60 Minuten angegeben, gibt der Server eine Anforderung aus und wartet 60 Minuten auf Ihre Antwort. Angenommen, Sie haben dagegen eine Wartezeit von 0 angegeben. Wenn Sie ein Band eingelegt haben, hat eine Wartezeit mit dem Wert Null zur Folge, dass die Operation ohne Aufforderung fortgesetzt wird. Haben Sie kein Band eingelegt, hat eine Wartezeit mit dem Wert Null zur Folge, dass die Operation fehlschlägt.

## Beispiel: Datenträger im Kassettenarchiv automatisch mit einem Kennsatz versehen

Bänder in dem SCSI-Kassettenarchiv `AUTO` automatisch mit einem Kennsatz versehen, wenn die Datenträger zurückgestellt werden.

```
label libvolume auto checkin=scratch search=yes labelsource=barcode  
overwrite=yes
```

## Beispiel: Sequenzielle Datenträger im Kassettenarchiv mit einem Kennsatz versehen

Die 3 Datenträger `bar11a` bis `bar13a` in dem SCSI-Kassettenarchiv `ABC` mit einem Kennsatz versehen. Wird der folgende Befehl ausgegeben, werden die drei Datenträger wie folgt gekennzeichnet: `bar11a, bar12a, bar13a`.

```
label libvolume abc checkin=scratch search=yes volrange=bar11a,bar13a  
labelsource=barcode
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für LABEL LIBVOLUME

| Befehl         | Beschreibung  |
|----------------|---|
| AUDIT LIBRARY  | Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet. |
| CANCEL PROCESS | Bricht einen Serverhintergrundprozess ab.   |



| Befehl             | Beschreibung   |
|--------------------|--|
| CHECKIN LIBVOLUME  | Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.                                       |
| CHECKOUT LIBVOLUME | Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.                                     |
| DEFINE LIBRARY     | Definiert ein automatisiertes oder manuelles Kassettenarchiv.  |
| DEFINE VOLUME      | Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll. |
| QUERY LIBRARY      | Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.  |
| QUERY LIBVOLUME    | Zeigt Informationen zu einem Datenträger im Kassettenarchiv an.  |
| QUERY PROCESS      | Zeigt Informationen über Hintergrundprozesse an.   |
| REPLY              | Erlaubt einer Anforderung, die Verarbeitung fortzusetzen.  |
| UPDATE LIBVOLUME   | Ändert den Status eines Speicherdatenträgers.  |

## LOAD DEFALERTRIGGERS (Standardgruppe von Alertauslösern laden)

Verwenden Sie diesen Befehl, um die Standardgruppe von Alertauslösern auf den IBM Spectrum Protect-Server zu laden.

Für einen neu installierten Server ist eine Standardgruppe von Nachrichten zum Auslösen von Alerts definiert. Sie können die Standardalertauslöser ändern oder löschen. Verwenden Sie diesen Befehl, um die folgenden Tasks auszuführen:

- Die Standardgruppe von Alertauslösern laden und alle Standardalertauslöser, die gelöscht wurden, zurückschreiben.
- Alle Alertauslöser durch die ursprüngliche Standardgruppe ersetzen.

Standardmäßig werden mit diesem Befehl keine anderen erstellten Alertauslöser gelöscht; außerdem werden keine geänderten Standardalertauslöser ersetzt. Um alle Alertauslöser zu löschen und die ursprüngliche Gruppe von Standardalertauslösern zurückzuschreiben, geben Sie RESET=yes an.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```

>>-L0ad DEFALertriggers--+-REset-----No-----+-----<<
                          '-REset-----+No--+-'
                          '-Yes-'

```

### Parameter

#### REset

Gibt an, ob alle Alertauslöser durch die Standardgruppe von Alertauslösern ersetzt werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

#### No

Gibt an, dass nur die Standardalertauslöser hinzugefügt werden. Die ursprünglichen Standardalertauslöser werden dem Server hinzugefügt. Vorhandene Auslöser werden nicht gelöscht. Wenn ein Standardauslöser auf dem Server vorhanden ist, wird er nicht ersetzt oder geändert.

#### Yes

Gibt an, dass die Alertauslöser mit den ursprünglichen Standardwerten zurückgeschrieben werden. Alle Alertauslöser werden gelöscht; anschließend wird die ursprüngliche Gruppe von Standardalertauslösern hinzugefügt.

### Beispiel: Standardalertauslöser auf den Server laden

Die Standardauslöser laden, um alle gelöschten Standardauslöser zurückzuschreiben. Den folgenden Befehl ausgeben:

```
load defalertriggers
```



## Beispiel: Einen Administrator sperren

---

Den Administrator CLAUDIA sperren. Den folgenden Befehl ausgeben:

```
lock admin claudia
```

## Beispiel: Alle Administratoren sperren, die sich mit der IBM Spectrum Protect-Serverdatenbank authentifizieren

---

Das Platzhalterzeichen (\*) verwenden, um alle Administratoren zu sperren, die ihre Kennwörter lokal authentifizieren. Konsolenadministratoren sind von diesem Befehl nicht betroffen. Den folgenden Befehl ausgeben:

```
lock admin * authentication=local
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für LOCK ADMIN

| Befehl       | Beschreibung   |
|--------------|--|
| QUERY ADMIN  | Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an. |
| UNLOCK ADMIN | Ermöglicht einem gesperrten Administrator den Zugriff auf IBM Spectrum Protect.        |

## LOCK NODE (Clientknoten sperren)

---

Mit diesem Befehl kann der Zugriff eines Clientknotens auf den Server verhindert werden. Ein gesperrter Clientknoten kann keine IBM Spectrum Protect-Operationen ausführen, auch wenn die Operationen geplant sind.

Nach der Konfiguration eines LDAP-Verzeichnisseservers für die Kennwortauthentifizierung können Sie Knoten sperren, um zu erzwingen, dass sie Kennwörter verwenden, die sich mit einem LDAP-Server authentifizieren.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der der Clientknoten gehört.

## Syntax

---

```
>>-LOCK Node---*-----+-----+-----+-----+<
          '-Knotenname-'  '-AUTHentication-----+Local--'
                               '-LDap--'
```

## Parameter

---

### Knotenname

Gibt den Namen des Clientknotens an, der gesperrt werden soll. Sie können ein Platzhalterzeichen anstelle eines Knotennamens verwenden, wenn alle Knoten gemäß ihrer Authentifizierungsmethode gesperrt werden sollen.

### AUTHentication

Gibt die Methode der Kennwortauthentifizierung an, die für die Anmeldung bei einem Knoten erforderlich ist.

### Local

Gibt an, dass Knoten gesperrt werden sollen, die sich mit dem IBM Spectrum Protect-Server authentifizieren.

### LDap

Gibt an, dass Knoten gesperrt werden sollen, die sich mit einem LDAP-Verzeichnisservers authentifizieren.

## Beispiel: Einen bestimmten Clientknoten sperren

---

Den Clientknoten SMITH sperren.

```
lock node smith
```

## Beispiel: Alle Knoten sperren, die sich mit der lokalen IBM Spectrum Protect-Datenbank authentifizieren

Geben Sie den folgenden Befehl aus, um alle Knoten zu sperren, die sich mit dem IBM Spectrum Protect-Server authentifizieren:

```
lock node * authentication=local
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für LOCK NODE

| Befehl      | Beschreibung  |
|-------------|---|
| QUERY NODE  | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.                           |
| UNLOCK NODE | Ermöglicht einem gesperrten Benutzer in einer bestimmten Maßnahmendomäne wieder den Zugriff auf den Server. |

## LOCK PROFILE (Profil sperren)

Mit diesem Befehl kann auf einem Konfigurationsmanager ein Profil vorübergehend gesperrt werden, so dass die Konfigurationsdaten nicht an subscribierende verwaltete Server verteilt werden.

Dieser Befehl kann verwendet werden, wenn mehrere Aktualisierungen an der Konfiguration vorgenommen werden und diese Informationen erst verteilt werden sollen, wenn die Änderungen abgeschlossen sind.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-LOCK PROFILE--Profilname---.-60-----+-----+----->>  
'-Minuten-'
```

### Parameter

Profilname (Erforderlich)

Gibt das Profil an, das gesperrt werden soll. Es können Platzhalterzeichen verwendet werden, um mehrere Namen anzugeben.

Minuten

Gibt die Zeit in Minuten an, bevor IBM Spectrum Protect das Konfigurationsprofil entsperrt. Eine ganze Zahl von 0 bis 10000 angeben. Der Standardwert ist 60 Minuten. Wenn 0 angegeben wird, wird das Konfigurationsprofil nicht automatisch entsperrt. Den Befehl UNLOCK PROFILE verwenden, um das Profil zu entsperren, bevor die Zeitperiode verstrichen ist, oder um das Profil zu entsperren, wenn der Wert 0 angegeben wurde. Dieser Parameter ist wahlfrei.

## Beispiel: Ein Profil für eine bestimmte Zeit sperren

Das Profil DELTA 30 Minuten lang sperren.

```
lock profile delta 30
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für LOCK PROFILE

| Befehl                 | Beschreibung  |
|------------------------|---|
| COPY PROFILE           | Erstellt eine Kopie eines Profils.  |
| DEFINE PROFASSOCIATION | Ordnet Objekte einem Profil zu.   |
| DEFINE PROFILE         | Definiert ein Profil für die Verteilung von Informationen an verwaltete Server. |

| Befehl                 | Beschreibung   |
|------------------------|--|
| DELETE PROFASSOCIATION | Löscht die Zuordnung zwischen einem Objekt und einem Profil.             |
| DELETE PROFILE         | Löscht ein Profil aus einem Konfigurationsmanager.                       |
| QUERY PROFILE          | Zeigt Informationen über Konfigurationsprofile an.                       |
| SET CONFIGMANAGER      | Gibt an, ob ein Server ein Konfigurationsmanager ist.                    |
| UNLOCK PROFILE         | Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server. |
| UPDATE PROFILE         | Ändert die Beschreibung eines Profils.                                   |

## MACRO (Makro aufrufen)

Mit diesem Befehl kann eine Datei über die Verwaltungsbefehlszeile aufgerufen werden, die auszuführende IBM Spectrum Protect-Verwaltungsbefehle enthält.

Einschränkung: Verwenden Sie diesen Befehl nur für Verwaltungsbefehlszeilenclients.

Ein Makro ist eine Datei, die IBM Spectrum Protect-Verwaltungsbefehle enthält. Ein Makro kann vom Verwaltungs-Client nur im Stapelmodus oder im interaktiven Modus ausgegeben werden. Ein Makro wird als Datei auf der Verwaltungs-Client-Maschine (oder dem System) gespeichert. Makros werden nicht an Server verteilt und können nicht auf dem Server geplant werden.

Die Erstellung eines Makros zur Eingabe von Befehlen kann hilfreich sein, wenn Befehle ausgegeben werden sollen, die wiederholt verwendet werden, wenn Befehle ausgegeben werden, die mehrere Parameter enthalten, oder wenn zugehörige Befehle in einer bestimmten Reihenfolge verarbeitet werden sollen. Nach der Erstellung eines Makros können die enthaltenen Informationen aktualisiert und wiederverwendet werden, oder die Makrodatei kann kopiert, die Kopie geändert und dann die Kopie ausgeführt werden.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-MACRO--Makroname-----+-----><
| .-----+-----+-----+
| v         | |
|'---Substitutionswert---+'
```

## Parameter

Makroname (Erforderlich)

Gibt den Namen des Makros an.

Substitutionswert

Gibt den Wert einer Substitutionsvariablen in einem Makro an. Wenn eine Substitutionsvariable verwendet wird, kann ein Makro immer wieder verwendet werden, wenn dieselbe Task für verschiedene Objekte oder mit anderen Parameterwerten ausgeführt werden muß. Um einen Wert anzugeben, der Leerzeichen enthält, muß er in Anführungszeichen eingeschlossen werden. Dieser Parameter ist wahlfrei.

## Beispiel: Ein Makro zum Registrieren eines neuen Administrators erstellen

Die Makrodatei REGNG erstellen. Mit Hilfe des Makros einen neuen Administrator registrieren und ihm eine Berechtigung erteilen. Das Makro wie folgt schreiben:

```
/* Neuen Administrator registrieren und Berechtigung erteilen */
REGister Admin jones passwd          -
CONtactinfo="x1235"
GRant AUTHority jones                 -
CLasses=Policy
```

Den folgenden Befehl ausgeben, um das Makro auszuführen:

```
macro regng.mac
```

## Beispiel: Ein Makro unter Verwendung von Substitutionsvariablen schreiben

Die Makrodatei AUTHRG erstellen, die Substitutionsvariablen enthält, um einen neuen Administrator zu registrieren und ihm eine Berechtigung zu erteilen. Das Makro wie folgt schreiben:

```
/* Neuen Administrator registrieren und Berechtigung erteilen */
REGister Admin %1 %2 - /* Benutzer-ID und Kennwort eingeben */
CONtact=%3 /* Kontaktinfo eingeben (evtl. in Anführungszeichen) */
GRant AUTHority %1 - /* Server verwendet die definierte */
- /* Variable bereits */
Classes=%4 /* Berechtigungsklasse eingeben */
```

Einen Befehl ausgeben, der dem folgenden Befehl ähnelt. Dabei die Werte eingeben, die an den Server übergeben werden sollen, um den Befehl zu verarbeiten, wenn das Makro ausgeführt wird.

```
macro authrg.mac jones passwd x1235 Policy
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für MACRO

| Befehl   | Beschreibung   |
|----------|--|
| COMMIT   | Schreibt Änderungen in der Datenbank fest.   |
| ROLLBACK | Löscht alle Änderungen, die seit dem letzten COMMIT nicht in der Datenbank festgeschrieben wurden. |

### Zugehörige Konzepte:

Makros des Verwaltungsclients

## MIGRATE STGPOOL (Speicherpool in nächsten Speicherpool umlagern)

Mit diesem Befehl können Dateien aus einem Speicherpool in den nächsten Speicherpool in der Speicherhierarchie umgelagert werden.

Dieser Befehl kann nur mit primären Speicherpools verwendet werden. Das Datenformat des Speicherpools darf nicht NETAPPDUMP, CELERRADUMP oder NDMPDUMP sein. Daten können nicht in oder aus Speicherpools umgelagert werden, die mit einer Einheitenklasse CENTERA definiert sind.

Für einen bestimmten Speicherpool ist nur jeweils ein Umlagerungs- oder Wiederherstellungsprozess zulässig. Wird für den Speicherpool bereits ein Umlagerungs- oder Wiederherstellungsprozess ausgeführt, kann kein anderer Umlagerungsprozess für den Speicherpool gestartet werden.

Dieser Befehl sollte nur verwendet werden, wenn die automatische Umlagerung für den Speicherpool nicht verwendet wird. Um die Ausführung der automatischen Umlagerung zu verhindern, setzen Sie das Attribut HIGHMIG der Speicherpooldefinition auf 100.

Wird dieser Befehl verwendet, um einen Umlagerungsprozess zu starten, aber ist für den Speicherpool kein nächster Speicherpool in der Hierarchie angegeben, wird ein Wiederherstellungsprozess für den Quellenspeicherpool ausgelöst. Um den Wiederherstellungsprozess zu verhindern, definieren Sie den nächsten Speicherpool in der Hierarchie. Starten Sie dann den Umlagerungsprozess.

Der Befehl MIGRATE STGPOOL berücksichtigt die Werte der folgenden Parameter in den Befehlen DEFINE STGPOOL und UPDATE STGPOOL:

- MIGPROCESS
- MIGDELAY
- MIGCONTINUE
- NEXTPOOL
- LOWMIG

Tipp: Sie können den Wert des Parameters LOWMIG in den Befehlen DEFINE STGPOOL und UPDATE STGPOOL überschreiben, indem Sie einen Wert für den Parameter LOWMIG im Befehl MIGRATE STGPOOL angeben.

Der Befehl MIGRATE STGPOOL ignoriert den Wert des Parameters HIGHMIG der Speicherpooldefinition. Die Umlagerung erfolgt unabhängig vom Wert des Parameters HIGHMIG.

Dieser Befehl erstellt einen oder mehrere Umlagerungsprozesse, die mit dem Befehl CANCEL PROCESS abgebrochen werden können. Die Anzahl der Prozesse wird durch das Attribut MIGPROCESS der Speicherpooldefinition begrenzt. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Hinweis: Beim Umlagern von Daten aus einem primären Speicherpool, der für die Deduplizierung von Daten definiert ist, in einen anderen primären Speicherpool, der ebenfalls für die Deduplizierung von Daten definiert ist, werden doppelte Daten entfernt.

## Berechtigungsklasse

Um diesen Befehl auszugeben, benötigen Sie Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool, aus dem die Dateien umgelagert werden sollen, und für den nächsten Speicherpool, in den Dateien umgelagert werden sollen.

## Syntax

```
>>-MIGrate STGpool--Poolname--+-----+----->
                                     '-LOWmig---Zahl-'
                                     .-REclaim---No-----
>--+-----+-----+----->
   '-Duration---Minuten-'   '-REclaim---+No--+-'
                               '-Yes-'

   .-Wait---No-----
>--+-----+-----><
   '-Wait---+No--+-'
       '-Yes-'
```

## Parameter

### Poolname (Erforderlich)

Gibt den primären Speicherpool an, aus dem Dateien umgelagert werden sollen.

### DURation

Gibt die maximale Anzahl Minuten an, die die Umlagerung ausgeführt wird, bevor sie automatisch abgebrochen wird. Wenn die angegebene Anzahl Minuten verstrichen ist, bricht der Server automatisch alle Umlagerungsprozesse für diesen Speicherpool ab. Sobald die Prozesse den automatischen Abbruch erkennen, werden sie beendet. Aus diesem Grund kann die Umlagerung länger dauern als mit dem Wert für diesen Parameter angegeben ist. Es kann eine Zahl von 1 bis 9999 angegeben werden. Dieser Parameter ist wahlfrei. Falls nicht angegeben, stoppt der Server erst nach Erreichen der unteren Umlagerungsschwelle.

### LOWmig

Gibt für Plattenspeicherpools mit wahlfreiem Zugriff und mit sequenziellem Zugriff an, dass die Umlagerung gestoppt werden soll, wenn das Datenvolumen in dem Pool diesen Prozentsatz der geschätzten Kapazität des Pools erreicht oder unter diesem Prozentsatz liegt. Dieser Parameter ist wahlfrei.

Die Berechnung für Plattenspeicherpools mit sequenziellem Zugriff schließt die Kapazität aller für den Pool angegebenen Arbeitsdatenträger ein. Da die Umlagerung je nach Kollokation nach Knoten oder Dateibereich erfolgt, kann die Belegung des Speicherpools unter den für diesen Parameter angegebenen Wert fallen. Um den Speicherpool zu leeren, definieren Sie LOWMIG=0. Für andere Typen von Speicherpools mit sequenziellem Zugriff stoppt der Server die Umlagerung, wenn das Verhältnis der Datenträger, die Daten enthalten, zur Gesamtzahl der Datenträger in dem Speicherpool diesen Prozentsatz erreicht oder unter diesem Prozentsatz liegt. Die Gesamtzahl der Datenträger schließt die maximale Anzahl Arbeitsdatenträger ein. Sie können eine Zahl von 0 bis 99 für diesen optionalen Parameter angeben. Der Standardwert ist das Attribut LOWMIG der Speicherpooldefinition.

### REclaim

Gibt an, ob vor der Ausführung der Umlagerung die Wiederherstellung für den Speicherpool versucht wird. Dieser Parameter kann nur für einen Speicherpool mit sequenziellem Zugriff angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

#### No

Gibt an, dass der Server keine Wiederherstellung vor dem Starten der Umlagerung ausführt.

#### Yes

Gibt an, dass der Server vor dem Starten der Umlagerung eine Wiederherstellung ausführt. Alle Datenträger in dem Speicherpool, die der Wiederherstellungsschwelle entsprechen, die mit dem Attribut RECLAIM der Speicherpooldefinition angegeben wird, werden vor der Ausführung der Umlagerung wiederhergestellt. Entsprechen keine Datenträger der Wiederherstellungsschwelle, oder wurde nach der Wiederherstellung die LOWMIG-Schwelle nicht erreicht, beginnt der Server mit der Umlagerung. Bevor Speicherbereich für Speicherpools wiederhergestellt wird, die mit RECLAMATIONTYPE=SNAPLOCK definiert sind, löscht der Server während der Wiederherstellungsverarbeitung alle leeren WORM-FILE-Datenträger, die ihren Wiederherstellungszeitraum überschritten haben.

### Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

#### No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet.

Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Nachrichten, die von dem Hintergrundprozess erstellt werden, werden entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird dieser Prozess abgebrochen, wurden möglicherweise bereits einige Dateien vor dem Abbruch umgelagert.

Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Der Server zeigt dann die Ausgabenachrichten dem Verwaltungsclient an, wenn die Operation beendet ist. Nachrichten werden auch im Aktivitätenprotokoll und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.

Anmerkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

## Beispiel: Einen Speicherpool in den nächsten Speicherpool umlagern

Daten aus dem Speicherpool BACKUPPOOL in den nächsten Speicherpool umlagern. Angeben, dass der Server die Umlagerung so schnell wie möglich nach 90 Minuten beenden soll.


```
migrate stgpool backuppool duration=90
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für MIGRATE STGPOOL

| Befehl          | Beschreibung   |
|-----------------|--|
| CANCEL PROCESS  | Bricht einen Serverhintergrundprozess ab.              |
| QUERY PROCESS   | Zeigt Informationen zu dem Hintergrundprozess an.      |
| QUERY STGPOOL   | Zeigt Informationen zu Speicherpools an.               |
| RECLAIM STGPOOL | Führt eine Wiederherstellung für den Speicherpool aus. |

### Zugehörige Informationen:

 Dateien in einer Speicherpoolhierarchie umlagern

## MOVE-Befehle

Mit den MOVE-Befehlen können Sicherungs- oder Archivierungsdaten zwischen Speicherpools oder Datenträger zur Wiederherstellung nach einem Katastrophenfall vor Ort und an einen ausgelagerten Standort versetzt werden.

- MOVE CONTAINER (Container versetzen)
- MOVE DATA (Dateien auf einem Speicherpooldatenträger versetzen)
- MOVE DRMEDIA (DRM-Datenträger aus- und einlagern)
- MOVE GRPMEMBER (Servergruppenteil versetzen)
- MOVE MEDIA (Speicherpooldatenträger mit sequenziellem Zugriff versetzen)
- MOVE NODEDATA (Daten nach Knoten in einem Speicherpool mit sequenziellem Zugriff versetzen)

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## MOVE CONTAINER (Container versetzen)

Verwenden Sie diesen Befehl, um den Inhalt eines Speicherpoolcontainers in einen anderen Container zu versetzen, wenn ein Speicherpoolverzeichnis entfernt wird oder ein Container beschädigt ist.

Mit diesem Befehl können Sie auch den Inhalt eines Speicherpoolcontainers unter den folgenden Bedingungen versetzen:

- Wenn ein Upgrade für die Hardware durchgeführt wird
- Wenn E/A-Fehler auf einer Platte auftreten

## Berechtigungsklasse

Für diesen Befehl ist die eingeschränkte Speicherberechtigung erforderlich.

## Syntax



```

>>-MOVE CONTAINER--Containername----->
>--+-----+----->
  '-STGPOOLDIRectory----Verzeichnisname-'
  .-Wait----Yes----.
>--+-----+----->
  '-Wait----+Yes--+'
      '-No--'

```

## Parameter

### Containername (Erforderlich)

Gibt den Namen des Containers an, der versetzt werden soll. Sie müssen den vollständigen Pfadnamen des Containers angeben.

### STGPOOLDIRectory

Gibt den Namen des Speicherpoolverzeichnisses an, in das der Container versetzt wird. Dieser Parameter ist wahlfrei.

Wenn Sie ein Speicherpoolverzeichnis angeben, muss es sich in demselben Speicherpool wie der ursprüngliche Container befinden. Das Speicherpoolverzeichnis wird für den neuen Container verwendet. Wenn Sie kein Speicherpoolverzeichnis angeben, wählt der IBM Spectrum Protect-Server ein Speicherpoolverzeichnis aus demselben Speicherpool aus.

### Wait

Gibt an, ob darauf gewartet werden soll, dass der IBM Spectrum Protect-Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Geben Sie die folgenden Werte an:

#### No


Der Server verarbeitet diesen Befehl im Hintergrund und Sie können mit anderen Tasks fortfahren, während der Befehl verarbeitet wird. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden entweder in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, je nachdem, wo die Nachrichten protokolliert werden. Dies ist der Standardwert.

#### Yes

Der Server verarbeitet diesen Befehl im Vordergrund. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.

Einschränkung: Sie können den Parameter WAIT=YES nicht an der Serverkonsole angeben.

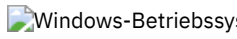
## Beispiel: Einen Container versetzen

 Linux-Betriebssysteme Den Container 0000000000000001.dcf aus dem Speicherpoolverzeichnis /data1/storage/dir1 in das Speicherpoolverzeichnis /data/storage/dir2 versetzen.

```

move container /data1/storage/dir1/00/0000000000000001.dcf
stgpooldir=/data/storage/dir2

```

 Windows-Betriebssysteme Den Container 0000000000000001.dcf aus dem Speicherpoolverzeichnis e:\data1\storage\dir1 in das Speicherpoolverzeichnis e:\data\storage\dir2 versetzen.

```

move container e:\data1\storage\dir1\00\0000000000000001.dcf
stgpooldir=e:\data\storage\dir2

```

Tabelle 1. Zugehörige Befehle für MOVE CONTAINER

| Befehl          | Beschreibung                                  |
|-----------------|---|
| AUDIT CONTAINER | Prüft einen Verzeichniscontainerspeicherpool. |
| QUERY CONTAINER | Zeigt Informationen zu einem Container an.    |

## MOVE DATA (Dateien auf einem Speicherpooldatenträger versetzen)

Mit diesem Befehl können Dateien von einem Speicherpooldatenträger auf andere Speicherpooldatenträger versetzt werden.

Einschränkung: Sie können diesen Befehl nicht für Datenträger verwenden, die Containerkopierspeicherpools zugeordnet sind. Dateien von einem Datenträger aus dem primären Speicherpool können nur auf Datenträger in demselben oder einem anderen primären Speicherpool versetzt werden. Dateien von einem Datenträger aus dem Kopierspeicherpool können nur auf Datenträger in demselben Kopierspeicherpool versetzt werden. Dateien von einem Datenträger aus dem Pool für aktive Daten können nur auf Datenträger in demselben Pool für aktive Daten versetzt werden.

Neben dem Versetzen von Daten von Datenträgern in Speicherpools mit dem Datenformat NATIVE oder NONBLOCK können Sie mit diesem Befehl auch Daten von Datenträgern in Speicherpools versetzen, die NDMP-Datenformate haben (NETAPPDUMP, CELERRADUMP oder NDMPDUMP). Der Zielspeicherpool muss dasselbe Datenformat wie der Quellenspeicherpool haben. Werden Daten aus einem Speicherpool zum Zweck eines Upgrades auf eine neue Bandtechnologie versetzt, muss der primäre Zielspeicherpool einem Speicherarchiv zugeordnet sein, das über die neue Einheit für die Bandlaufwerke verfügt. IBM Spectrum Protect unterstützt die Back-End-Datenversetzung für NDMP-Images.

Sie können keine Daten in einen Speicherpool oder aus einem Speicherpool versetzen, der mit einer Einheitenklasse CENTERA definiert ist.

Werden Dateien auf Datenträger in demselben Speicherpool versetzt, muss auf den Datenträgern genügend Speicherbereich verfügbar sein. Andernfalls schlägt die Operation fehl.

Werden Dateien von einem Datenträger mit sequenziellem Zugriff versetzt, sind mehrere Mountoperationen für Datenträger mit sequenziellem Zugriff erforderlich, um Dateien zu versetzen, die sich über mehrere Datenträger erstrecken.

Werden Dateien von einem Datenträger mit wahlfreiem Zugriff versetzt, löscht der Server alle Cachekopien von Dateien auf dem Datenträger.

Ein Datenträger ist möglicherweise nach dem Versetzen von Daten nicht leer, wenn Dateien aufgrund von Ein-/Ausgabefehlern auf der Einheit oder aufgrund von Fehlern in der Datei nicht auf einen anderen Datenträger verlagert werden können. Falls erforderlich, kann der Datenträger mit der Option zum Löschen aller Daten gelöscht werden. Die Dateien mit Ein-/Ausgabefehlern oder anderen Fehlern werden dann gelöscht.

Mit diesem Befehl können Dateien von einem ausgelagerten Datenträger in einen Kopierspeicherpool oder einen Pool für aktive Daten versetzt werden. Da der ausgelagerte Datenträger nicht geladen werden kann, ruft der Server die Dateien auf dem ausgelagerten Datenträger entweder aus einem primären Speicherpool oder einem anderen Kopierspeicherpool ab. Diese Dateien werden dann auf die Zieldatenträger im ursprünglichen Kopierspeicherpool oder Pool für aktive Daten geschrieben.

Während des Datenversetzungsprozesses können Pools für aktive Daten nicht verwendet werden, um Daten abzurufen.

Wenn Sie den Befehl MOVE DATA für einen ausgelagerten Datenträger angeben, der durch Kollokation zusammengefasste Daten enthält, müssen Sie den Befehl MOVE DATA möglicherweise mehrmals ausgeben, um alle Daten von dem Datenträger zu versetzen. Wenn Sie beispielsweise Dateibereichskollokationsgruppen mit einem ausgelagerten Datenträger verwenden, der Dateibereiche in einer Kollokationsgruppe und Dateibereiche, die nicht in der Gruppe sind, enthält, müssen Sie zwei Befehle MOVE DATA ausgeben. Mit jedem Befehl MOVE DATA werden die Daten für eine einzelne kollokierte oder nicht kollokierte Gruppe von Dateien versetzt.

Der Befehl MOVE DATA darf nicht verwendet werden, wenn ein Zurückschreibungsprozess (RESTORE STGPOOL oder RESTORE VOLUME) ausgeführt wird. Durch den Befehl MOVE DATA könnte die Zurückschreibung unvollständig sein. Wird der Befehl MOVE DATA während einer Zurückschreibungsoperation ausgegeben und empfangen Sie eine Fehlermeldung, die angibt, dass eine oder mehrere Dateien gesperrt sind und nicht versetzt werden können, müssen Sie den Befehl MOVE DATA nach Beendigung der Zurückschreibungsoperation erneut ausgeben, damit alle übrigen Dateien versetzt werden.

Hinweis:

Wird dieser Befehl ausgegeben, werden doppelte Daten entfernt, wenn:

- Daten aus einem primären Speicherpool, der für die Deduplizierung von Daten definiert ist, in einen anderen primären Speicherpool versetzt werden, der ebenfalls für die Deduplizierung von Daten definiert ist.
- Daten innerhalb eines Kopierspeicherpools versetzt werden, der für die Deduplizierung von Daten definiert ist.
- Daten innerhalb eines Pools für aktive Daten versetzt werden, der für die Deduplizierung von Daten definiert ist.

Ein Datenträger in einem deduplizierten Speicherpool kann Dateien enthalten, die logisch gelöscht sind, aber dennoch mit Dateien auf anderen Datenträgern verknüpft sind. Wenn Sie den Befehl MOVE DATA verwenden, um den Inhalt eines deduplizierten Speicherpooldatenträgers in einen nicht deduplizierten Speicherpool zu versetzen, werden die logisch gelöschten Dateien nicht auf den neuen Datenträger geschrieben, da sie logisch nicht vorhanden sind. Die gelöschten Dateien werden zur Referenzierung anderer Dateien auf den Originaldatenträgern aufbewahrt. Der Prozess MOVE DATA wird erfolgreich beendet, aber die gelöschten Dateien werden nicht auf den neuen Zieldatenträger versetzt und der Quelldatenträger wird nicht gelöscht. Sie können den Befehl QUERY CONTENT mit dem Parameter FOLLOWLINKS=YES oder FOLLOWLINKS=JUSTLINKS ausgeben, um zu prüfen, ob der Datenträger Dateien enthält, die mit Dateien auf anderen Datenträgern verknüpft sind.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder die eingeschränkte Speicherberechtigung für den Speicherpool erforderlich, zu dem der Datenträger gehört, sowie für den neuen Speicherpool, sofern angegeben.

## Syntax

---

```

>>-MOVE Data--Datenträgername--+-+-----+----->
                                     '-STGpool-----Poolname-'

.-SHREDTONoshred---No-----.
>--+-+-----+----->
    '-SHREDTONoshred---No---+'
                                     '-Yes-'

                                     (1) (2)
.-RECONStruct-----No oder Yes-----
>--+-+-----+----->
    '-RECONStruct-----+No---+'
                                     '-Yes-'

.-Wait-----No-----
>--+-+-----+-----><
    '-Wait-----+No---+'
                                     '-Yes-'

```

#### Anmerkungen:

1. Der Standardwert ist NO, wenn entweder der Quellen- oder der Zielspeicherpool ein Speicherpool mit wahlfreiem Zugriff ist. Der Standardwert ist YES, wenn sowohl der Quellenspeicherpool als auch der Zielspeicherpool ein Speicherpool mit sequenziellem Zugriff ist.
2. Dieser Parameter ist nicht verfügbar oder wird ignoriert, wenn das Datenformat NETAPPDUMP, CELERRADUMP oder NDMPDUMP ist.

## Parameter

#### Datenträgername (Erforderlich)

Gibt den Speicherpooldatenträger an, von dem Dateien versetzt werden sollen.

#### STGpool

Gibt den primären Speicherpool an, in den Dateien versetzt werden sollen (Zielspeicherpool). Dieser Parameter ist wahlfrei und gilt nur für das Versetzen von Daten von Datenträgern aus dem primären Speicherpool. Wird kein Wert für diesen Parameter angegeben, werden Dateien auf andere Datenträger in demselben Speicherpool versetzt.

#### SHREDTONoshred

Gibt an, ob Daten aus einem Speicherpool, der das Schreddern erzwingt, in einen Speicherpool, der das Schreddern nicht erzwingt, versetzt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

##### No

Gibt an, dass es der Server nicht erlaubt, dass Daten aus einem Speicherpool, der das Schreddern erzwingt, in einen Speicherpool, der das Schreddern nicht erzwingt, versetzt werden. Wenn der Quellenspeicherpool das Schreddern erzwingt und der Zielspeicherpool das Schreddern nicht erzwingt, schlägt die Operation fehl.

##### Yes

Gibt an, dass es der Server erlaubt, dass Daten aus einem Speicherpool, der das Schreddern erzwingt, in einen Speicherpool, der das Schreddern nicht erzwingt, versetzt werden. Die Quelldaten werden geschreddert, wenn die Operation abgeschlossen ist. Die Zieldaten werden beim Löschen nicht geschreddert.

#### RECONStruct

Gibt an, ob Dateiaggregate beim Versetzen von Daten wiederhergestellt werden sollen. Bei der Wiederherstellung wird leerer Speicherbereich entfernt, der sich durch das Löschen von logischen Dateien aus einem Aggregat angesammelt hat. Dieser Parameter ist wahlfrei. Ist sowohl der Quellenspeicherpool als auch der Zielspeicherpool ein Speicherpool mit sequenziellem Zugriff, ist der Standardwert YES. Ist entweder der Quellen- oder der Zielspeicherpool ein Speicherpool mit wahlfreiem Zugriff, ist der Standardwert NO.

Der Parameter ist nicht verfügbar oder wird ignoriert, wenn eine der folgenden Bedingungen zutrifft:

- Das Datenformat ist NETAPPDUMP, CELERRADUMP oder NDMPDUMP.
- Die Daten befinden sich in einem Speicherpool, der für die Deduplizierung von Daten konfiguriert ist.
- Der Zielspeicherpool für die Datenversetzung ist für die Deduplizierung von Daten konfiguriert.

**Achtung:** Bei der Wiederherstellung werden inaktive Sicherungsdateien in Pools für aktive Daten entfernt. Geben Sie RECONSTRUCT=NO an, wenn die Daten in einen Pool für aktive Daten versetzt werden, der nicht für die Deduplizierung von Daten konfiguriert ist, verbleiben inaktive Sicherungsdateien in dem Speicherpool.

#### Gültige Werte:

##### No

Gibt an, dass die Wiederherstellung von Dateiaggregaten beim Versetzen von Daten nicht ausgeführt wird.

Yes

Gibt an, dass die Wiederherstellung von Dateiaгрегатам beim Versetzen von Daten ausgeführt wird. Sie können diese Option nur angeben, wenn Quellen- und Zielspeicherpool Speicherpools mit sequenziellem Zugriff sind.

Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

Bei dem Hintergrundprozess erstellte Nachrichten werden vom Server entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird ein Hintergrundprozess MOVE DATA abgebrochen, wurden einige Dateien möglicherweise vor dem Abbruch bereits versetzt.

Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Der Befehl muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist.

Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

## Beispiel: Dateien auf einem Speicherpooldatenträger versetzen

Dateien vom Speicherpooldatenträger STGVOL.1 auf alle verfügbaren Datenträger versetzen, die dem Speicherpool 8MMPool zugeordnet sind.

```
move data stgvol.1 stgpool=8mmpool
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für MOVE DATA

| Befehl            | Beschreibung   |
|-------------------|--|
| CANCEL PROCESS    | Bricht einen Serverhintergrundprozess ab.  |
| DEFINE VOLUME     | Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll. |
| DELETE VOLUME     | Löscht einen Datenträger aus einem Speicherpool.   |
| MOVE DRMEDIA      | Versetzt DRM-Datenträger vor Ort und lagert sie aus.   |
| QUERY ACTLOG      | Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.   |
| QUERY CONTENT     | Zeigt Informationen über Dateien in einem Speicherpooldatenträger an.  |
| QUERY DRMEDIA     | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.                  |
| QUERY PROCESS     | Zeigt Informationen über Hintergrundprozesse an.   |
| QUERY SHREDSTATUS | Zeigt Informationen zu Daten an, die auf das Schreddern warten.  |
| SHRED DATA        | Startet manuell den Prozess zum Schreddern gelöschter Daten.   |

## MOVE DRMEDIA (DRM-Datenträger aus- und einlagern)

Mit diesem Befehl können Datenträger verfolgt werden, die ausgelagert werden sollen, und verfallene oder leere Datenträger identifiziert werden, die vor Ort versetzt werden sollen. Sie können Datenbanksicherungsdaterträge und Datenträger in Kopierspeicherpools, Containerkopierspeicherpools und Speicherpools für aktive Daten verfolgen.

Die Verarbeitung von Datenträgern durch diesen Befehl hängt vom Verwendungszweck der Datenträger ab:

Sicherungen der Serverdatenbank

Mit dem Parameter SOURCE in diesem Befehl kann gesteuert werden, ob der Befehl Datenbanksicherungsdaterträge verarbeitet. Der Befehl kann Datenträger verarbeiten, die für Gesamt- und Teilsicherungen oder Datenbankmomentaufnahmesicherungen

verwendet werden. Es können keine virtuellen Datenträger angegeben werden (Sicherungsobjekte, die auf einem anderen Server gespeichert werden). Datenträger können von Status zu Status geändert werden, oder es können der Parameter TOSTATE verwendet und Status übersprungen werden, um die Bewegungen zu vereinfachen.

#### Kopienspeicherpools

Der Befehl MOVE DRMEDIA verarbeitet immer Kopienspeicherpooldatenträger.

#### Containerkopienspeicherpools

Standardmäßig sind Datenträger in Containerkopienspeicherpools nicht für die Verarbeitung mit dem Befehl MOVE DRMEDIA auswählbar. Um Datenträger in Containerkopienspeicherpools zu verarbeiten, müssen Sie zuerst den Befehl SET DRMCOPYCONTAINERSTGPOOL ausgeben oder den Parameter COPYCONTAINERSTGPOOL im Befehl MOVE DRMEDIA angeben.

#### Speicherpools für aktive Daten

Standardmäßig sind Datenträger in Speicherpools für aktive Daten nicht für die Verarbeitung mit dem Befehl MOVE DRMEDIA auswählbar. Um Datenträger in Pools für aktive Daten zu verarbeiten, müssen Sie zuerst den Befehl SET DRMACTIVEDATASTGPOOL ausgeben oder den Parameter ACTIVATEDATASTGPOOL im Befehl MOVE DRMEDIA angeben.

Mit dem Befehl QUERY ACTLOG kann abgefragt werden, ob der Befehl MOVE DRMEDIA erfolgreich ausgeführt wurde. Diese Informationen können auch über die Serverkonsole angezeigt werden.

Einschränkung: Führen Sie die Befehle MOVE DRMEDIA und BACKUP STGPOOL nicht gleichzeitig aus. Stellen Sie sicher, dass die Speicherpoolsicherungsprozesse abgeschlossen wurden, bevor der Befehl MOVE DRMEDIA ausgegeben wird.

## Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Wenn der Parameter CMD angegeben wird und die Serveroption REQSYSAUTHOUTFILE auf NO gesetzt ist: Bedienerberechtigung, uneingeschränkte Speicherberechtigung oder Systemberechtigung.
- Wenn der Parameter CMD angegeben wird und die Serveroption REQSYSAUTHOUTFILE auf YES (Standardwert) gesetzt ist: Systemberechtigung.

## Syntax

```
>>-MOVE DRMedia--Datenträgername----->
>--+-----+----->
  '-WHEREState----+MOUNTable-----+'
      +-NOTMOUNTable----+
      +-COUrier-----+
      +-VAULTRetrieve----+
      '-COURIERRetrieve-'
>--+-----+----->
  '-BEGINDate----Datum-' '-ENDDate----Datum-'
>--+-----+----->
  '-BEGINTime----Zeit-' '-ENDTime----Zeit-'
>--+-----+----->
  '-COPYContainerstgpool----Poolname-'
>--+-----+----->
  '-COPYstgpool----Poolname-'
>--+-----+----->
  '-ACTIVEDatastgpool----Poolname-'
  .-Source----DBBackup----- .
>--+-----+----->
  '-Source----+DBBackup----+'
      +-DBSnapshot+
      '-DBNone-----'
  .-REMove----Bulk----- .
>--+-----+----->
  '-REMove----+No-----+'
      +-Yes-----+
      +-Bulk-----+
      '-Untileefull-'
>--+-----+----->
  '-TOSState----+NOTMOUNTable----+'
      +-COUrier-----+
```



#### BEGINDate

Gibt das Anfangsdatum an, das zum Auswählen der Datenträger verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder nach dem angegebenen Datum in seinen aktuellen Status ändert. Standardwert ist das früheste Datum, ab dem Datenträgerdaten vorliegen.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                           | Beschreibung  | Beispiel   |
|--------------------------------|---|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum.                                     | 09/15/1998   |
| TODAY                          | Das aktuelle Datum.                                       | TODAY  |
| TODAY-Tage oder -Tage          | Das aktuelle Datum minus der Anzahl der angegebenen Tage. | TODAY-7 oder -7<br>Sollen Datenträger identifiziert werden, die vor einer Woche in ihren aktuellen Status geändert wurden, können Sie TODAY-7 oder -7 angeben. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.                             | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.       | EOLM-1<br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.   |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.                       | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.  | BOTM+9<br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.  |

#### ENDDate

Gibt das Enddatum an, das zum Auswählen der Datenträger verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder vor dem angegebenen Datum in seinen aktuellen Status ändert. Standardwert ist das aktuelle Datum.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum.  | 09/15/1998   |
| TODAY                          | Das aktuelle Datum.  | TODAY<br>Sollen Datenträger identifiziert werden, die heute in ihren aktuellen Status geändert wurden, geben Sie TODAY an.                                     |
| TODAY-Tage oder -Tage          | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage beträgt 9999. | TODAY-1 oder -1<br>Sollen Datenträger identifiziert werden, die vor einer Woche in ihren aktuellen Status geändert wurden, können Sie TODAY-1 oder -1 angeben. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.   |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.  |

#### BEGINTime

Gibt die Anfangszeit an, die zum Auswählen der Datenträger für die Verarbeitung verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder nach der angegebenen Uhrzeit und dem angegebenen Datum in seinen aktuellen Status ändert. Der Standardwert ist Mitternacht (00:00:00) an dem mit dem Parameter BEGINDATE angegebenen Datum.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert                  | Beschreibung   | Beispiel  |
|-----------------------|--|---|
| HH:MM:SS              | Eine bestimmte Uhrzeit am angegebenen Anfangsdatum.                                    | 12:33:28  |
| NOW                   | Die aktuelle Uhrzeit am angegebenen Anfangsdatum.                                      | NOW   |
| NOW+HH:MM oder +HH:MM | Die aktuelle Uhrzeit plus der Anzahl Stunden und Minuten am angegebenen Anfangsdatum.  | NOW+03:00 oder +03:00   |
| NOW-HH:MM oder -HH:MM | Die aktuelle Uhrzeit minus der Anzahl Stunden und Minuten am angegebenen Anfangsdatum. | NOW-03:30 oder -03:30<br><br>Wird der Befehl MOVE DRMEDIA um 9:00 Uhr mit der Angabe BEGINTIME=NOW-03:30 oder BEGINTIME=-03:30 ausgegeben, identifiziert der Server die Datenträger, die um 5:30 Uhr am angegebenen Anfangsdatum in ihren aktuellen Status geändert wurden. |

#### ENDTime

Gibt die Endzeit an, die zum Auswählen der Datenträger für die Verarbeitung verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder nach der angegebenen Uhrzeit und dem angegebenen Datum in seinen aktuellen Status ändert. Der Standardwert ist 23:59:59.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert                  | Beschreibung   | Beispiel   |
|-----------------------|--|--|
| HH:MM:SS              | Eine bestimmte Uhrzeit am angegebenen Enddatum.                                    | 12:33:28   |
| NOW                   | Die aktuelle Uhrzeit am angegebenen Enddatum.                                      | NOW  |
| NOW+HH:MM oder +HH:MM | Die aktuelle Uhrzeit plus der Anzahl Stunden und Minuten am angegebenen Enddatum.  | NOW+03:00 oder +03:00<br><br>Wird der Befehl MOVE DRMEDIA um 9:00 Uhr mit der Angabe ENDTIME=NOW+03:30 oder ENDTIME=+03:30 ausgegeben, identifiziert der Server die Datenträger, die um 12:30 Uhr am angegebenen Enddatum in ihren aktuellen Status geändert wurden. |
| NOW-HH:MM oder -HH:MM | Die aktuelle Uhrzeit minus der Anzahl Stunden und Minuten am angegebenen Enddatum. | NOW-03:30 oder -03:30  |

#### COPYCONTAINERSTGPOOL

Gibt den Namen des Containerkopierspeicherpools an, dessen Datenträger verarbeitet werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Werden bei der Angabe dieses Namens Platzhalterzeichen verwendet, muss auch der Parameter WHERESTATE angegeben werden.

Die mit diesem Parameter angegebenen Containerkopierspeicherpools überschreiben die mit dem Befehl SET DRMCOPYCONTAINERSTGPOOL angegebenen Speicherpools. Wird dieser Parameter nicht angegeben, wählt der Server die Speicherpools wie folgt aus:

- Wenn der Befehl SET DRMCOPYCONTAINERSTGPOOL zuvor mit gültigen Containerkopierspeicherpoolnamen ausgegeben wurde, verarbeitet der Server nur diese Speicherpools.
- Wenn der Befehl SET DRMCOPYCONTAINERSTGPOOL nicht ausgegeben wurde oder alle Containerkopierspeicherpools mit dem Befehl SET DRMCOPYCONTAINERSTGPOOL entfernt wurden, verarbeitet der Server alle Containerkopierspeicherpooldatenträger auf der Basis der Einstellung des Parameters WHERESTATE. Wird der Parameter auf den Wert NOTMOUNTABLE, COURIER, VAULTRETRIEVE oder COURIERRETRIEVE gesetzt, werden die Datenträger verarbeitet. Lautet der Wert MOUNTABLE, werden die Datenträger nicht verarbeitet.

#### COPYSTGPOOL

Gibt den Namen des Kopierspeicherpools an, dessen Datenträger verarbeitet werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Werden bei der Angabe dieses Namens Platzhalterzeichen verwendet, muss auch der Parameter WHERESTATE angegeben werden.

Die mit diesem Parameter angegebenen Kopierspeicherpools überschreiben die mit dem Befehl SET DRMCOPYSTGPOOL angegebenen Kopierspeicherpools. Wird dieser Parameter nicht angegeben, wählt der Server die Speicherpools wie folgt aus:



- Wurde der Befehl SET DRMCOPYSTGPOOL zuvor mit gültigen Kopierspeicherpoolnamen ausgegeben, verarbeitet der Server nur diese Speicherpools.
- Wurde der Befehl SET DRMCOPYSTGPOOL nicht ausgegeben, oder werden alle Kopierspeicherpools mit dem Befehl SET DRMCOPYSTGPOOL entfernt, verarbeitet der Server alle Kopierspeicherpooldatenträger in dem angegebenen Status. Die verfügbaren Status sind MOUNTABLE, NOTMOUNTABLE, COURIER, VAULTRETRIEVE und COURIERRETRIEVE.

#### ACTIVEDatastgpool

Gibt den Namen des Pools für aktive Daten an, dessen Datenträger verarbeitet werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Werden bei der Angabe dieses Namens Platzhalterzeichen verwendet, muss auch der Parameter WHERESTATE angegeben werden.

Die mit diesem Parameter angegebenen Pools für aktive Daten überschreiben die mit dem Befehl SET DRMACTIVEDATASTGPOOL angegebenen Pools für aktive Daten. Wird dieser Parameter nicht angegeben, wählt der Server die Speicherpools wie folgt aus:

- Wurde der Befehl SET DRMACTIVEDATASTGPOOL zuvor mit gültigen Namen von Pools für aktive Daten ausgegeben, verarbeitet der Server nur diese Speicherpools.
- Wurde der Befehl SET DRMACTIVEDATASTGPOOL nicht ausgegeben, oder werden alle Pools für aktive Daten mit dem Befehl SET DRMACTIVEDATASTGPOOL entfernt, verarbeitet der Server alle Datenträger im Pool für aktive Daten in dem angegebenen Status. Die verfügbaren Status sind NOTMOUNTABLE, COURIER, VAULTRETRIEVE und COURIERRETRIEVE. Datenträger im Status MOUNTABLE werden nicht verarbeitet.

#### Source

Gibt an, ob Datenbanksicherungsdatenträger bei der Verarbeitung berücksichtigt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist DBBACKUP. Geben Sie einen der folgenden Werte an:

##### DBBackup

Gibt an, dass der Server Datenbanksicherungsdatenträger mit Gesamt- und Teilsicherungen bei der Verarbeitung berücksichtigt.

##### DBSnapshot

Gibt an, dass der Server Sicherungsdatenträger mit Datenbankmomentaufnahmen bei der Verarbeitung berücksichtigt.

##### DBNone

Gibt an, dass der Server keine Datenbanksicherungsdatenträger bei der Verarbeitung berücksichtigt.

#### REMove

Gibt an, dass der Server versucht, den Datenträger aus dem Kassettenarchiv in die Serviceein-/-ausgabestation oder die Eingangs-/Ausgangsanschlüsse zu versetzen. Dieser Parameter ist wahlfrei. Gültige Werte sind YES, NO, BULK und UNTILEEFULL. Der Standardwert ist BULK. Die Antwort des Servers auf jeden Wert und den Standardwert hängt vom Typ des Speicherarchivs ab. Einschränkung: Sie können die Option REMOVE=UNTILEEFULL nur mit dem Speicherarchivtyp SCSI verwenden.

#### SCSI-Kassettenarchive

Die Antwort des Servers auf den Befehl ist davon abhängig, ob das Speicherarchiv Eingangs-/Ausgangsanschlüsse hat und, wenn dies der Fall ist, ob ein Anschluss für die Verwendung verfügbar ist. Siehe die folgende Tabelle.

Tabelle 1. Antwort des Servers für SCSI-Kassettenarchive

| Kassettenarchivmerkmal                                 | Antwort des Servers bei Angabe von REMOVE=YES   | Antwort des Servers bei Angabe von REMOVE=BULK  | Antwort des Servers bei Angabe von REMOVE=NO  | Antwort des Servers bei Angabe von REMOVE=UNTILEEFULL   |
|--|---|---|---|---|
| Kassettenarchiv hat keine Eingangs-/Ausgangsanschlüsse | Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben. | Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. | Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. | Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. |

| Kassettenarchivmerkmal   | Antwort des Servers bei Angabe von REMOVE=YES   | Antwort des Servers bei Angabe von REMOVE=BULK  | Antwort des Servers bei Angabe von REMOVE=NO   | Antwort des Servers bei Angabe von REMOVE=UNTILEE FULL  |
|--|---|---|--|---|
| Kassettenarchiv hat Eingangs-/Ausgangsanschlüsse und ein Eingangs-/Ausgangsanschluss ist verfügbar | Versetzt der Server die Kassette in den verfügbaren Eingangs-/Ausgangsanschluss und gibt die Anschlussadresse in einer Nachricht an.<br><br>Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben. | Versetzt der Server die Kassette in den verfügbaren Eingangs-/Ausgangsanschluss und gibt die Anschlussadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. | Gibt der Server die Anschlussadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. | Versetzt der Server die Kassette in den verfügbaren Eingangs-/Ausgangsanschluss und gibt die Anschlussadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. |
| Kassettenarchiv hat Eingangs-/Ausgangsanschlüsse, aber es sind keine Anschlüsse verfügbar          | Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben.     | Wartet der Server auf einen verfügbaren Anschluss.  | Gibt der Server die Anschlussadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. | Schlägt der Befehl fehl, und alle verbleibenden auswählbaren Datenträger werden nicht verarbeitet.<br><br>Machen Sie den Anschluss verfügbar und wiederholen Sie den Befehl.  |

#### 349X-Kassettenarchive

##### REMOVE=YES

Der 3494-Kassettenarchivmanager (Library Manager) gibt die Kassette an die Serviceein-/ausgabestation aus.

##### REMOVE=BULK

Der 3494-Kassettenarchivmanager (Library Manager) gibt die Kassette an die Ausgabeeinrichtung mit hoher Speicherkapazität aus.

##### REMOVE=NO

Der 3494-Kassettenarchivmanager (Library Manager) gibt den Datenträger nicht aus. Der Server lässt die Kassette für die Verwendung durch andere Anwendungen in dem Kassettenarchiv in der Kategorie INSERT.

#### ACSL5-Kassettenarchive

##### REMOVE=YES oder REMOVE=BULK

Der Server gibt die Kassette an die Serviceein-/ausgabestation aus.

Dann löscht der Server den Datenträgereintrag aus dem Serverdatenträgerbestand im Kassettenarchiv.

Wenn Sie Datenträger aus dem Status MOUNTABLE unter Angabe von REMOVE=YES versetzen, verwendet der Befehl MOVE MEDIA mehrere Schächte in dem CAP für ein StorageTek-Kassettenarchiv mit ACSLS.

##### REMOVE=NO

Der Server gibt die Kassette nicht aus.

Der Server löscht den Datenträgereintrag aus dem Kassettenarchivbestand des Servers und lässt den Datenträger in dem Kassettenarchiv.

#### Externe Kassettenarchive

Sie können REMOVE=YES, REMOVE=BULK oder REMOVE=NO angeben. Für jeden Wert fordert der Server den externen Kassettenarchivmanager zur Ausgabe des Datenträgers aus dem Kassettenarchiv auf.

Es hängt vom externen Kassettenarchivmanager ab, ob der Datenträger aus dem Kassettenarchiv ausgegeben wird. Lesen Sie in der Dokumentation zum externen Kassettenarchiv die Informationen zu den Prozeduren, die ausgeführt werden müssen, wenn Sie den Befehl MOVE DRMEDIA verwenden, um Datenträger zu verfolgen.

#### TOSTate

Gibt den Zielstatus der Datenträger an, die verarbeitet werden. Dieser Parameter ist erforderlich, wenn der Parameter WHERESTATE nicht angegeben wird. Wird der Parameter TOSTATE angegeben, aber der Parameter WHERESTATE nicht angegeben, müssen Sie den Datenträgernamen angeben. Platzhalterzeichen sind nicht zulässig. Siehe Tabelle 2 und Tabelle 3. Geben Sie einen der folgenden Werte an:

##### NOTMOUNTable

Gibt an, dass Datenträger in den Status NOTMOUNTABLE übergehen sollen. Dieser Wert ist nur gültig, wenn die Datenträger den Status MOUNTABLE haben.

Befinden sich Datenträger in einem automatisierten Kassettenarchiv, kann der Server die Datenträger abhängig vom Verhalten des Parameters REMOVE aus dem Kassettenarchiv ausgeben, bevor sie in den Status NOTMOUNTABLE geändert werden.

Bei externen Kassettenarchiven sendet der Server Anforderungen zur Ausgabe der Datenträger an den externen Kassettenarchivmanager. Es hängt vom externen Kassettenarchivmanager ab, ob die Datenträger aus dem Kassettenarchiv ausgegeben werden. Lesen Sie in der Dokumentation zum externen Kassettenarchiv die Informationen zu den Prozeduren, die ausgeführt werden müssen, wenn Sie den Befehl MOVE DRMEDIA verwenden, um die Datenträger zu verfolgen.

##### COUrier

Gibt an, dass Datenträger in den Status COURIER übergehen sollen. Dieser Wert ist nur gültig, wenn die Datenträger den Status MOUNTABLE oder NOTMOUNTABLE haben.

Abhängig vom Verhalten des Parameters REMOVE und davon, ob sich Datenträger in einem automatisierten Kassettenarchiv befinden, kann der Server die Datenträger aus dem Kassettenarchiv ausgeben, bevor sie in den Status COURIER geändert werden.

Bei externen Kassettenarchiven sendet der Server Anforderungen zur Ausgabe der Datenträger an den externen Kassettenarchivmanager. Es hängt vom externen Kassettenarchivmanager ab, ob die Datenträger aus dem Kassettenarchiv ausgegeben werden. Lesen Sie in der Dokumentation zum externen Kassettenarchiv die Informationen zu den Prozeduren, die ausgeführt werden müssen, wenn Sie den Befehl MOVE DRMEDIA verwenden, um die Datenträger zu verfolgen.

##### VAult

Gibt an, dass Datenträger in den Status VAULT übergehen sollen. Dieser Wert ist nur gültig, wenn die Datenträger den Status MOUNTABLE, NOTMOUNTABLE oder COURIER haben.

Abhängig vom Verhalten des Parameters REMOVE und davon, ob sich Datenträger in einem automatisierten Kassettenarchiv befinden, kann der Server die Datenträger aus dem Kassettenarchiv ausgeben, bevor sie in den Status VAULT geändert werden.

Bei externen Kassettenarchiven sendet der Server Anforderungen zur Ausgabe der Datenträger an den externen Kassettenarchivmanager. Es hängt vom externen Kassettenarchivmanager ab, ob die Datenträger aus dem Kassettenarchiv ausgegeben werden. Lesen Sie in der Dokumentation zum externen Kassettenarchiv die Informationen zu den Prozeduren, die ausgeführt werden müssen, wenn Sie den Befehl MOVE DRMEDIA verwenden, um die Datenträger zu verfolgen.

##### COURIERRetrieve

Gibt an, dass Datenträger in den Status COURIERRETRIEVE übergehen sollen. Dieser Wert ist nur gültig, wenn die Datenträger den Status VAULTRETRIEVE haben.

##### ONSITERetrieve

Gibt an, dass Datenträger in den Status ONSITERETRIEVE übergehen sollen. Dieser Wert ist nur gültig, wenn die Datenträger den Status VAULTRETRIEVE oder COURIERRETRIEVE haben. Für Datenbanksicherungsdatenträger und Arbeitsdatenträger aus Kopierspeicherpools, die in den Status ONSITERETRIEVE übergehen, löscht der Server die Datenträgersätze aus der Datenbank.

#### WHERELocation

Gibt den aktuellen Standort der Datenträger an. Dieser Parameter ist wahlfrei. Die maximale Länge des Standorts beträgt 255 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

#### TOLocation

Gibt den Zielstandort der Datenträger an. Dieser Parameter ist wahlfrei. Die maximale Länge des angegebenen Standorts beträgt 255 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält. Wird kein Zielstandort angegeben, wird

der mit dem Befehl SET DRMNOTMOUNTABLE definierte Standort verwendet.

## CMD

Gibt einen Befehl an, der für jeden Datenträger ausgegeben werden soll, der von dem Befehl MOVE DRMEDIA verarbeitet wird. DRM schreibt die Befehle in eine Datei, die mit dem Parameter CMDFILENAME angegeben wird. Nach Abschluss der Operation MOVE DRMEDIA können die Befehle in der Datei ausgegeben werden. Der Befehl kann bis zu 255 Zeichen enthalten. Enthält der Befehl mehr als 240 Zeichen, wird er in mehrere Zeilen geteilt und es werden Fortsetzungszeichen (+) hinzugefügt. Sie müssen möglicherweise das Fortsetzungszeichen auf der Basis des Betriebssystems ändern. Dieser Parameter ist wahlfrei.

### Befehl

Die Befehlszeichenfolge, die in Anführungszeichen eingeschlossen wird. Die Zeichenfolge darf keine eingebetteten Anführungszeichen enthalten. Beispielsweise ist der folgende Parameter CMD gültig:

```
cmd="checkin libvol lib8mm &vol status=scratch"
```

Das folgende Beispiel zeigt eine ungültige Angabe des Parameters CMD:

```
cmd=""checkin libvol lib8mm" &vol status=scratch""
```

Der Befehl kann Substitutionsvariablen enthalten. Bei den Variablen muss die Groß-/Kleinschreibung nicht berücksichtigt werden. Die Variablen dürfen keine Leerstellen hinter dem Et-Zeichen (&) enthalten. Sie können die folgenden Werte angeben:

#### &VOL

Ein Datenträgername.

#### &LOC

Ein Datenträgerstandort.



#### &VOLDSN

Der Dateiname, der in die Kennsätze der Datenträger mit sequenziellem Zugriff geschrieben werden soll. Wenn beispielsweise die entsprechende Einheitenklasse BKP als Präfix des Banddatenträgers definiert, könnte der Dateiname eines Kopierspeicherpoolbanddatenträgers BKP.BFS und der Dateiname eines Datenbanksicherungsbanddatenträgers BKP.DBB lauten.

#### &NL

Das Zeilenvorschubzeichen. Wenn Sie das Zeilenvorschubzeichen verwenden, wird der Befehl bei der Variablen &NL geteilt. Falls erforderlich, muss das entsprechende Fortsetzungszeichen vor dem &NL-Zeichen angegeben werden. Wird das &NL-Zeichen nicht angegeben und hat die Befehlszeile mehr als 240 Zeichen, wird die Zeile in mehrere Zeilen geteilt und es werden Fortsetzungszeichen (+) hinzugefügt.

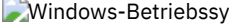
## CMDFilename

  Gibt den vollständig qualifizierten Namen der Datei an, die die durch den Parameter CMD angegebenen Befehle enthält. Dieser Parameter ist wahlfrei.

Wird kein Dateiname angegeben oder wird eine Nullzeichenfolge ("" ) angegeben, verwendet DRM den mit dem Befehl SET DRMCMDFILENAME angegebenen Dateinamen. Wird kein Dateiname mit dem Befehl SET DRMCMDFILENAME angegeben, generiert DRM einen Dateinamen, indem `exec.cmds` an den Namen des Verzeichnispfads des aktuellen Arbeitsverzeichnisses des Servers angehängt wird.

Schlägt die Operation fehl, nachdem die Befehlsdatei erstellt wurde, wird die Datei nicht gelöscht.

## CMDFilename

 Gibt den vollständig qualifizierten Namen der Datei an, die die durch den Parameter CMD angegebenen Befehle enthält. Dieser Parameter ist wahlfrei.

Die maximale Länge des Dateinamens beträgt 259 Zeichen. Wird kein Dateiname angegeben oder wird eine Nullzeichenfolge ("" ) angegeben, verwendet DRM den mit dem Befehl SET DRMCMDFILENAME angegebenen Dateinamen. Wird kein Dateiname mit dem Befehl SET DRMCMDFILENAME angegeben, generiert DRM einen Dateinamen, indem `exec.cmd` an das Verzeichnis angehängt wird, das diese Instanz des Servers darstellt (normalerweise das Verzeichnis, aus dem der Server installiert wurde). DRM ordnet den angegebenen oder generierten Dateinamen zu. Ist der Dateiname vorhanden, versucht DRM, den Namen zu verwenden; alle vorhandenen Daten werden überschrieben. Wenn dies eintritt und die ausführbaren Befehle in der Datei noch nicht ausgeführt wurden, geben Sie den Befehl QUERY DRMEDIA aus, um die ausführbaren Befehle für das gewünschte Datum und den gewünschten Datenträgerübergang wiederherzustellen.

Schlägt der Befehl MOVE DRMEDIA fehl und werden keine Informationen der mit dem Parameter CMD angegebenen Befehlszeichenfolge für den erfolgreich versetzten Datenträger geschrieben, wird der zugeordnete Dateiname gelöscht.

## APPend

Gibt an, ob der vorhandene Inhalt der Befehlsdatei überschrieben werden soll oder ob die Befehle an die Datei angehängt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Geben Sie einen der folgenden Werte an:

No

DRM überschreibt den Inhalt der Datei.

Yes

DRM hängt die Befehle an die Datei an.

Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Geben Sie einen der folgenden Werte an:

No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet.

Nachrichten, die von dem Hintergrundprozess erstellt werden, werden entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Um zu prüfen, ob die Operation erfolgreich war, den Befehl QUERY ACTLOG ausgeben.

Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Erst nachdem der Befehl vollständig ausgeführt wurde, kann mit anderen Aufgaben fortgefahren werden. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an. Einschränkung: Sie können nicht WAIT=YES an der Serverkonsole angeben.

CAP

Gibt an, welcher Cartridge Access Port (CAP) für die Ausgabe von Datenträgern verwendet werden soll, wenn REMOVE=YES angegeben wird. Dieser Parameter gilt nur für Datenträger in ACSLS-Kassettenarchiven. Wenn der CAP-Prioritätswert in dem Kassettenarchiv auf 0 gesetzt wird, ist dieser Parameter erforderlich. Ist ein CAP-Prioritätswert größer als Null in dem Kassettenarchiv definiert, ist dieser Parameter optional. Standardmäßig haben alle CAPs anfänglich den Prioritätswert 0, der bedeutet, dass ACSLS nicht automatisch den Kassettenzugriffsport auswählt. Zum Anzeigen der gültigen CAP-Kennungen (x,y,z) geben Sie den Befehl QUERY CAP mit der Option ALL von der ACSSA-Konsole (ACSSA = Automated Cartridge System System Administrator) auf dem ACSLS-Server-Host aus. Die Kennungen sind:

x

Die ACS-ID (ACS = Automated Cartridge System). Diese Kennung kann eine Zahl im Bereich von 0 bis 126 sein.

y

Die LSM-ID (LSM = Library Storage Module). Diese Kennung kann eine Zahl im Bereich von 0 bis 23 sein.

z

Die CAP-ID. Diese Kennung kann eine Zahl im Bereich von 0 bis 11 sein.

Weitere Informationen enthält die StorageTek-Dokumentation.

## Regeln für Zielstatus und Zielstandorte

Die folgende Tabelle zeigt, wie DRM den Zielstatus und Zielstandort eines Datenträgers bestimmt.

Zielstatus

- Der Wert des Parameters TOSTATE, der angegeben wurde
- Der nächste Status des Parameters WHERESTATE, der angegeben wurde, wenn der Parameter TOSTATE nicht angegeben wurde

Zielstandort

- Der Wert des Parameters TOLOCATION, der angegeben wurde
- Der Standort des Parameters TOSTATE, der angegeben wurde, wenn der Parameter TOLOCATION nicht angegeben wurde
- Der Standort des nächsten Status des Parameters WHERESTATE, der angegeben wurde, wenn die Parameter TOLOCATION und TOSTATE nicht angegeben werden

Tabelle 2. Datenträgerzielstatus und -zielstandort

| Angegebene Parameter            | Zielstatus                        | Zielstandort                 |
|---------------------------------|-----------------------------------|------------------------------|
| WHERESTATE                      | Der nächste Status von WHERESTATE | Standort des nächsten Status |
| WHERESTATE, TOSTATE             | TOSTATE                           | Standort von TOSTATE         |
| WHERESTATE, TOLOCATION          | Der nächste Status von WHERESTATE | TOLOCATON                    |
| WHERESTATE, TOSTATE, TOLOCATION | TOSTATE                           | TOLOCATION                   |
| TOSTATE                         | TOSTATE                           | Standort von TOSTATE         |
| TOSTATE, WHERELOCATION          | TOSTATE                           | Standort von TOSTATE         |

| Angegebene Parameter               | Zielstatus | Zielstandort |
|------------------------------------|------------|--------------|
| TOSTATE, WHERELOCATION, TOLOCATION | TOSTATE    | TOLOCATION   |

## Regeln für Statusübergang

Die folgenden Tabellen zeigen die Statusübergänge, für die Datenträger auf der Basis ihres aktuellen Status ausgewählt werden können.

Tabelle 3. Statusübergänge für Datenträger

| Der aktuelle Status des Datenträgers | Zielstatus |              |         |
|--------------------------------------|------------|--------------|---------|
|                                      | MOUNTABLE  | NOTMOUNTABLE | COURIER |
| MOUNTABLE                            | N          | J            | J       |
| NOTMOUNTABLE                         | N          | N            | J       |
| COURIER                              | N          | N            | N       |
| VAULT                                | N          | N            | N       |
| VAULTRETRIEVE                        | N          | N            | N       |
| COURIERRETRIEVE                      | N          | N            | N       |
| ONSITERETRIEVE                       | N          | N            | N       |

Tabelle 4. Statusübergänge für Datenträger

| Der aktuelle Status des Datenträgers | Zielstatus |               |
|--------------------------------------|------------|---------------|
|                                      | VAULT      | VAULTRETRIEVE |
| MOUNTABLE                            | J          | N             |
| NOTMOUNTABLE                         | J          | N             |
| COURIER                              | J          | N             |
| VAULT                                | N          | N             |
| VAULTRETRIEVE                        | N          | N             |
| COURIERRETRIEVE                      | N          | N             |
| ONSITERETRIEVE                       | N          | N             |

Tabelle 5. Statusübergänge für Datenträger

| Der aktuelle Status des Datenträgers | Zielstatus      |                |
|--------------------------------------|-----------------|----------------|
|                                      | COURIERRETRIEVE | ONSITERETRIEVE |
| MOUNTABLE                            | N               | N              |
| NOTMOUNTABLE                         | N               | N              |
| COURIER                              | N               | N              |
| VAULT                                | N               | N              |
| VAULTRETRIEVE                        | J               | J              |
| COURIERRETRIEVE                      | N               | J              |
| ONSITERETRIEVE                       | N               | N              |

## Beispiel: Datenträger zur Wiederherstellung nach einem Katastrophenfall aus dem Status NOTMOUNTABLE versetzen

Datenträger zur Wiederherstellung nach einem Katastrophenfall, die sich im Status NOTMOUNTABLE befinden, in den Status COURIER versetzen und dann die Ergebnisse abfragen.

```
move drmedia * wherestate=notmountable
tostate=courier
```

```
query actlog search="MOVE DRMEDIA"
```

```
08/11/1999 11:12:24 ANR0984I Prozess 10 für MOVE DRMEDIA
im BACKGROUND um 11:12:24 gestartet.
```

```

08/11/1999 11:12:24      ANR0610I MOVE DRMEDIA von HSIAO als
                          Prozess 10 gestartet.
08/11/1999 11:12:25      ANR6683I MOVE DRMEDIA: Datenträger TAPE0P
                          wurde von Status NOTMOUNTABLE in Status
                          COURIER versetzt.
08/11/1999 11:12:25      ANR6683I MOVE DRMEDIA: Datenträger TAPE1P
                          wurde von Status NOTMOUNTABLE in Status
                          COURIER versetzt.
08/11/1999 11:12:25      ANR6683I MOVE DRMEDIA: Datenträger DBTP02
                          wurde von Status NOTMOUNTABLE in Status
                          COURIER versetzt.
08/11/1999 11:12:25      ANR6683I MOVE DRMEDIA: Datenträger DBTP01
                          wurde von Status NOTMOUNTABLE in Status
                          COURIER versetzt.
08/11/1999 11:12:25      ANR6682I Befehl MOVE DRMEDIA beendet: 4
                          verarbeitet.
08/11/1999 11:12:25      ANR0611I MOVE DRMEDIA, der von HSIAO als
                          Prozess 10 gestartet wurde, wurde beendet.
08/11/1999 11:12:25      ANR0985I Prozess 10 für MOVE DRMEDIA, der
                          im BACKGROUND ausgeführt wird, hat 4 Objekte
                          mit Beendigungsstatus SUCCESS um
                          11:12:25 beendet.

```

## Beispiel: Datenträger zur Wiederherstellung nach einem Katastrophenfall aus dem Status MOUNTABLE versetzen

---

Datenträger zur Wiederherstellung nach einem Katastrophenfall vom Status MOUNTABLE in den Status COURIER versetzen. Befinden sich die Datenträger in einem automatisierten Kassettenarchiv, gibt MOVE DRMEDIA die Datenträger aus, bevor der Status geändert wird.

```
move drmedia * wherestate=mountable tostate=courier wait=yes
```

```

ANR0984I Prozess 12 für MOVE DRMEDIA
  im FOREGROUND um 09:57:17 gestartet.
ANR0609I MOVE DRMEDIA als Prozess 12 gestartet.
ANR0610I MOVE DRMEDIA von HSIAO als
  Prozess 12 gestartet.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger TAPE01 in Kassettenarchiv LIB8MM wird gestartet.
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger TAPE01 in Kassettenarchiv LIB8MM
  erfolgreich beendet.
ANR6683I MOVE DRMEDIA: Datenträger TAPE01 wurde von
  Status MOUNTABLE in Status COURIER versetzt.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger TAPE02 in Kassettenarchiv LIB8MM wird gestartet.
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger TAPE02 in Kassettenarchiv LIB8MM
  erfolgreich beendet.
ANR6683I MOVE DRMEDIA: Datenträger TAPE02 wurde von
  Status MOUNTABLE in Status COURIER versetzt.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger DBTP05 in Kassettenarchiv LIB8MM wird gestartet.
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger DBTP05 in Kassettenarchiv LIB8MM
  erfolgreich beendet.
ANR6683I MOVE DRMEDIA: Datenträger DBTP05 wurde von
  Status MOUNTABLE in Status COURIER versetzt.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger DBTP04 in Kassettenarchiv LIB8MM wird gestartet.
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger DBTP04 in Kassettenarchiv LIB8MM
  erfolgreich beendet.
ANR6683I MOVE DRMEDIA: Datenträger DBTP04 wurde von
  Status MOUNTABLE in Status COURIER versetzt.
ANR6682I Befehl MOVE DRMEDIA beendet: 4 Datenträger
  verarbeitet.
ANR0611I MOVE DRMEDIA, der von HSIAO als
  Prozess 12 gestartet wurde, wurde beendet.
ANR0985I Prozess 12 für MOVE DRMEDIA, der im
  FOREGROUND ausgeführt wird, hat 4 Objekte mit
  Beendigungsstatus SUCCESS um 10:12:25 beendet.

```

## Beispiel: Datenträger zur Wiederherstellung nach einem Katastrophenfall aus dem Status VAULTRETRIEVE versetzen

---

Datenträger zur Wiederherstellung nach einem Katastrophenfall, die sich im Status VAULTRETRIEVE befinden, sollen in den Status ONSITERETRIEVE versetzt werden. Einen Befehl CHECKIN LIBVOLUME für jeden Datenträger generieren, der erfolgreich verarbeitet wird, und die Befehle in einer Datei speichern:

#### AIX-Betriebssysteme Linux-Betriebssysteme

```
move drmedia * wherestate=vaultretrieve tostate=onsiteretrieve
cmdfilename=/drm/move/exec.cmds
cmd="checkin libvol lib8mm &vol status=scratch"
```

#### Windows-Betriebssysteme



```
move drmedia * wherestate=vaultretrieve tostate=onsiteretrieve
cmdfilename=c:\drm\move\exec.cmd
cmd="checkin libvol lib8mm &vol status=scratch"
```

Die Ergebnisse abfragen:

```
query actlog search="MOVE DRMEDIA"

08/13/1999 09:12:24 ANR0984I Prozess 15 für MOVE DRMEDIA
                   im BACKGROUND um 09:12:24 gestartet
08/13/1999 09:12:24 ANR0610I MOVE DRMEDIA von HSIAO als Prozess
                   15 gestartet.
08/13/1999 09:12:24 ANR6684I MOVE DRMEDIA: Datenträger CSTP01
                   wurde gelöscht.
08/13/1999 09:12:24 ANR6684I MOVE DRMEDIA: Datenträger CSTP02
                   wurde gelöscht.
08/13/1999 09:12:24 ANR6684I MOVE DRMEDIA: Datenträger DBTP10
                   wurde gelöscht.
08/13/1999 09:12:24 ANR6684I MOVE DRMEDIA: Datenträger DBTP11
                   wurde gelöscht.
08/13/1999 09:12:27 ANR6682I Befehl MOVE DRMEDIA beendet: 4 Datenträger
                   verarbeitet.
08/13/1999 09:12:42 ANR0611I MOVE DRMEDIA, der von HSIAO als Prozess
                   15 gestartet wurde, wurde beendet.
08/13/1997 09:12:42 ANR0985I Prozess 15 für MOVE DRMEDIA, der im
                   im BACKGROUND ausgeführt wird, hat 4 Objekte
                   Beendigungsstatus SUCCESS um 09:12:42 beendet.
```

Die Befehle zum Zurückstellen der Datenträger wurden ebenfalls in der Datei erstellt, die mit dem Parameter CMDFILENAME angegeben wurde:

-  AIX-Betriebssysteme  Linux-Betriebssysteme/drm/move/exec.cmds
-  Windows-Betriebssystemec:\drm\move\exec.cmd

Die Datei enthält diese Zeilen:

```
checkin libvol lib8mm CSTP01 status=scratch
checkin libvol lib8mm CSTP02 status=scratch
checkin libvol lib8mm DBTP10 status=scratch
checkin libvol lib8mm DBTP11 status=scratch
```



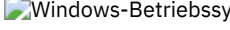


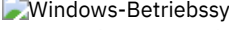
Tipp: Um die Befehle CHECKIN LIBVOLUME zu verarbeiten, geben Sie den Befehl MACRO mit dem Dateinamen als Makronamen aus.

## Zugehörige Befehle

Tabelle 6. Zugehörige Befehle für MOVE DRMEDIA

| Befehl             | Beschreibung   |
|--------------------|--|
| BACKUP DB          | Sichert die IBM Spectrum Protect-Datenbank auf Datenträgern mit sequenziellem Zugriff. |
| BACKUP STGPOOL     | Sichert einen primären Speicherpool in einem Kopierspeicherpool.                       |
| CANCEL PROCESS     | Bricht einen Serverhintergrundprozess ab.  |
| CHECKOUT LIBVOLUME | Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.             |
| DISMOUNT VOLUME    | Entlädt einen sequenziellen entfernbaren Datenträger anhand des Datenträgernamens.     |
| PREPARE            | Erstellt eine Wiederherstellungsplandatei.   |



| Befehl   | Beschreibung   |
|--|--|
| QUERY ACTLOG   | Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.   |
| QUERY DRMEDIA  | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.  |
| QUERY DRMSTATUS  | Zeigt DRM-Systemparameter an.  |
| QUERY PROCESS  | Zeigt Informationen über Hintergrundprozesse an.   |
| SET DRMACTIVEDATASTGPOOL   | Gibt an, dass Speicherpools für aktive Daten von DRM verwaltet werden.   |
|  <br> SET DRMCOPYCONTAINERSTGPOOL |  <br> Gibt die Containerkopierspeicherpools an, die in DRM-Befehlen verwendet werden. |
| SET DRMCOPYSTGPOOL   | Gibt an, dass Kopierspeicherpools von DRM verwaltet werden.  |
| SET DRMCOURIERNAME   | Gibt den Kuriernamen für DRM an.   |
| SET DRMDBBACKUPEXPIREDAYS  | Gibt die Kriterien für den Verfall von Datenbanksicherungsserien an.   |
| SET DRMVaultNAME   | Gibt den Namen des Aufbewahrungsorts an, an dem DRM-Datenträger gespeichert werden.  |
| SET DRMCMDFILENAME   | Gibt den Namen einer Datei an, in die ausführbare DRM-Befehle gestellt werden sollen.  |
| SET DRMFILEPROCESS   | Gibt an, ob der Befehl MOVE DRMEDIA oder QUERY DRMEDIA Dateien verarbeitet, die den Einheitentyp FILE aufweisen.   |
| SET DRMNOTMOUNTABLENAME  | Gibt den Standortnamen der DRM-Datenträger an, die ausgelagert werden sollen.  |

## MOVE GRPMEMBER (Servergruppenteil versetzen)

Mit diesem Befehl kann ein Teil aus einer Servergruppe in eine andere Servergruppe versetzt werden. Der Befehl schlägt fehl, wenn das Teil, das versetzt wird, denselben Namen wie ein aktuelles Teil der Gruppe hat.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-MOVE GRPMEMber--Name_des_Teils--aus_Gruppe--in_Gruppe-----<<
```

### Parameter

Name\_des\_Teils (Erforderlich)  
Gibt das Teil an (Server oder Servergruppe), das versetzt werden soll.

aus\_Gruppe (Erforderlich)  
Gibt die Servergruppe an, der das Teil gegenwärtig zugeordnet ist.

in\_Gruppe (Erforderlich)  
Gibt die neue Servergruppe des Teils an.

### Beispiel: Einen Server in eine andere Servergruppe versetzen

Teil PAYSON aus Gruppe REGION1 in Gruppe REGION2 versetzen.

```
move grpmember payson region1 region2
```

### Zugehörige Befehle



```

'-EMPTy---'
>----->
'-ACCess---+READWrite+-' '-OVFLocation---Standort-'
'-READOnly--'

.-REMOve---Bulk----.
>----->
'-REMOve---+No---+' '-CMd---"Befehl"-'
'+Yes--+
'-Bulk-'

.-APPend---No-----.
>----->
'-CMDFilename---Dateiname-' '-APPend---+No---+'
'-Yes-'

.-CHECKLabel---Yes-----.
>-----><
'-CHECKLabel---+Yes---+' '-CAP---x,y,z---'
'-No--'

```

## Parameter

### Datenträgername (Erforderlich)

Gibt den Namen des zu verarbeitenden Datenträgers mit sequenziellem Zugriff aus einem primären Speicherpool oder einem Kopierspeicherpool an. Es kann ein Platzhalterzeichen verwendet werden, um den Namen anzugeben. Alle übereinstimmenden Datenträger werden bei der Verarbeitung berücksichtigt.

### STGpool (Erforderlich)

Gibt den Namen des primären Speicherpools oder Kopierspeicherpools mit sequenziellem Zugriff an, aus dem die Datenträger für die Verarbeitung ausgewählt werden. Es kann ein Platzhalterzeichen verwendet werden, um den Namen anzugeben. Alle übereinstimmenden Speicherpools werden verarbeitet. Wird der angegebene Speicherpool nicht durch ein automatisiertes Kassettenarchiv verwaltet, werden keine Datenträger verarbeitet.

### Days

Gibt die Anzahl Tage an, die nach dem Schreiben oder Lesen des Datenträgers verstreichen müssen, bevor der Datenträger durch den Befehl verarbeitet werden kann. Dieser Parameter ist wahlfrei. Es kann eine Zahl von 0 bis 9999 angegeben werden. Der Standardwert ist 0. Die Anzahl der verstrichenen Tage wird anhand des letzten Lese- oder Schreibdatums (das aktuellere von beiden) der Datenträger berechnet.

### WHEREState

Gibt den aktuellen Status der zu verarbeitenden Datenträger an. Mit diesem Parameter wird die Verarbeitung auf die Datenträger beschränkt, die den angegebenen Status haben. Dieser Parameter ist wahlfrei. Der Standardwert ist MOUNTABLEINLIB. Gültige Werte:

#### MOUNTABLEInlib

Gibt an, dass Speicherpooldatenträger vom Status MOUNTABLEINLIB in den Status MOUNTABLENOTINLIB versetzt werden sollen. Datenträger mit dem Status MOUNTABLEINLIB enthalten gültige Daten und befinden sich im Kassettenarchiv.

#### MOUNTABLENotinlib

Gibt an, dass Speicherpooldatenträger vom Status MOUNTABLENOTINLIB wieder in den Status MOUNTABLEINLIB übergehen sollen. Datenträger mit dem Status MOUNTABLENOTINLIB können gültige Daten enthalten und befinden sich am Überlaufstandort.

- Bei leeren Arbeitsdatenträgern löscht der Befehl MOVE MEDIA die Datenträgersätze, so dass sie wiederverwendet werden können.
- Bei privaten Datenträgern setzt der Befehl MOVE MEDIA den Datenträgerstandort auf leer (blank) zurück, ändert den Datenträgerstatus in CHECKIN und das letzte Aktualisierungsdatum in das aktuelle Datum.
- Bei Arbeitsdatenträgern mit Daten setzt der Befehl MOVE MEDIA den Datenträgerstandort auf leer (blank) zurück, ändert den Datenträgerstatus in CHECKIN und das letzte Aktualisierungsdatum in das aktuelle Datum.

Achtung: Datenträger mit dem Status CHECKIN können gültige Daten enthalten und müssen in das Kassettenarchiv zurückgestellt werden.

### WHERESTATUS

Gibt an, dass der Versetzungsprozess auf einen bestimmten Datenträgerstatus beschränkt werden muss. Dieser Parameter ist wahlfrei. Es können mehrere Status in einer Liste angegeben werden, indem jeder Status ohne Leerzeichen durch ein Komma voneinander getrennt wird. Wird dieser Parameter nicht angegeben, sind Datenträger, die vom Status MOUNTABLEINLIB in den Status MOUNTABLENOTINLIB versetzt werden, nur auf volle Datenträger beschränkt, und sind Datenträger, die vom Status MOUNTABLENOTINLIB in den Status MOUNTABLEINLIB versetzt werden, nur auf leere Datenträger beschränkt.

Gültige Werte:

FULL

Datenträger mit dem Status FULL werden versetzt.

FILLing

Datenträger mit dem Status FILLING werden versetzt.

EMPTy

Datenträger mit dem Status EMPTY werden versetzt.

#### ACCess

Gibt an, wie Benutzer und Systemprozesse auf Dateien auf dem Speicherpoolatenträger zugreifen, der durch den Befehl MOVE MEDIA aus einem automatisierten Kassettenarchiv versetzt und an einem Überlaufstandort gespeichert wird. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, wird der Zugriffsmodus der Datenträger durch das Versetzen von Datenträgern vom Status MOUNTABLEINLIB in den Status MOUNTABLENOTINLIB in READONLY geändert und durch das Versetzen von Datenträgern vom Status MOUNTABLENOTINLIB in den Status MOUNTABLEINLIB in READWRITE.

Gültige Werte:

READWrite

Gibt an, dass Benutzer und Systemprozesse Dateien auf dem Datenträger, der sich am Überlaufstandort befindet, lesen und in diese schreiben können. Wenn dieser Wert angegeben wird, fordert IBM Spectrum Protect das Zurückstellen des Datenträgers in das Kassettenarchiv an, wenn er für eine Lese- oder Schreiboperation benötigt wird.

READOnly

Gibt an, dass Benutzer und Systemprozesse Dateien auf dem Datenträger, der sich am Überlaufstandort befindet, lesen, aber nicht in diese schreiben können. Der Server fordert das Zurückstellen des Datenträgers in das Kassettenarchiv nur an, wenn er für eine Leseoperation benötigt wird.

#### OVFLocation

Gibt den Überlaufstandort an, der der Zielort für die Datenträger ist, die gerade verarbeitet werden. Der Standortname darf maximal 255 Zeichen lang sein. Wenn der Standortname Leerzeichen enthält, muss er in Anführungszeichen stehen. Wird kein Überlaufstandort angegeben und hat auch der Speicherpool keinen Überlaufstandort identifiziert, ändert der Server den Standort des ausgegebenen Datenträgers in eine leere Zeichenfolge ("").

#### REMOve

Gibt an, dass der Server versucht, den Datenträger aus dem Kassettenarchiv in die Serviceein-/ausgabestation oder die Eingangs-/Ausgangsanschlüsse zu versetzen. Dieser Parameter ist wahlfrei. Gültige Werte sind YES, BULK und NO. Der Standardwert ist BULK. Die Antwort des Servers auf jede dieser Optionen und die Standardwerte werden in den folgenden Tabellen beschrieben.

**349X-Kassettenarchive:** Die folgende Tabelle zeigt, wie der Server für 349X-Kassettenarchive antwortet.

Tabelle 1. Antwort des Servers für 349X-Kassettenarchive

| REMOVE=YES   | REMOVE=BULK  | REMOVE=NO  |
|--|--|--|
| Der 3494-Kassettenarchivmanager (Library Manager) gibt die Kassette an die Serviceein-/ausgabestation aus. | Der 3494-Kassettenarchivmanager (Library Manager) gibt die Kassette an die Ausgabeeinrichtung mit hoher Speicherkapazität aus. | Der 3494-Kassettenarchivmanager (Library Manager) gibt den Datenträger nicht aus.<br><br>Der Server lässt die Kassette für die Verwendung durch andere Anwendungen in dem Kassettenarchiv in der Kategorie INSERT. |

**SCSI-Kassettenarchive:** Die folgende Tabelle zeigt, wie der Server für SCSI-Kassettenarchive auf YES, BULK und NO antwortet.

Tabelle 2. Antwort des Servers für SCSI-Kassettenarchive

| Wenn ein Kassettenarchiv... | Und REMOVE=YES... | Und REMOVE=BULK... | Und REMOVE=NO |
|-----------------------------|-------------------|--------------------|---------------|
|-----------------------------|-------------------|--------------------|---------------|

| Wenn ein Kassettenarchiv...  | Und REMOVE=YES...   | Und REMOVE=BULK...  | Und REMOVE=NO   |
|--|---|---|---|
| Keine Eingangs-/Ausgangsanschlüsse hat   | Lässt der Server die Kasette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden dann vom Server aufgefordert, die Kasette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben.     | Lässt der Server die Kasette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kasette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.     | Lässt der Server die Kasette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kasette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. |
| Eingangs-/Ausgangsanschlüsse hat und ein Eingangs-/Ausgangsanschluss verfügbar ist | Versetzt der Server die Kasette in den verfügbaren Eingangs-/Ausgangsanschluss und gibt die Anschlussadresse in einer Nachricht an.<br><br>Sie werden dann vom Server aufgefordert, die Kasette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben. | Versetzt der Server die Kasette in den verfügbaren Eingangs-/Ausgangsanschluss und gibt die Anschlussadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kasette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. | Lässt der Server die Kasette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kasette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. |
| Eingangs-/Ausgangsanschlüsse hat, aber keine Anschlüsse verfügbar sind             | Lässt der Server die Kasette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden dann vom Server aufgefordert, die Kasette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben.     | Wartet der Server auf einen verfügbaren Eingangs-/Ausgangsanschluss.  | Lässt der Server die Kasette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an.<br><br>Sie werden nicht vom Server aufgefordert, die Kasette zu entnehmen, und müssen keinen Befehl REPLY ausgeben. |

**ACSLs-Kassettenarchive:** Die folgende Tabelle zeigt, wie der Server für ACSLS-Kassettenarchive antwortet.

Tabelle 3. Antwort des Servers für ACSLS-Kassettenarchive



| REMOVE=YES oder REMOVE=BULK  | REMOVE=NO   |
|--|---|
| Der Server gibt die Kasette an die Serviceein-/ausgabestation aus.<br><br>Dann löscht der Server den Datenträgereintrag aus dem Serverdatenträgerbestand im Kassettenarchiv.<br><br>Beim Versetzen von Datenträgern aus dem Status MOUNTABLE unter Angabe von REMOVE=YES verwendet der Befehl MOVE MEDIA mehrere Schächte in dem CAP für ein StorageTek-Kassettenarchiv mit ACSLS. | Der Server gibt die Kasette nicht aus.<br><br>Der Server löscht den Datenträgereintrag aus dem Kassettenarchivbestand des Servers und lässt den Datenträger in dem Kassettenarchiv. |

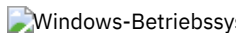
**Externe Kassettenarchive:** Die folgende Tabelle zeigt, wie der Server für externe Kassettenarchive antwortet.

Tabelle 4. Antwort des Servers für externe Kassettenarchive

| REMOVE=YES oder REMOVE=BULK   | REMOVE=NO   |
|---|---|
| Der Server gibt die Kasette an die Serviceein-/ausgabestation aus. Dann löscht der Server den Datenträgereintrag aus dem Serverdatenträgerbestand im Kassettenarchiv. | Der Server gibt die Kasette nicht aus.<br><br>Der Server löscht den Datenträgereintrag aus dem Kassettenarchivbestand des Servers und lässt den Datenträger in dem Kassettenarchiv. |

Gibt an, dass ausführbare Befehle erstellt werden. Dieser Parameter ist wahlfrei. Die Befehlsangabe muss in Anführungszeichen eingeschlossen werden. Die maximale Länge der Befehlsangabe beträgt 255 Zeichen. Für jeden Datenträger, den der Befehl MOVE MEDIA erfolgreich verarbeitet hat, schreibt der Server die zugeordneten Befehle in eine Datei. Den Dateinamen mit dem Parameter CMDFILENAME angeben.

  Wird der Dateiname nicht angegeben, generiert der Befehl MOVE MEDIA einen Standarddateinamen, indem die Zeichenfolge `exec.cmds.media` an das IBM Spectrum Protect-Serververzeichnis angehängt wird.

 Wird der Dateiname nicht angegeben, generiert der Befehl MOVE MEDIA einen Standarddateinamen, indem die Zeichenfolge `exec.cmd.media` an das IBM Spectrum Protect-Serververzeichnis angehängt wird.

Wenn die Länge des Befehls, der in die Datei geschrieben wird, 255 Zeichen überschreitet, wird er in mehrere Zeilen aufgeteilt, wobei an das Ende jeder Zeile (mit Ausnahme der letzten Befehlszeile) ein Fortsetzungszeichen (+) eingefügt wird. Sie müssen das Fortsetzungszeichen entsprechend den Anforderungen des Produkts, das die Befehle ausführt, ändern.

Wird CMD nicht angegeben, generiert der Befehl MOVE MEDIA möglicherweise keine ausführbaren Befehle.

#### Zeichenfolge

Gibt die Zeichenfolge für die Erstellung eines ausführbaren Befehls an. Für die Zeichenfolge kann beliebiger Text im freien Format angegeben werden. Die gesamte Zeichenfolge muss in Anführungszeichen eingeschlossen werden. Das folgende Beispiel zeigt eine gültige Angabe eines ausführbaren Befehls:

```
CMD="UPDATE VOLUME &VOL"
```

Die folgende Angabe ist ungültig:

```
CMD=" "UPDATE VOLUME" &VOL"
```

#### Substitution

Gibt eine Variable an, für die der Befehl einen Wert ersetzen soll. Gültige Substitutionsvariablen:

##### &VOL

Den Datenträgernamen für &VOL ersetzen. Kleinbuchstaben können angegeben werden (&vol). Zwischen Et-Zeichen (&) und VOL dürfen keine Leerschritte oder Leerzeichen stehen. Befinden sich an dieser Stelle Leerzeichen, behandelt der Befehl MOVE MEDIA diese Zeichen als Zeichenfolge, und es wird keine Substitution definiert. Wird &VOL nicht angegeben, wird in dem ausführbaren Befehl kein Datenträgername definiert.

##### &LOC

Den Datenträgerstandort für &LOC ersetzen. Kleinbuchstaben können angegeben werden (&loc). Zwischen Et-Zeichen (&) und LOC dürfen keine Leerschritte oder Leerzeichen stehen. Befinden sich an dieser Stelle Leerzeichen, behandelt der Befehl MOVE MEDIA diese Zeichen als Zeichenfolge, und es wird keine Substitution definiert. Wird &LOC nicht angegeben, wird in dem ausführbaren Befehl kein Standortname definiert.

##### &VOLDSN



Den Datenträgerdateinamen für &VOLDSN ersetzen. Ein Beispiel für einen Dateinamen eines Banddatenträgers aus dem Speicherpool, der das Standardpräfix AD SM verwendet, ist AD SM.BFS. Wird &VOLDSN nicht angegeben, wird in dem ausführbaren Befehl kein Datenträgerdateiname definiert.


##### &NL

Ein Zeilenvorschubzeichen für &NL ersetzen. Wenn &NL angegeben wird, teilt der Befehl MOVE MEDIA den Befehl an der Position, an der sich &NL befindet; es werden keine Fortsetzungszeichen angehängt. Die Angabe des richtigen Fortsetzungszeichens (falls erforderlich) vor &NL ist Aufgabe des Benutzers. Der Benutzer ist außerdem verantwortlich für die Länge der Zeile. Wenn &NL nicht angegeben wird und die Länge der Befehlszeile 255 Zeichen überschreitet, wird sie in mehrere Zeilen aufgeteilt, wobei an das Ende jeder Zeile (mit Ausnahme der letzten Befehlszeile) ein Fortsetzungszeichen (+) eingefügt wird.

#### CMDFilename

Gibt den vollständigen Pfadnamen einer Datei an, die die mit CMD angegebenen Befehle enthält. Dieser Parameter ist wahlfrei. Die maximale Länge des Dateinamens beträgt 1279 Zeichen.

  Wird kein Dateiname angegeben, generiert der Befehl MOVE MEDIA einen Standarddateinamen, indem die Zeichenfolge `exec.cmds.media` an das IBM Spectrum Protect-Serververzeichnis angehängt wird. Das Serververzeichnis ist das aktuelle Arbeitsverzeichnis des IBM Spectrum Protect-Serverprozesses.

 Wird kein Dateiname angegeben, generiert der Befehl MOVE MEDIA einen Standarddateinamen, indem die Zeichenfolge `exec.cmd.media` an das IBM Spectrum Protect-Serververzeichnis angehängt wird. Das Serververzeichnis ist das aktuelle Arbeitsverzeichnis des IBM Spectrum Protect-Serverprozesses.

Der Befehl MOVE MEDIA ordnet den angegebenen oder generierten Dateinamen automatisch zu. Ist der Dateiname vorhanden, kann mit dem Parameter APPEND=YES an die Datei angefügt werden. Andernfalls wird die Datei überschrieben. Wird eine Datei versehentlich überschrieben und müssen die Befehle, die in der Datei enthalten waren, ausgeführt werden, geben Sie den Befehl

QUERY MEDIA aus, um die ausführbaren Befehle für die gewünschten Datenträger wiederherzustellen. Wenn der Befehl MOVE MEDIA nach der Zuordnung der Befehlsdatei fehlschlägt, wird die Datei nicht gelöscht.

#### APPend

Gibt an, dass am Anfang oder Ende der Befehlsdateidaten geschrieben werden soll. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, dass die Daten an den Anfang der Befehlsdatei geschrieben werden sollen. Wenn die Befehlsdatei vorhanden ist, wird ihr Inhalt überschrieben.

Yes

Gibt an, dass die Befehlsdatei angehängt werden soll, indem am Ende der Befehlsdateidaten geschrieben wird.

#### CHECKLabel

Gibt an, ob der Server Datenträgerkennsätze für sequenzielle Datenträger liest. Bei SCSI-Einheiten kann die Kennsatzprüfung unterdrückt werden, indem CHECKLabel auf NO gesetzt wird. Dieser Parameter gilt nicht für 349X-Kassettenarchive. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Gültige Werte:

Yes

Gibt an, dass der Server versucht, den Datenträgerkennsatz zu lesen. Das Lesen des Datenträgerkennsatzes bestätigt, dass der richtige Datenträger entnommen wird.

No

Gibt an, dass der Server nicht versucht, den Datenträgerkennsatz zu lesen. Da der Lesevorgang entfällt, verbessert sich die Leistung.

#### CAP

Gibt an, welcher Cartridge Access Port (CAP) für die Ausgabe von Datenträgern verwendet werden soll, wenn REMOVE=YES angegeben wird. Dieser Parameter gilt nur für Datenträger in ACSLS-Kassettenarchiven. Wenn der CAP-Prioritätswert in dem Kassettenarchiv auf 0 gesetzt wird, ist dieser Parameter erforderlich. Ist ein CAP-Prioritätswert größer als Null in dem Kassettenarchiv definiert, ist dieser Parameter optional. Standardmäßig haben alle CAPs anfänglich den Prioritätswert 0, der bedeutet, dass ACSLS nicht automatisch den Kassettenzugriffsport auswählt. Zum Anzeigen der gültigen CAP-Kennungen (x,y,z) geben Sie den Befehl QUERY CAP mit der Option ALL von der ACSSA-Konsole (ACSSA = Automated Cartridge System System Administrator) auf dem ACSLS-Server-Host aus. Die Kennungen sind:

x

Die ACS-ID (ACS = Automated Cartridge System). Diese Kennung kann eine Zahl im Bereich von 0 bis 126 sein.

y

Die LSM-ID (LSM = Library Storage Module). Diese Kennung kann eine Zahl im Bereich von 0 bis 23 sein.

z

Die CAP-ID. Diese Kennung kann eine Zahl im Bereich von 0 bis 11 sein.

Weitere Informationen enthält die StorageTek-Dokumentation.

## Beispiel: Alle vollen Datenträger aus dem Kassettenarchiv versetzen


Alle vollen Datenträger, die sich im sequenziellen primären Speicherpool ARCHIVE befinden, aus dem Kassettenarchiv versetzen.

```
move media * stgpool=archive
```

## Beispiel: Die Befehle zum Zurückstellen generieren

Die Befehle CHECKIN LIBVOLUME für volle und teilweise volle Datenträger generieren, die sich im primären Speicherpool ONSITE.ARCHIVE befinden und im Überlaufstandort Room 2948/Bldg31 aufbewahrt werden.




  MOVE MEDIA erstellt die ausführbaren Befehle in /tsm/move/media/checkin.vols.

 MOVE MEDIA erstellt die ausführbaren Befehle in c:\tsm\move\media\checkin.vols.

```
move media * stgpool=onsite.archive
wherestate=mountablenotinlib wherestatus=full,filling
ovflocation=room2948/bldg31
cmd="checkin libvol lib3494 &vol status=private"
cmdfilename=/tsm/move/media/checkin.vols
```

```
checkin libvolume lib3494 TAPE04 status=private
checkin libvolume lib3494 TAPE13 status=private
checkin libvolume lib3494 TAPE14 status=private
```

Tipp: Führen Sie die Befehle CHECKIN LIBVOLUME aus, indem Sie den Befehl MACRO mit dem folgenden Wert als Makronamen ausgeben:

-  AIX-Betriebssysteme  Linux-Betriebssysteme/tsm/move/media/checkin.vols
-  Windows-Betriebssystemec:\tsm\move\media\checkin.vols

## Zugehörige Befehle

Tabelle 5. Zugehörige Befehle für MOVE MEDIA

| Befehl         | Beschreibung  |
|----------------|---|
| CANCEL PROCESS | Bricht einen Serverhintergrundprozess ab.   |
| QUERY MEDIA    | Zeigt Informationen über Speicherpooldatenträger an, die mit dem Befehl MOVE MEDIA versetzt wurden. |
| QUERY PROCESS  | Zeigt Informationen über Hintergrundprozesse an.  |

## MOVE NODEDATA (Daten nach Knoten in einem Speicherpool mit sequenziellem Zugriff versetzen)

Verwenden Sie diesen Befehl, um Daten zu versetzen, die sich in einem Speicherpool mit sequenziellem Zugriff befinden. Sie können Daten für einen oder mehrere Knoten, eine Gruppe von Dateibereichen oder eine Gruppe von zusammengefassten Knoten versetzen. Sie können auch ausgewählte Dateibereiche für einen einzelnen Knoten versetzen. Die Daten können sich in einem primären Speicherpool, einem Kopierspeicherpool oder einem Pool für aktive Daten befinden.

Mit diesem Befehl kann die Anzahl der Datenträgerladevorgänge bei Zurückschreibungs- oder Abrufoperationen des Clients reduziert werden, indem Daten für einen bestimmten Knoten innerhalb eines Speicherpools zusammengefasst werden. Außerdem können Daten in einen anderen Speicherpool versetzt werden. Beispielsweise kann der Befehl zum Versetzen von Daten in einen Speicherpool mit wahlfreiem Zugriff als Vorbereitung für eine Client-Zurückschreibungsverarbeitung verwendet werden.

Stellen Sie sicher, dass der Zugriffsmodus der Datenträger, von denen die Knotendaten versetzt werden, "Lesen/Schreiben" oder "Lesezugriff" lautet, und der Zugriffsmodus der Datenträger, auf die die Knotendaten versetzt werden, auf "Lesen/Schreiben" gesetzt ist. Diese Operation versetzt keine Daten auf Datenträgern mit den Zugriffsmodi "Ausgelagert", "Nicht verfügbar" oder "Zerstört".

Der Befehl MOVE NODEDATA hat zwei Formen, je nachdem, ob Daten nur für ausgewählte Dateibereiche versetzt werden. Syntax und Parameter der jeweiligen Form werden separat definiert.

Einschränkung: Sie können keine Knotendaten in einen Speicherpool oder aus einem Speicherpool versetzen, der mit einer Einheitenklasse CENTERA definiert ist.

Tabelle 1. Zugehörige Befehle für MOVE NODEDATA

| Befehl              | Beschreibung   |
|---------------------|--|
| CANCEL PROCESS      | Bricht einen Serverhintergrundprozess ab.  |
| COPY ACTIVATEDATA   | Kopiert aktive Sicherungsdaten.  |
| DEFINE COLLOGROUP   | Definiert eine Kollokationsgruppe.   |
| DEFINE COLLOCMEMBER | Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.                              |
| DELETE COLLOGROUP   | Löscht eine Kollokationsgruppe.  |
| DELETE COLLOCMEMBER | Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.                              |
| MOVE DATA           | Versetzt Daten aus einem angegebenen Speicherpooldatenträger in einen anderen Speicherpooldatenträger. |
| QUERY ACTLOG        | Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.   |
| QUERY COLLOGROUP    | Zeigt Informationen zu Kollokationsgruppen an.   |
| QUERY FILESPACE     | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.                        |
| QUERY NODEDATA      | Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.                        |
| QUERY OCCUPANCY     | Zeigt Dateibereichsdaten anhand des Speicherpools an.  |
| QUERY PROCESS       | Zeigt Informationen über Hintergrundprozesse an.   |



| Befehl            | Beschreibung  |
|-------------------|---|
| QUERY STGPOOL     | Zeigt Informationen zu Speicherpools an.                |
| QUERY VOLUME      | Zeigt Informationen über Speicherpooldatenträger an.    |
| UPDATE COLLOGROUP | Aktualisiert die Beschreibung einer Kollokationsgruppe. |

- MOVE NODEDATA (Daten in Dateibereichen für einen oder mehrere Knoten oder eine Kollokationsgruppe versetzen)  
Verwenden Sie diesen Befehl, um Daten in Dateibereichen zu versetzen, die zu einem oder mehreren Knoten, einer Knotenkollokationsgruppe oder einer Dateibereichskollokationsgruppe gehören.
- MOVE NODEDATA (Daten aus ausgewählten Dateibereichen eines einzelnen Knotens versetzen)  
Verwenden Sie diesen Befehl, um Daten für ausgewählte Dateibereiche zu versetzen, die zu einem einzelnen Knoten gehören.

## MOVE NODEDATA (Daten in Dateibereichen für einen oder mehrere Knoten oder eine Kollokationsgruppe versetzen)

Verwenden Sie diesen Befehl, um Daten in Dateibereichen zu versetzen, die zu einem oder mehreren Knoten, einer Knotenkollokationsgruppe oder einer Dateibereichskollokationsgruppe gehören.

### Berechtigungsklasse

Um diesen Befehl auszugeben, benötigen Sie die Systemberechtigung, die uneingeschränkte Speicherberechtigung oder die eingeschränkte Speicherberechtigung für den Quellenspeicherpool. Wenn Ihre Berechtigung die eingeschränkte Speicherberechtigung ist und Sie Daten in einen anderen Speicherpool versetzen, benötigen Sie die entsprechende Berechtigung für den Zielspeicherpool.

### Syntax

```

      .-,'-----'.
      v           |
>>-MOVE NODEdata+---Knotenname-+-----+----->
      '-COLLOGroup----Gruppenname-'

>--FROMstgpool----Name_des_Quellenpools----->

>+-----+----->
  '-TOstgpool----Name_des_Zielpools-'

      .-Type----ANY-----'.
>+-----+----->
  '-Type----+ANY-----+-'
      +-Backup-----+
      +-ARchive-----+
      '-SPacemanaged-'

      .-MAXPRocess----1-----'.  .-Wait----No-----'.
>+-----+-----+-----+----->
  '-MAXPRocess----Anzahl_Prozesse-'  '-Wait----+No--+-'
                                     '-Yes-'

                                     (1)
      .-RECONStruct----No oder Yes-----'.
>+-----+-----+-----+----->
  '-RECONStruct----+No--+-----+'
                                     '-Yes-'

```

Anmerkungen:

1. Der Standardwert ist NO, wenn entweder der Quellen- oder der Zielspeicherpool ein Speicherpool mit wahlfreiem Zugriff ist. Der Standardwert ist YES, wenn sowohl der Quellenspeicherpool als auch der Zielspeicherpool ein Speicherpool mit sequenziellem Zugriff ist.

### Parameter

Knotenname (Erforderlich, wenn nicht der Parameter COLLOGROUP angegeben ist)

Gibt den Knotennamen für die Daten an, die mit diesem Befehl versetzt werden. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

COLLOCGroup (Erforderlich, wenn nicht der Parameter für den Knotennamen angegeben ist)

Gibt den Namen der Kollokationsgruppe an, deren Daten versetzt werden müssen. Daten für alle Knoten und Dateibereiche, die zu der Kollokationsgruppe gehören, werden versetzt.

FROMstgpool (Erforderlich)

Gibt den Namen eines Speicherpools mit sequenziellem Zugriff an, der Daten enthält, die versetzt werden sollen. Dieser Speicherpool muss das Datenformat NATIVE oder NONBLOCK haben.

TOstgpool

Gibt den Namen eines Speicherpools an, in den die Daten versetzt werden. Dieser Speicherpool muss das Datenformat NATIVE oder NONBLOCK haben. Dieser Parameter ist optional und gilt nicht, wenn der Quellenspeicherpool ein Kopierspeicherpool oder ein Pool für aktive Daten ist. Ist der Quellenspeicherpool ein Kopierspeicherpool, muss das Ziel derselbe Kopierspeicherpool sein. Ist der Quellenspeicherpool ein Pool für aktive Daten, muss das Ziel ebenfalls derselbe Pool für aktive Daten sein. Wird kein Wert angegeben, werden Daten auf andere Datenträger innerhalb des Quellenspeicherpools versetzt.

Wichtig: Werden Daten innerhalb desselben Speicherpools versetzt, müssen Datenträger verfügbar sein, die nicht die Knotendaten enthalten, die versetzt werden. Der Server kann nicht Datenträger, die die zu versetzenden Daten enthalten, als Zieldatenträger verwenden.

Type

Gibt den Typ der Dateien an, die versetzt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Ist der Quellenspeicherpool ein Pool für aktive Daten, sind nur die Werte ANY und BACKUP gültig. Bei TYPE=ANY werden jedoch nur die aktiven Versionen von Sicherungsdateien versetzt. Geben Sie einen der folgenden Werte an:

ANY

Gibt an, dass alle Typen der Dateien versetzt werden.

Backup

Gibt an, dass Sicherungsdateien versetzt werden.

ARchive

Gibt an, dass Archivierungsdateien versetzt werden. Dieser Wert ist für Pools für aktive Daten nicht gültig.

SPacemanaged

Gibt an, dass speicherverwaltete Dateien (Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden) versetzt werden. Dieser Wert ist für Pools für aktive Daten nicht gültig.

MAXPRocess

Gibt die maximale Anzahl paralleler Prozesse an, die zum Versetzen von Daten verwendet werden. Dieser Parameter ist wahlfrei. Sie können einen Wert von 1 bis einschließlich 999 angeben. Der Standardwert ist 1. Bei einer Erhöhung der Anzahl paralleler Prozesse wird normalerweise der Durchsatz verbessert.

Bei der Bestimmung dieses Werts ist die Anzahl der logischen und physischen Laufwerke zu berücksichtigen, die dieser Operation zugeordnet werden kann. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl der verfügbaren Mountpunkte und Laufwerke ist von anderen IBM Spectrum Protect-Systemaktivitäten abhängig. Die Mountpunkte und Laufwerke sind auch von den Grenzwerten für Ladeanforderungen der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die von der Versetzung betroffen sind. Jeder Prozess benötigt einen Mountpunkt für Speicherpoolatenträger und, falls der Einheitentyp nicht FILE lautet, außerdem ein Laufwerk.

Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Geben Sie einen der folgenden Werte an:

No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

Bei dem Hintergrundprozess erstellte Nachrichten werden vom Server entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird ein Hintergrundprozess abgebrochen, wurden einige Dateien möglicherweise vor dem Abbruch versetzt.

Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Der Befehl muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist.

Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

RECONStruct

Gibt an, ob Dateiaaggregate beim Versetzen von Daten wiederhergestellt werden sollen. Bei der Wiederherstellung wird leerer Speicherbereich entfernt, der sich durch das Löschen von logischen Dateien aus einem Aggregat angesammelt hat. Dieser Parameter ist wahlfrei. Ist sowohl der Quellenspeicherpool als auch der Zielspeicherpool ein Speicherpool mit sequenziellem

Zugriff, ist der Standardwert YES. Ist entweder der Quellen- oder der Zielspeicherpool ein Speicherpool mit wahlfreiem Zugriff, ist der Standardwert NO.

Der Parameter ist nicht verfügbar oder wird ignoriert, wenn eine der folgenden Bedingungen zutrifft:

- Das Datenformat ist NETAPPDUMP, CELERRADUMP oder NDMPDUMP.
- Die Daten befinden sich in einem Speicherpool, der für die Deduplizierung von Daten konfiguriert ist.
- Der Zielspeicherpool für die Datenversetzung ist für die Deduplizierung von Daten konfiguriert.

Achtung: Bei der Wiederherstellung werden inaktive Sicherungsdateien in Pools für aktive Daten entfernt. Geben Sie RECONSTRUCT=NO an, wenn die Daten in einen Pool für aktive Daten versetzt werden, der nicht für die Deduplizierung von Daten konfiguriert ist, verbleiben inaktive Sicherungsdateien in dem Speicherpool.

Sie können einen der folgenden Werte angeben:

No

Gibt an, dass die Wiederherstellung von Dateiaгрегaten beim Versetzen von Daten nicht ausgeführt wird.

Yes

Gibt an, dass die Wiederherstellung von Dateiaгрегaten beim Versetzen von Daten ausgeführt wird. Sie können diese Option nur angeben, wenn die Quellen- und Zielspeicherpools Speicherpools mit sequenziellem Zugriff sind.

## Die Daten eines bestimmten Knotens aus einem Bandspeicherpool in einen Plattenspeicherpool versetzen

---

Alle Daten für Knoten MARY versetzen, die im Speicherpool TAPEPOOL gespeichert sind. Die Daten können in den Plattenspeicherpool BACKUPPOOL versetzt werden.

```
move nodedata mary
  fromstgpool=tapepool tostgpool=backuppool
```

## Daten für eine Knotenkollokationsgruppe aus einem Speicherpool in einen anderen Speicherpool versetzen

---

Alle Daten für die Knotenkollokationsgruppe NODEGROUP1 aus dem Speicherpool SOURCEPOOL in den Speicherpool TARGETPOOL versetzen.

```
move nodedata collogroup=nodegroup1 fromstgpool=sourcespool tostgpool=targetpool
```

## Daten für eine Dateibereichskollokationsgruppe aus einem Speicherpool in einen anderen Speicherpool versetzen

---

Alle Daten für die Dateibereichskollokationsgruppe FSGROUP1 aus dem Speicherpool SOURCEPOOL2 in den Speicherpool TARGETPOOL2 versetzen.

```
move nodedata collogroup=fsgroup1 fromstgpool=sourcespool2 tostgpool=targetpool2
```

## MOVE NODEDATA (Daten aus ausgewählten Dateibereichen eines einzelnen Knotens versetzen)

---

Verwenden Sie diesen Befehl, um Daten für ausgewählte Dateibereiche zu versetzen, die zu einem einzelnen Knoten gehören.

## Berechtigungsklasse

---

Um diesen Befehl auszugeben, benötigen Sie die Systemberechtigung, die uneingeschränkte Speicherberechtigung oder die eingeschränkte Speicherberechtigung für den Quellenspeicherpool. Ist Ihre Berechtigung die eingeschränkte Speicherberechtigung und möchten Sie Daten in einen anderen Speicherpool versetzen, benötigen Sie auch die entsprechende Berechtigung für den Zielspeicherpool.

## Syntax

---

```
>>-MOVE NODEdata--Knotenname----->
>--FROMstgpool---Name_des_Quellenpools----->
>--+-----+
  '-TOstgpool---Name_des_Zielpools-'
```

```

>----->
|           .-,----- . |
|           v           | |
|'-Filespace-----Dateibereichsname+-'
>----->
|           .-,----- . |
|           v           | |
|'-UNIFILESpace-----Unicode-Dateibereichsname+-'
>----->
|           .-,----- . |
|           v           | |
|'-FSID-----Dateibereichs-ID+-'
|
| .-Type-----ANY----- .
>----->
|'-Type-----+ANY-----+'
|           +-Backup-----+
|           +-ARchive-----+
|           '-SPacemanaged-'
|
| .-MAXPRocess-----1----- . .-Wait-----No----- .
>----->
|'-MAXPRocess-----Anzahl_Prozesse-' '-Wait-----+No--+-'
|                                     '-Yes-'
|
|                                     (1)
| .-RECONStruct-----No oder Yes----- .
>----->
|'-RECONStruct-----+No--+-----+'
|                                     '-Yes-'

```

#### Anmerkungen:

1. Der Standardwert ist NO, wenn entweder der Quellen- oder der Zielspeicherpool ein Speicherpool mit wahlfreiem Zugriff ist. Der Standardwert ist YES, wenn sowohl der Quellenspeicherpool als auch der Zielspeicherpool ein Speicherpool mit sequenziellem Zugriff ist.

## Parameter

### Knotenname (Erforderlich)

Gibt den Knotennamen für die Daten an, die mit diesem Befehl versetzt werden. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

### FROMstgpool (Erforderlich)

Gibt den Namen eines Speicherpools mit sequenziellem Zugriff an, der Daten enthält, die versetzt werden sollen. Dieser Speicherpool muss das Datenformat NATIVE oder NONBLOCK haben.

### TOstgpool

Gibt den Namen eines Speicherpools an, in den Daten versetzt werden. Dieser Speicherpool muss das Datenformat NATIVE oder NONBLOCK haben. Dieser Parameter ist optional und gilt nicht, wenn der Quellenspeicherpool ein Kopierspeicherpool oder ein Pool für aktive Daten ist. Ist der Quellenspeicherpool ein Kopierspeicherpool, muss das Ziel derselbe Kopierspeicherpool sein. Ist der Quellenspeicherpool ein Pool für aktive Daten, muss das Ziel ebenfalls derselbe Pool für aktive Daten sein. Wird kein Wert angegeben, werden Daten auf andere Datenträger innerhalb des Quellenpools versetzt.

Wichtig: Werden Daten innerhalb desselben Speicherpools versetzt, müssen Datenträger verfügbar sein, die nicht die Knotendaten enthalten, die versetzt werden. Der Server kann nicht Datenträger, die die zu versetzenden Daten enthalten, als Zieldatenträger verwenden.

### FILEspace

Gibt den Namen des Nicht-Unicode-Dateibereichs an, der Daten enthält, die versetzt werden sollen. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Geben Sie für diesen Parameter und für UNIFILESPACE und/oder FSID keine Werte an, werden Nicht-Unicode-Dateibereiche nicht versetzt.

### UNIFILESpace

Gibt den Namen des Unicode-Dateibereichs an, der Daten enthält, die versetzt werden sollen. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Geben Sie für diesen Parameter und für FILESPACE und/oder FSID keine Werte an, werden Nicht-Unicode-Dateibereiche nicht versetzt.

### FSID

Gibt die Dateibereich-IDs (FSIDs) für die Dateibereiche an, die versetzt werden sollen. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Dieser Parameter ist wahlfrei.

## Type

Gibt den Typ der Dateien an, die versetzt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Ist der Quellenspeicherpool ein Pool für aktive Daten, sind nur die Werte ANY und BACKUP gültig. Bei TYPE=ANY werden jedoch nur die aktiven Versionen von Sicherungsdateien versetzt. Gültige Werte:

### ANY

Gibt an, dass alle Typen der Dateien versetzt werden.

### Backup

Gibt an, dass Sicherungsdateien versetzt werden.

### ARchive

Gibt an, dass Archivierungsdateien versetzt werden. Dieser Wert ist für Pools für aktive Daten nicht gültig.

### SPacemanaged

Gibt an, dass speicher verwaltete Dateien (Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden) versetzt werden. Dieser Wert ist für Pools für aktive Daten nicht gültig.

## MAXPRocess

Gibt die maximale Anzahl paralleler Prozesse an, die zum Versetzen von Daten verwendet werden. Dieser Parameter ist wahlfrei. Mögliche Werte sind 1–999 einschließlich. Der Standardwert ist 1. Eine Erhöhung der Anzahl paralleler Prozesse sollte den Durchsatz verbessern.

Bei der Bestimmung dieses Werts ist die Anzahl der logischen und physischen Laufwerke zu berücksichtigen, die dieser Operation zugeordnet werden kann. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl der verfügbaren Mountpunkte und Laufwerke ist von anderen IBM Spectrum Protect-Systemaktivitäten sowie von den Grenzwerten für Ladeanforderungen der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die von dem Versetzen betroffen sind. Jeder Prozess benötigt einen Mountpunkt für Speicherpool datenträger und, falls der Einheitentyp nicht FILE lautet, außerdem ein Laufwerk.

## Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

### No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

Bei dem Hintergrundprozess erstellte Nachrichten werden vom Server entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird ein Hintergrundprozess abgebrochen, wurden einige Dateien möglicherweise vor dem Abbruch bereits versetzt.

### Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Der Befehl muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist.

Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

## RECONStruct

Gibt an, ob Dateiaggregate beim Versetzen von Daten wiederhergestellt werden sollen. Bei der Wiederherstellung wird leerer Speicherbereich entfernt, der sich durch das Löschen von logischen Dateien aus einem Aggregat angesammelt hat. Dieser Parameter ist wahlfrei. Ist sowohl der Quellenspeicherpool als auch der Zielspeicherpool ein Speicherpool mit sequenziellem Zugriff, ist der Standardwert YES. Ist entweder der Quellen- oder der Zielspeicherpool ein Speicherpool mit wahlfreiem Zugriff, ist der Standardwert NO.

Der Parameter ist nicht verfügbar oder wird ignoriert, wenn eine der folgenden Bedingungen zutrifft:

- Das Datenformat ist NETAPPDUMP, CELERRADUMP oder NDMPDUMP.
- Die Daten befinden sich in einem Speicherpool, der für die Deduplizierung von Daten konfiguriert ist.
- Der Zielspeicherpool für die Datenversetzung ist für die Deduplizierung von Daten konfiguriert.

Achtung: Bei der Wiederherstellung werden inaktive Sicherungsdateien in Pools für aktive Daten entfernt. Geben Sie RECONSTRUCT=NO an, wenn die Daten in einen Pool für aktive Daten versetzt werden, der nicht für die Deduplizierung von Daten konfiguriert ist, verbleiben inaktive Sicherungsdateien in dem Speicherpool.

Gültige Werte:

### No

Gibt an, dass die Wiederherstellung von Dateiaggregaten beim Versetzen von Daten nicht ausgeführt wird.

### Yes

Gibt an, dass die Wiederherstellung von Dateiaгрегатат beim Versetzen von Daten ausgeführt wird. Sie können diese Option nur angeben, wenn Quellen- und Zielspeicherpool Speicherpools mit sequenziellem Zugriff sind.

## Beispiel: Nicht-Unicode- und Unicode-Daten eines Knotens versetzen

---

Daten für Knoten TOM im Speicherpool TAPEPOOL versetzen. Das Versetzen von Daten auf Dateien in Nicht-Unicode-Dateibereichen und Unicode-Dateibereichen \\jane\d\$ beschränken. Die Daten sollen in den Plattenspeicherpool BACKUPPOOL versetzt werden.

```
move nodedata tom
  fromstgpool=tapepool tostgpool=backuppool
  filespace=* unifilespace=\\jane\d$
```

## Beispiel: Alle Knotendaten aus Bandspeicherpools in einen Plattenspeicherpool versetzen

---

Alle Daten für Knoten SARAH aus allen primären Speicherpools mit sequenziellem Zugriff (in diesem Beispiel TAPEPOOL\*) nach DISKPOOL versetzen. Um eine Liste der Speicherpools zu erhalten, die Daten für Knoten SARAH enthalten, geben Sie einen der folgenden QUERY OCCUPANCY- oder SELECT-Befehle aus:

```
query occupancy sarah

SELECT * from OCCUPANCY where node_name='sarah'
```

Achtung: In diesem Beispiel wird angenommen, dass die Ergebnisse TAPEPOOL1, TAPEPOOL4 und TAPEPOOL5 lauten.

```
move nodedata sarah
  fromstgpool=tapepool1 tostgpool=DISKPOOL

move nodedata sarah
  fromstgpool=tapepool4 tostgpool=DISKPOOL

move nodedata sarah
  fromstgpool=tapepool5 tostgpool=DISKPOOL
```

## Beispiel: Nicht-Unicode- und Unicode-Dateibereiche eines Knotens versetzen

---

Das folgende Beispiel zeigt das Versetzen von Nicht-Unicode-Dateibereichen und Unicode-Dateibereichen für einen Knoten. Für Knoten NOAH den Nicht-Unicode-Dateibereich \\servtuc\d\$ und den Unicode-Dateibereich \\tmserv1e\$ mit der Dateibereichs-ID 2 aus dem Speicherpool TAPEPOOL mit sequenziellem Zugriff in den Speicherpool DISKPOOL mit wahlfreiem Zugriff versetzen.

```
move nodedata noah
  fromstgpool=tapepool tostgpool=diskpool
  filespace=\\tmserv1\d$ fsid=2
```

## NOTIFY SUBSCRIBERS (Verwaltete Server auf Profilaktualisierung hinweisen)

---

Mit diesem Befehl können auf einem Konfigurationsmanager ein oder mehrere verwaltete Server benachrichtigt werden, dass ihre Konfigurationsdaten sofort aktualisiert werden müssen.

### Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

---

```
>>>NOTIfy SUBSCRIBers--.-PROFILE-----*----->>>
|-----+-----|
|          .-,----- . |
|          v          | |
|'-PROFILE-----Profilname+-'|
```

### Parameter

---

PROFIle (Erforderlich)

Gibt den Namen des Profils an. Alle verwalteten Server, die für das Profil subscribieren, werden benachrichtigt. Es können Platzhalterzeichen verwendet werden, um mehrere Profile anzugeben. Sollen mehrere Profile angegeben werden, die Namen

ohne Leerzeichen durch Kommas voneinander trennen. Standardmäßig werden alle Subskribenten benachrichtigt.

## Beispiel: Verwaltete Server zum Aktualisieren von Profilen benachrichtigen

Alle verwalteten Server, die für das Profil DELTA subskribieren, darauf hinweisen, die Aktualisierung ihrer Konfigurationsdaten anzufordern.

```
notify subscribers profile=delta
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für NOTIFY SUBSCRIBERS

| Befehl              | Beschreibung   |
|---------------------|--|
| DEFINE SUBSCRIPTION | Subskribiert einen verwalteten Server für ein Profil.  |
| DELETE SUBSCRIBER   | Löscht veraltete Subskriptionen verwalteter Server.  |
| DELETE SUBSCRIPTION | Löscht eine angegebene Profilsubskription.   |
| QUERY SUBSCRIBER    | Zeigt Informationen über Subskribenten und ihre Subskriptionen für Profile an.                   |
| QUERY SUBSCRIPTION  | Zeigt Informationen über Profilsubskriptionen an.  |
| SET CONFIGMANAGER   | Gibt an, ob ein Server ein Konfigurationsmanager ist.  |
| SET CONFIGREFRESH   | Gibt das Zeitintervall an, in dem verwaltete Server die Konfigurationsmanager ansprechen sollen. |


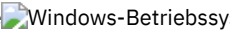
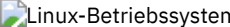
## PERFORM LIBACTION (Alle Laufwerke und Pfade für ein Kassettenarchiv definieren oder löschen)

Verwenden Sie diesen Befehl, um alle Laufwerke und ihre Pfade für ein einzelnes Kassettenarchiv in einem Schritt zu definieren oder zu löschen.

Dieser Befehl kann verwendet werden, wenn eine Kassettenarchivumgebung definiert oder eine vorhandene Hardwarekonfiguration, die Änderungen an vielen Laufwerkdefinitionen erfordert, geändert wird. Nachdem Sie ein Kassettenarchiv definiert haben, geben Sie den Befehl PERFORM LIBACTION aus, um die Laufwerke und ihre Pfade für das Kassettenarchiv zu definieren. Sie können auch alle Laufwerke und Pfade für ein Kassettenarchiv löschen, indem Sie den Befehl mit ACTION=DELETE ausgeben.

Dieser Befehl ist nur für die Speicherarchivtypen SCSI und VTL gültig. Um diesen Befehl mit ACTION=DEFINE verwenden zu können, muss die Option SANDISCOVERY unterstützt werden und aktiviert sein.

Ausführliche und aktuelle Informationen zur Kassettenarchivunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

-   Supported devices for AIX and Windows
-  Supported devices for Linux

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-PERForm LIBACTion--Kassettenarchivname----->
>---ACTion-----+DEFine--| A |----->
      +-DELete-----+
      +-RESet--| B |--+
      '-QUIesce-----'
                                     .-PREView-----No-----
>--+-----+-----+-----+-----><
      '-SOURCe-----Quellename-' '-PREView-----+Yes+-'
                                     '-No--'
```

```

A (DEFine)
|-----+----->
  '-DEVIce-----Name der Kassettenarchiveinheit-'
  .-PREFix-----Kassettenarchivname-.
>-----+-----|
  '-PREFix-----Laufwerkpräfix-----'

B (RESet)
  .-DRIVEsonly-----No----- .
|---ACTion-----RESet---+-----+-----|
  '-DRIVEsonly-----+Yes+-'
  '-No--'

```

## Parameter

### Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das definiert oder gelöscht werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen, es sei denn, Sie geben den Befehl PERFORM LIBACTION mit ACTION=DEFINE aus und verwenden den PREFIX-Standardwert. In diesem Fall beträgt die maximale Länge des Namens 25 Zeichen.

### ACTION

Gibt die Aktion für den Befehl PERFORM LIBACTION an. Gültige Werte:

#### DEFine

Gibt an, dass Laufwerke und ihre Pfade für das angegebene Kassettenarchiv definiert werden. Die SAN-Erkennung muss aktiviert sein, bevor dieser Parameterwert angegeben wird.

#### DELeTe

Gibt an, dass Laufwerke und ihre Pfade für das angegebene Kassettenarchiv gelöscht werden.

#### RESet

Gibt an, dass Laufwerke und ihre Pfade für das angegebene Kassettenarchiv in 'online' aktualisiert werden.

#### DRIVEsonly

Gibt an, dass nur Laufwerke für das angegebene Kassettenarchiv in 'online' aktualisiert werden.  
Gültige Werte:

#### No

Gibt an, dass die Laufwerke und Pfade in 'online' aktualisiert werden.

#### Yes

Gibt an, dass nur die Laufwerke in 'online' aktualisiert werden.

#### QUIEsce

Gibt an, dass die Laufwerke in 'offline' aktualisiert werden.

### DEVIce

Gibt den Namen der Kassettenarchiveinheit an, der beim Definieren von Pfaden verwendet wird, wenn noch kein Pfad zu dem Kassettenarchiv definiert wurde. Ist bereits ein Pfad definiert, wird der Parameter DEVICE ignoriert. Die maximale Länge für diesen Wert beträgt 64 Zeichen. Dieser Parameter ist wahlfrei.

### PREFix

Gibt das Präfix an, das für alle Laufwerkdefinitionen verwendet wird. Beispielsweise werden mit dem PREFIX-Wert *DR* Laufwerke *DRO*, *DR1*, *DR2* für so viele Laufwerke erstellt, wie erstellt werden sollen. Wird für den Parameter PREFIX kein Wert angegeben, wird der Kassettenarchivname als Präfix für Laufwerkdefinitionen verwendet. Die maximale Länge für diesen Wert beträgt 25 Zeichen.

### SOURCE

Gibt den Namen des Quellenservers an, der beim Definieren oder Löschen von Laufwerkpfaddefinitionen auf einem Kassettenarchivclient oder einem LAN-unabhängigen Client verwendet werden soll. Verwenden Sie diesen Parameter nur, wenn die Laufwerke in dem Kassettenarchiv für den lokalen Server definiert sind. Wenn kein Wert für den Parameter SOURCE angegeben wird, wird der Name des lokalen Servers (Standardwert) verwendet. Die maximale Länge für den Quellennamen beträgt 64 Zeichen.

Wird der Parameter SOURCE angegeben, können Sie nur Pfade für angegebene SOURCE-Werte zurücksetzen. Der Parameter SOURCE ist mit den Optionen RESET DRIVESONLY=YES und QUIESCE nicht kompatibel.

Wird ein anderer Quellename als der Name des lokalen Servers mit ACTION=DEFINE angegeben, werden Laufwerkpfaddefinitionen mit dem Tokenwert UNDISCOVERED definiert. Die Pfaddefinitionen werden dann dynamisch von Kassettenarchivclients, die die SAN-Erkennung unterstützen, aktualisiert, wenn das Laufwerk zum ersten Mal angehängt wird.



## PREView

Gibt die Ausgabe aller Befehle an, die für PERFORM LIBACTION verarbeitet werden, bevor der Befehl ausgegeben wird. Der Parameter PREVIEW ist mit dem Parameter DEVICE nicht kompatibel. Wenn Sie den Befehl PERFORM LIBACTION ausgeben, um ein Kassettenarchiv zu definieren, können Sie nicht beide Parameter PREVIEW und DEVICE angeben.

Gültige Werte:

No

Gibt an, dass keine Voranzeige der Befehle, die für PERFORM LIBACTION ausgegeben werden, angezeigt wird.

Yes

Gibt an, dass eine Voranzeige der Befehle, die für PERFORM LIBACTION ausgegeben werden, angezeigt wird.

## Beispiel: Ein gemeinsam genutztes Kassettenarchiv definieren

---

Angenommen, Sie arbeiten in einem SAN und haben einen Kassettenarchivmanager mit dem Namen LIBMGR1 konfiguriert. Definieren Sie jetzt ein Kassettenarchiv mit dem Namen SHAREDTSM für einen Kassettenarchivclientserver mit dem Namen LIBCL1.

Geben Sie den Befehl DEFINE LIBRARY auf dem Kassettenarchivclientserver LIBCL1 aus:

```
define library sharedtsm libtype=shared primarylibmanager=libmgr1
```

Geben Sie dann den Befehl PERFORM LIBACTION auf dem Kassettenarchivmanager LIBMGR1 aus, um die Laufwerkpfade für den Kassettenarchivclient zu definieren:

```
perform libaction sharedtsm action=define source=libcl1
```

Anmerkung: Die Option SANDISCOVERY muss unterstützt werden und auf dem Kassettenarchivclientserver aktiviert sein.


## Beispiel: Kassettenarchiv mit vier Laufwerken definieren

---

Ein SCSI-Kassettenarchiv mit dem Namen KONA definieren:

```
define library kona libtype=scsi
```

Anschließend den Befehl PERFORM LIBACTION ausgeben, um Laufwerke und Pfade für das Kassettenarchiv zu definieren:

 AIX-Betriebssysteme

```
perform libaction kona action=define device=/dev/lb3  
prefix=dr
```

Der Server führt dann die folgenden Befehle aus:

```
define path server1 kona srct=server destt=library  
device=/dev/lb3  
define drive kona dr0  
define path server1 dr0 srct=server destt=drive library=kona  
device=/dev/mt1  
define drive kona dr1  
define path server1 dr1 srct=server destt=drive library=kona  
device=/dev/mt2  
define drive kona dr2  
define path server1 dr2 srct=server destt=drive library=kona  
device=/dev/mt3define drive kona dr3  
define path server1 dr3 srct=server destt=drive library=kona  
device=/dev/mt4
```

 Linux-Betriebssysteme

```
perform libaction kona action=define device=/dev/tmsmcsi/lb3  
prefix=dr
```

Der Server führt dann die folgenden Befehle aus:

```
define path server1 kona srct=server destt=library  
device=/dev/tmsmcsi/lb3  
define drive kona dr0  
define path server1 dr0 srct=server destt=drive library=kona  
device=/dev/tmsmcsi/mt1  
define drive kona dr1  
define path server1 dr1 srct=server destt=drive library=kona  
device=/dev/tmsmcsi/mt2  
define drive kona dr2  
define path server1 dr2 srct=server destt=drive library=kona  
device=/dev/tmsmcsi/mt3define drive kona dr3
```

```
define path server1 dr3 srct=server destt=drive library=kona
device=/dev/tsmcsci/mt4
```

## Windows-Betriebssysteme

```
perform libaction kona action=define device=lb0.0.0.2
prefix=dr
```

Der Server führt dann die folgenden Befehle aus:

```
define path server1 kona srct=server destt=library
device=lb0.0.0.2
define drive kona dr0
define path server1 dr0 srct=server destt=drive library=kona
device=mt0.1.0.2
define drive kona dr1
define path server1 dr1 srct=server destt=drive library=kona
device=mt0.2.0.2
define drive kona dr2
define path server1 dr2 srct=server destt=drive library=kona
device=mt0.3.0.2
define drive kona dr3
define path server1 dr3 srct=server destt=drive library=kona
device=mt0.4.0.2
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für PERFORM LIBACTION

| Befehl         | Beschreibung  |
|----------------|---|
| AUDIT LIBRARY  | Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet. |
| DEFINE DRIVE   | Ordnet ein Laufwerk einem Kassettenarchiv zu.   |
| DEFINE LIBRARY | Definiert ein automatisiertes oder manuelles Kassettenarchiv.                                       |
| DEFINE PATH    | Definiert einen Pfad von einer Quelle zu einem Ziel.  |
| DEFINE SERVER  | Definiert einen Server für die Übertragung zwischen Servern.  |
| DELETE DRIVE   | Löscht ein Laufwerk aus einem Kassettenarchiv.  |
| DELETE LIBRARY | Löscht ein Kassettenarchiv.   |
| DELETE PATH    | Löscht einen Pfad von einer Quelle zu einem Ziel.   |
| QUERY DRIVE    | Zeigt Informationen zu Laufwerken an.   |
| QUERY LIBRARY  | Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.                                 |
| QUERY PATH     | Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.                                     |
| UPDATE DRIVE   | Ändert die Attribute eines Laufwerks.   |
| UPDATE LIBRARY | Ändert die Attribute eines Kassettenarchivs.  |
| UPDATE PATH    | Ändert die zu einem Pfad gehörigen Attribute.   |

## PING SERVER (Verbindung zwischen Servern testen)

Mit diesem Befehl kann die Verbindung zwischen dem lokalen Server und einem fernen Server getestet werden.

Wichtig: Name und Kennwort des Administrator-Clients, der diesen Befehl ausgibt, müssen auch auf dem fernen Server definiert sein. Verfügt der ferne Server über die aktuelle Version, werden die Serverberechtigungs-nachweise automatisch geprüft, wenn der Befehl PING SERVER ausgeführt wird. Verfügt der ferne Server nicht über die aktuelle Version, werden die Serverberechtigungs-nachweise nicht geprüft.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-PING SERVER--Servername----->>
```

## Parameter

Servername (Erforderlich)

Gibt den Namen des fernen Servers an.

## Beispiel: Mit Ping einen Server überprüfen

Die Verbindung zu Server FRED testen.

```
ping server fred
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für PING SERVER

| Befehl        | Beschreibung   |
|---------------|--|
| DEFINE SERVER | Definiert einen Server für die Übertragung zwischen Servern. |
| QUERY SERVER  | Zeigt Informationen über Server an.                          |

## PREPARE (Wiederherstellungsplandatei erstellen)

Mit diesem Befehl kann eine Wiederherstellungsplandatei erstellt werden, die die für die Wiederherstellung eines IBM Spectrum Protect-Servers erforderlichen Daten enthält. Eine Wiederherstellungsplandatei kann in einem Dateisystem gespeichert werden, auf das vom Quellenserver oder einem Zielserver zugegriffen werden kann.

Mit dem Befehl QUERY ACTLOG kann abgefragt werden, ob der Befehl PREPARE erfolgreich ausgeführt wurde.

Diese Informationen können auch von der Serverkonsole oder, wenn für den Parameter WAIT der Wert YES angegeben wird, von einer Verwaltungsklientsitzung aus abgefragt werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```

>>-Prepare .-Source-----DBBackup----->
      |-----+-----+-----|
      |'-Source-----+DBBackup--+-'
      |         '-DBSnapshot-'
>-----+-----+----->
      |'-DEVclass-----Einheitenklassename-'
>-----+-----+-----+-----+----->
      |'-PLANPrefix-----Präfix-'  '-INSTRPrefix-----Präfix-'
>-----+-----+-----+----->
      |           .-,------ . |
      |           V           | |
      |'-COPYstgpool-----Poolname-+-'
>-----+-----+-----+----->
      |           .-,------ . |
      |           V           | |
      |'-ACTIVEDatastgpool-----Poolname-+-'
>-----+-----+-----+-----+----->
      |           .-,------ . |
      |           V           | |
      |'-PRIMstgpool-----Poolname-+-'
      |           '-Wait-----No-----'
      |           |-----+-----+-----|
      |           |'-Wait-----+No-+-'
      |           |         '-Yes-'
      |
      |-----+-----+-----+----->>

```

## Parameter

---

### Source

Gibt die Art der Datenbanksicherungsserie an, die IBM Spectrum Protect beim Generieren der Wiederherstellungsplandatei annimmt. Dieser Parameter ist wahlfrei. Der Standardwert ist DBBACKUP. Unter folgenden Möglichkeiten kann gewählt werden:

#### DBBackup

Gibt an, dass IBM Spectrum Protect die letzte vollständige Datenbanksicherungsserie annimmt.

#### DBSnapshot

Gibt an, daß IBM Spectrum Protect die letzte Sicherungsserie mit Datenbankmomentaufnahmen annimmt.



### DEVclass

Gibt den Namen der Einheitenklasse an, mit der ein Wiederherstellungsplandateiobjekt auf einem Ziel-Server erstellt wird. Die Einheitenklasse muß den Einheitentyp SERVER haben.

Wichtig: Die maximale Kapazität für die Einheitenklasse muß größer als die Größe der Wiederherstellungsplandatei sein.

Überschreitet die Größe der Wiederherstellungsplandatei die maximale Kapazität, schlägt der Befehl fehl.

Die Namenskonvention für das Archivierungsobjekt mit der Wiederherstellungsplandatei auf dem Ziel-Server lautet:

- **Dateibereichsname:**
  - ADSM.SERVER
- **Qualifikationsmerkmal der oberen Ebene:**
  -  Linux-Betriebssystemedevclassprefix/servername.yyyymmdd.hhmmss
  -  Windows-Betriebssystemedevclassprefix\servername.yyyymmdd.hhmmss
- **Qualifikationsmerkmal der unteren Ebene:**
  - RPF.OBJ.1



Der Name des virtuellen Bereichs der Wiederherstellungsplandatei, der in der Datenträger-History-Tabelle auf dem Quellen-Server aufgezeichnet ist, hat das Format `servername.yyyymmdd.hhmmss`.

Wird der Parameter DEVCLASS nicht angegeben, wird die Wiederherstellungsplandatei auf der Basis des Planpräfix in eine Datei geschrieben.

Wird SOURCE=DBBACKUP angegeben oder als Standardwert verwendet, gibt der Datenträger-History-Eintrag für das Wiederherstellungsplandateiobjekt den Datenträgertyp RPFIL an. Wird SOURCE=DBSNAPSHOT angegeben, gibt der Datenträger-History-Eintrag den Datenträgertyp RPFNSAPSHOT an.


### PLANPrefix

Gibt das Pfadnamenpräfix an, das im Namen der Wiederherstellungsplandatei verwendet wird. Dieser Parameter ist wahlfrei.

-  Linux-BetriebssystemeDie maximale Länge beträgt 250 Zeichen.
-  Die maximale Länge beträgt 200 Zeichen.

 Gibt das Pfadnamenpräfix an, das im Namen der Wiederherstellungsplandatei verwendet wird.

IBM Spectrum Protect hängt an das Präfix das sortierbare Datums- und Zeitformat `jjjjmmtt.hhmmss`. Beispiel: `20081115.051421`.

 Linux-BetriebssystemeDas Präfix kann Folgendes sein:

#### Verzeichnispfad

Das Präfix mit dem Schrägstrich (/) beenden. Beispiel:

```
PLANPREFIX=/admsrv/recplans/
```

Der daraus resultierende Dateiname würde wie folgt aussehen:

```
/admsrv/recplans/20081115.051421
```

#### Verzeichnispfad, gefolgt von einer Zeichenfolge

IBM Spectrum Protect behandelt die Zeichenfolge als Teil des Dateinamens. Beispiel:

```
PLANPREFIX=/admsrv/recplans/accounting
```

Der daraus resultierende Dateiname sieht wie folgt aus:

```
/admsrv/recplans/accounting.20081115.051421
```

Den Punkt vor dem Datum und der Uhrzeit beachten.

Nur Zeichenfolge

IBM Spectrum Protect gibt den Verzeichnispfad an. IBM Spectrum Protect verwendet den Namen des aktuellen Arbeitsverzeichnisses. Beispiel: Das aktuelle Arbeitsverzeichnis lautet /opt/tivoli/tsm/server/bin und es wird der folgende Parameter angegeben:

```
PLANPREFIX=shipping
```

Der daraus resultierende Dateiname sieht wie folgt aus:

```
/opt/tivoli/tsm/server/bin/shipping.20081115.051421
```

Den Punkt vor dem Datum und der Uhrzeit beachten.

 Windows-Betriebssysteme Das Präfix kann Folgendes sein:

Verzeichnispfad

Das Präfix mit dem umgekehrten Schrägstrich (\) beenden. Beispiel:

```
PLANPREFIX=c:\admsrv\recplans\
```

Der daraus resultierende Dateiname sieht wie folgt aus:

```
c:\admsrv\recplans\20081115.051421
```

Tipp: Wenn Sie den Befehl PREPARE über den Verwaltungsbefehlszeilenclient ausgeben und das letzte Zeichen in der Befehlszeile ein umgekehrter Schrägstrich ist, wird er als Fortsetzungszeichen interpretiert. Um dies zu vermeiden, den Präfixwert in Anführungszeichen setzen. Beispiel:

```
PLANPREFIX="c:\admsrv\recplans\"
```

Verzeichnispfad, gefolgt von einer Zeichenfolge

IBM Spectrum Protect behandelt die Zeichenfolge als Teil des Dateinamens. Beispiel:

```
PLANPREFIX=c:\admsrv\recplans\accounting
```

Der daraus resultierende Dateiname sieht wie folgt aus:

```
c:\admsrv\recplans\accounting.20081115.051421
```

Den Punkt vor dem Datum und der Uhrzeit beachten.

Nur Zeichenfolge


IBM Spectrum Protect hängt das Datum und die Uhrzeit im Format *.yyyymmdd.hhmmss* (den Punkt vor dem Datum und der Uhrzeit beachten) an das Präfix an. Der von dem Befehl PREPARE verwendete Verzeichnispfad ist das Verzeichnis, das dieses "Exemplar" des IBM Spectrum Protect-Servers darstellt. Dabei handelt es sich normalerweise um das ursprüngliche Installationsverzeichnis des IBM Spectrum Protect-Servers. Im folgenden Beispiel stellt `c:\Programme\Tivoli\TSM;\server2` dieses Verzeichnis dar, und der Befehl PREPARE wird mit folgendem Parameter ausgegeben:

```
PLANPREFIX=shipping
```

Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

```
c:\Programme\Tivoli\TSM;\server2\shipping.20081115.051421
```



Wird der Parameter PLANPREFIX nicht angegeben, wählt IBM Spectrum Protect das Präfix wie folgt aus:

- Wurde der Befehl SET DRMPREFIX ausgegeben, verwendet IBM Spectrum Protect das in diesem Befehl angegebene Präfix.
-  Windows-Betriebssysteme Ist der Befehl SET DRMPREFIX nicht definiert, verwendet IBM Spectrum Protect als Pfad das Verzeichnis, das dieses "Exemplar" des IBM Spectrum Protect-Servers darstellt. Hierbei handelt es sich normalerweise um das ursprüngliche Installationsverzeichnis des IBM Spectrum Protect-Servers. Beispiel: Folgendes Verzeichnis bildet das vorliegende Exemplar des Servers:

```
c:\Programme\Tivoli\TSM;\server2
```

Der daraus resultierende Name der Wiederherstellungsplandatei lautet wie folgt:

```
c:\Programme\Tivoli\TSM;\server2\20081115.051421
```






-  AIX-Betriebssysteme  Linux-Betriebssysteme Wurde der Befehl SET DRMPREFIX nicht ausgegeben, verwendet IBM Spectrum Protect den Verzeichnispfadnamen des aktuellen Arbeitsverzeichnisses. Das aktuelle Arbeitsverzeichnis lautet beispielsweise:

```
/opt/tivoli/tsm/server/bin
```

Der daraus resultierende Dateiname sieht wie folgt aus:

/opt/tivoli/txm/server/bin/20081115.051421

## INSTRPrefix

Gibt das Präfix des Pfadnamens an, das von IBM Spectrum Protect zum Lokalisieren der Dateien verwendet wird, die die Wiederherstellungsanweisungen enthalten. Die maximale Länge beträgt  AIX-Betriebssysteme  Linux-Betriebssysteme 250  Windows-Betriebssysteme 200 Zeichen.  
 AIX-Betriebssysteme  Linux-Betriebssysteme Das Präfix kann Folgendes sein:

### Verzeichnispfad

Das Präfix mit dem Schrägstrich (/) beenden. Beispiel:

```
INSTRPREFIX=/admsrv/recinstr/  
  
/admsrv/recinstr/RECOVERY.INSTRUCTIONS.GENERAL
```

### Verzeichnispfad, gefolgt von einer Zeichenfolge

IBM Spectrum Protect behandelt die Zeichenfolge als Teil des Dateinamens. Beispiel:

```
INSTRPREFIX=/admsrv/recinstr/accounts
```

IBM Spectrum Protect hängt den entsprechenden Namen der Zeilengruppe für die Wiederherstellungsplandatei an. Für die Datei RECOVERY.INSTRUCTIONS.GENERAL lautet der daraus resultierende Dateiname wie folgt:

```
/admsrv/recinstr/accounts.RECOVERY.INSTRUCTIONS.GENERAL
```

### Nur Zeichenfolge

- IBM Spectrum Protect gibt den Verzeichnispfad an und hängt den entsprechenden Namen der Zeilengruppe für die Wiederherstellungsplandatei an. IBM Spectrum Protect verwendet den Namen des aktuellen Arbeitsverzeichnisses. Beispiel: Das aktuelle Arbeitsverzeichnis lautet /opt/tivoli/txm/server/bin und es wird der folgende Parameter angegeben:

```
INSTRPREFIX=shipping
```

Für die Datei RECOVERY.INSTRUCTIONS.GENERAL sieht der daraus resultierende Dateiname wie folgt aus:

```
/opt/tivoli/txm/server/bin/shipping.RECOVERY.INSTRUCTIONS.GENERAL
```

 Windows-Betriebssysteme Das Präfix kann Folgendes sein:

### Verzeichnispfad

Das Präfix mit dem umgekehrten Schrägstrich (\) beenden. Beispiel:

```
INSTRPREFIX=c:\admsrv\recinstr\
```

IBM Spectrum Protect hängt den entsprechenden Namen der Zeilengruppe für die Wiederherstellungsplandatei an. Für die Datei RECOVERY.INSTRUCTIONS.GENERAL lautet der daraus resultierende Dateiname wie folgt:

```
c:\admsrv\recinstr\RECOVERY.INSTRUCTIONS.GENERAL
```

Tipp: Wenn Sie den Befehl PREPARE über den Verwaltungsbefehlszeilenclient ausgeben und das letzte Zeichen in der Befehlszeile ein umgekehrter Schrägstrich ist, wird er als Fortsetzungszeichen interpretiert. Um dies zu vermeiden, den Präfixwert in Anführungszeichen setzen. For example:

```
INSTRPREFIX="c:\admserv\recinstr\"
```

### Verzeichnispfad, gefolgt von einer Zeichenfolge

IBM Spectrum Protect behandelt die Zeichenfolge als Teil des Dateinamens. Beispiel:

```
INSTRPREFIX=c:\admsrv\recinstr\accounts
```

IBM Spectrum Protect hängt den entsprechenden Namen der Zeilengruppe für die Wiederherstellungsplandatei an. Für die Datei RECOVERY.INSTRUCTIONS.GENERAL lautet der daraus resultierende Dateiname wie folgt:

```
c:\admsrv\recinstr\accounts.RECOVERY.INSTRUCTIONS.GENERAL
```

### Nur Zeichenfolge

IBM Spectrum Protect gibt den Verzeichnispfad an und hängt den entsprechenden Namen der Zeilengruppe für die Wiederherstellungsplandatei an. IBM Spectrum Protect hängt den Namen der Zeilengruppe für die Wiederherstellungsplandatei an das Präfix an. Ist das Präfix nur eine Zeichenfolge, ist der von dem Befehl PREPARE verwendete Verzeichnispfad das Verzeichnis, das dieses Exemplar des IBM Spectrum Protect-Servers darstellt. Dabei handelt es sich normalerweise um das ursprüngliche Installationsverzeichnis des IBM Spectrum Protect-Servers. Im


folgenden Beispiel stellt c:\Programme\Tivoli\TSM;\server2 dieses Verzeichnis dar, und der Befehl PREPARE wird mit folgendem Parameter ausgegeben:

```
INSTRPREFIX=dock
```

Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

```
c:\Programme\Tivoli\TSM;\server2\shipping.20081115.051421
```



Wird der Parameter INSTRPREFIX nicht angegeben, wählt IBM Spectrum Protect das Präfix wie folgt aus:

- Wurde der Befehl SET DRMINSTRPREFIX ausgegeben, verwendet IBM Spectrum Protect das in diesem Befehl angegebene Präfix.
-  Windows-Betriebssysteme Wenn der Befehl SET DRMINSTRPREFIX nicht ausgegeben wurde, verwendet IBM Spectrum Protect das Verzeichnis, das diese "Instanz" des IBM Spectrum Protect-Servers darstellt, als Pfad; hierbei handelt es sich normalerweise um das ursprüngliche Installationsverzeichnis des Servers. Beispiel: Folgendes Verzeichnis bildet das vorliegende Exemplar des Servers:

```
c:\Programme\Tivoli\TSM;\server2
```

Der daraus resultierende Name der Wiederherstellungsplandatei lautet wie folgt:

```
c:\Programme\Tivoli\TSM;\server2\RECOVERY.INSTRUCTIONS.GENERAL
```

-  AIX-Betriebssysteme  Linux-Betriebssysteme Wurde der Befehl SET DRMINSTRPREFIX nicht ausgegeben, verwendet IBM Spectrum Protect das aktuelle Arbeitsverzeichnis. Lautet beispielsweise das aktuelle Arbeitsverzeichnis /opt/tivoli/tsm/server/bin, würde für die Datei RECOVERY.INSTRUCTIONS.GENERAL der daraus resultierende Dateiname wie folgt lauten:

```
/opt/tivoli/tsm/server/bin/RECOVERY.INSTRUCTIONS.GENERAL
```

#### PRIMStgpool

Gibt die Namen der primären Speicherpools an, die wiederhergestellt werden sollen. Die Speicherpoolnamen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden. Wird dieser Parameter nicht angegeben, wählt IBM Spectrum Protect die Speicherpools wie folgt aus:

- Wurde der Befehl SET DRMPRIMSTGPOOL ausgegeben, berücksichtigt IBM Spectrum Protect die in diesem Befehl angegebenen primären Speicherpools.
- Wurde der Befehl SET DRMPRIMSTGPOOL nicht ausgegeben, berücksichtigt IBM Spectrum Protect alle primären Speicherpools.

#### COPYStgpool

Gibt die Namen der Kopierspeicherpools an, die zum Sichern der primären Speicherpools verwendet wurden, die wiederhergestellt werden sollen (siehe Parameter PRIMSTGPOOL). Die Speicherpoolnamen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden. Wird dieser Parameter nicht angegeben, wählt IBM Spectrum Protect die Speicherpools wie folgt aus:

- Wurde der Befehl SET DRMCOPYSTGPOOL ausgegeben, berücksichtigt IBM Spectrum Protect diese Kopierspeicherpools.
- Wurde der Befehl SET DRMCOPYSTGPOOL nicht ausgegeben, berücksichtigt IBM Spectrum Protect alle Kopierspeicherpools.

#### ACTIVEDataStgpool

Gibt die Namen der Speicherpools für aktive Daten an, die für den Zugriff an einem anderen Standort verfügbar sein sollen. Die Namen der Speicherpools für aktive Daten sind ohne Leerzeichen durch Kommas voneinander zu trennen. Es können Platzhalterzeichen verwendet werden. Wird dieser Parameter nicht angegeben, wählt IBM Spectrum Protect die Speicherpools wie folgt aus:

- Wurde der Befehl SET ACTIVEDATASTGPOOL zuvor mit gültigen Namen von Speicherpools für aktive Daten ausgegeben, verarbeitet IBM Spectrum Protect diese Speicherpools.
- Wurde der Befehl SET ACTIVEDATASTGPOOL nicht ausgegeben, oder wurden alle Speicherpools für aktive Daten mit dem Befehl SET ACTIVEDATASTGPOOL entfernt, verarbeitet IBM Spectrum Protect nur die Datenträger im Pool für aktive Daten, die zum Zeitpunkt der Ausführung des Befehls PREPARE als ONSITE markiert waren. IBM Spectrum Protect markiert diese Datenträger als UNAVAILABLE.

#### Wait



Gibt an, ob dieser Befehl im Hintergrund oder Vordergrund verarbeitet wird.

No

Gibt die Hintergrundverarbeitung an. Dies ist der Standardwert.

Yes

Gibt die Vordergrundverarbeitung an.

  YES kann nicht von der Server-Konsole aus angegeben werden.

## Beispiel: Eine Wiederherstellungsplandatei erstellen

Den Befehl PREPARE ausgeben und das Aktivitätenprotokoll abfragen, um die Ergebnisse zu prüfen.

```
prepare
query actlog search=prepare
```

```
05/03/2008 12:01:13 ANR0984I Prozess 3 für PREPARE im
BACKGROUND um 12:01:13 gestartet.
05/03/2008 12:01:13 ANR6918W PREPARE: Datei mit Wiederherstellungsanweisungen
/home/guest/drmtest/prepare/tserver/DSM1509/
RECOVERY.INSTRUCTIONS.DATABASE nicht gefunden.
05/03/2008 12:01:13 ANR6918W PREPARE: Datei mit Wiederherstellungsanweisungen
/home/guest/drmtest/prepare/tserver/DSM1509/
RECOVERY.INSTRUCTIONS.STGPOOL nicht gefunden.
05/03/2008 12:01:13 ANR6913W PREPARE: Keine Datenträger mit Sicherungsdaten
im Kopienspeicherpool CSTORAGEP vorhanden.
05/03/2008 12:01:13 ANR6913W PREPARE: Keine Datenträger mit Sicherungsdaten
im Kopienspeicherpool CSTORAGEPSM vorhanden.
05/03/2008 12:01:14 ANR6920W PREPARE: Generierter Ersatzdatenträger
BACK4X@ für Einheitentyp 8MM ungültig.
Originaldatenträgername: BACK4X. Zeilengruppe
ist Makro PRIMARY.VOLUMES.REPLACEMENT.
05/03/2008 12:01:14 ANR6900I PREPARE: Wiederherstellungsplandatei
/home/guest/drmtest/prepare/plandir/DSM1509/
r.p.20080503.120113 wurde erstellt.
05/03/2008 12:01:14 ANR0985I Prozess 3 für PREPARE, der im
BACKGROUND ausgeführt wird, wurde mit Status
SUCCESS um 12:01:14 beendet.
```



```
05/03/2008 12:01:13 ANR0984I Prozess 3 für PREPARE im
BACKGROUND um 12:01:13 gestartet.
05/03/2008 12:01:13 ANR6918W PREPARE: Datei mit Wiederherstellungsanweisungen
c:\drmtest\prepare\RECOVERY.INSTRUCTIONS.DATABASE
nicht gefunden.
05/03/2008 12:01:13 ANR6918W PREPARE: Datei mit Wiederherstellungsanweisungen
c:\drmtest\prepare\RECOVERY.INSTRUCTIONS.STGPOOL
nicht gefunden.
05/03/2008 12:01:13 ANR6913W PREPARE: Keine Datenträger mit Sicherungsdaten
im Kopienspeicherpool CSTORAGEP vorhanden.
05/03/2008 12:01:13 ANR6913W PREPARE: Keine Datenträger mit Sicherungsdaten
im Kopienspeicherpool CSTORAGEPSM vorhanden.
05/03/2008 12:01:14 ANR6920W PREPARE: Generierter Ersatzdatenträger
BACK4X@ für Einheitenklasse 8MM ungültig.
Originaldatenträgername: BACK4X. Zeilengruppe
ist Makro PRIMARY.VOLUMES.REPLACEMENT.
05/03/2008 12:01:14 ANR6900I PREPARE: Wiederherstellungsplandatei
c:\drmtest\prepare\r.p.20080503.120113
wurde erstellt.
05/03/2008 12:01:14 ANR0985I Prozess 3 für PREPARE, der im
BACKGROUND ausgeführt wird, wurde mit Status
SUCCESS um 12:01:14 beendet.
```




## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für PREPARE

| Befehl            | Beschreibung  |
|-------------------|---|
| CANCEL PROCESS    | Bricht einen Serverhintergrundprozess ab.   |
| DELETE VOLHISTORY | Löscht History-Daten sequenzieller Datenträger aus der Datenträger-History-Datei. |
| QUERY DRMSTATUS   | Zeigt DRM-Systemparameter an.   |
| QUERY RPFCONTENT  | Zeigt den Inhalt einer Wiederherstellungsplandatei an.                            |
| QUERY RPFFILE     | Zeigt Informationen über Wiederherstellungsplandateien an.                        |



| Befehl                   | Beschreibung   |
|--------------------------|--|
| QUERY SERVER             | Zeigt Informationen über Server an.  |
| QUERY VOLHISTORY         | Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.                                 |
| SET DRMACTIVEDATASTGPOOL | Gibt an, dass Speicherpools für aktive Daten von DRM verwaltet werden.   |
| SET DRMCOPYSTGPOOL       | Gibt an, dass Kopierspeicherpools von DRM verwaltet werden.  |
| SET DRMINSTRPREFIX       | Gibt das Präfix des Pfadnamens für die Wiederherstellungsplananweisungen an.                                       |
| SET DRMPPLANVPOSTFIX     | Gibt die Namen der Ersatzdatenträger in der Wiederherstellungsplandatei an.  |
| SET DRMPPLANPREFIX       | Gibt das Präfix des Pfadnamens für den Wiederherstellungsplan an.  |
| SET DRMPRIMSTGPOOL       | Gibt an, dass primäre Speicherpools von DRM verwaltet werden.  |
| SET DRMRPFEXPIREDAYS     | Definiert Verfallskriterien für Wiederherstellungsplandateien.   |
| UPDATE VOLHISTORY        | Ändert Standortinformationen für einen Datenträger in der Datenträger-History-Datei oder fügt Informationen hinzu. |

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## PROTECT STGPOOL (Daten schützen, die zu einem Speicherpool gehören)

Verwenden Sie diesen Befehl, um Daten in einem Verzeichniscontainerspeicherpool zu schützen, indem eine Kopie der Daten in einem anderen Speicherpool auf einem Zielreplikationsserver oder auf demselben Server gespeichert wird und die Daten auf Band geschützt werden. Wenn Sie den Verzeichniscontainerspeicherpool schützen, können Sie später mithilfe des Befehls REPAIR STGPOOL versuchen, beschädigte Daten in dem Speicherpool zu reparieren.

Wenn Sie den Befehl PROTECT STGPOOL für einen Verzeichniscontainerspeicherpool ausgeben, werden in diesem Speicherpool gespeicherte Daten in dem Zielpool gesichert, den Sie angeben. Die Daten können in den folgenden Zielpools gesichert werden:

- Verzeichniscontainerspeicherpool auf dem Zielreplikationsserver.  
Voraussetzung: Für den Speicherpool, der geschützt wird, müssen Sie den Zielpool angeben, indem Sie den Parameter PROTECTSTGPOOL im Befehl DEFINE STGPOOL oder UPDATE STGPOOL verwenden.

Wenn Sie den Befehl PROTECT STGPOOL regelmäßig verwenden, können Sie in der Regel die Verarbeitungszeit für den Befehl REPLICATE NODE verringern. Die Datenbereiche, die bereits durch Speicherpoolschutzoperationen auf den Zielreplikationsserver kopiert wurden, werden übersprungen, wenn die Knotenreplikation gestartet wird.

Als Teil der Operation PROTECT STGPOOL können Prozesse ausgeführt werden, um beschädigte Bereiche im Speicherpool des Zielservers zu reparieren. Die Reparaturoperation wird unter den folgenden Bedingungen ausgeführt:

- Sowohl der Quellenserver als auch der Zielservers müssen über Version 7.1.5 oder eine höhere Version verfügen.
- Bereiche, die auf dem Zielservers bereits als beschädigt markiert sind, werden repariert. Der Reparaturprozess führt keinen Prüfprozess aus, um beschädigte Daten zu identifizieren.
- Nur Zielbereiche, die mit Quellbereichen übereinstimmen, werden repariert. Zielbereiche, die beschädigt sind, aber keine Entsprechung auf dem Quellenserver haben, werden nicht repariert.

Einschränkungen: Für die Reparaturoperation, die als Teil der Operation PROTECT STGPOOL ausgeführt wird, gelten die folgenden Einschränkungen:

- Bereiche, die zu verschlüsselten Objekten gehören, werden nicht repariert.
- Der Zeitpunkt des Auftretens der Beschädigung in dem Zielspeicherpool und die Reihenfolge der Befehle REPLICATE NODE und PROTECT STGPOOL können Auswirkungen darauf haben, ob der Reparaturprozess erfolgreich ist. Einige Bereiche, die mit einem Befehl REPLICATE NODE in dem Zielspeicherpool gespeichert wurden, werden möglicherweise nicht repariert.
- Durch Kopieren auf Band geschützte Containerkopierspeicherpools auf demselben Server.  
Voraussetzung: Für den Speicherpool, der geschützt wird, müssen Sie den Zielspeicherpool angeben, indem Sie den Parameter PROTECTLOCALSTGPools verwenden. Details zu dem Parameter finden Sie unter den Befehlen zum Definieren und Aktualisieren von Verzeichniscontainerspeicherpools (Befehle DEFINE STGPOOL und UPDATE STGPOOL).

Als Teil der Operation PROTECT STGPOOL können Datenträger in dem Zielpool konsolidiert werden. Der Wert des Parameters RECLAIM für den Containerkopierspeicherpool hat Auswirkungen darauf, ob Datenträger konsolidiert werden. Details zu dem Parameter finden Sie unter den Befehlen zum Definieren und Aktualisieren von Containerkopierspeicherpools (Befehle DEFINE STGPOOL und UPDATE STGPOOL).

Einschränkung: Es ist nicht möglich, eine gleichzeitige Ausführung mehrerer Operationen PROTECT STGPOOL zu planen. Warten Sie auf die Beendigung einer Operation PROTECT STGPOOL, bevor Sie eine weitere Operation starten.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax, wenn das Ziel der Replikationsserver ist

```
>>-PROTECT STGPool--Quellenspeicherpool----->
. -Type---Replserver-. .-FORCEREconcile---No-----.
>+-----+-----+-----+-----+----->
' -Type---Replserver-' ' -FORCEREconcile---No---+'
                                     '-Yes-'



(1)

. -MAXSESSions---10-----.
>+-----+-----+-----+-----+----->
' -MAXSESSions---Anzahl Sitzungen--'

. -Preview---No----- . -PURGEdata---No----- .
>+-----+-----+-----+-----+----->
' -Preview---No---+' ' -PURGEdata---No---+'
                    '-Yes-'                    '+-All-----+'
                                                '-Deleted-'

. -Wait---No----- . -TRANSFERMethod---Tcpi-----.
>+-----+-----+-----+-----+----->
' -Wait---No---+' | ' -TRANSFERMethod---Tcpi---+' (2) |
                    '-Yes-' | ' -TRANSFERMethod---Fasp---+'
                                '-Fasp--'
```

Anmerkungen:

-  Wird der Parameter TRANSFERMETHOD auf den Standardwert TCPIP gesetzt, ist der Standardwert des Parameters MAXSESSIONS 10. Wird der Parameter TRANSFERMETHOD auf FASP gesetzt, ist der Standardwert des Parameters MAXSESSIONS 2.
-  Der Parameter TRANSFERMETHOD ist nur auf Betriebssystemen Linux x86\_64 verfügbar.

## Syntax, wenn das Ziel ein Bandspeicherpool auf demselben Server ist

```
>>-PROTECT STGPool--Quellenspeicherpool--Type---Local----->
. -Preview---No----- . -RECLaim---Yes----- .
>+-----+-----+-----+-----+----->
' -Preview---No---+' ' -RECLaim---Yes-----+'
                    '-Yes-'                    '+-No-----+'
                                                '+-Only-----+'
                                                '+-YESLIMITed--+'
                                                '-ONLYLIMITed-'

. -Wait---No----- .
>+-----+-----+-----+-----+----->
' -Wait---No---+'
                    '-Yes-'
```

## Parameter

Quellenspeicherpool (Erforderlich)

Gibt den Namen des Verzeichniscontainerspeicherpools auf dem Quellenserver an.

Type

Gibt den Typ des Ziels für die Schutzoperation an. Dieser Parameter ist wahlfrei. Der Standardwert ist REPLSERVER. Geben Sie einen der folgenden Werte an:

Replserver

Gibt an, dass das Ziel der Speicherpool auf dem Zielreplikationsserver ist, der für den Quellenspeicherpool mit dem Parameter PROTECTSTGPOOL im Befehl DEFINE STGPOOL oder UPDATE STGPOOL definiert wurde.

#### Local

Gibt an, dass sich das Ziel auf demselben Server wie der Quellenspeicherpool befindet. Das Ziel ist der Containerkopierspeicherpool, der mit dem Parameter PROTECTLOCALSTGPOOLS im Befehl DEFINE STGPOOL oder UPDATE STGPOOL für den Quellenspeicherpool definiert wird.

Tipp: Standardmäßig verwendet der Server maximal zwei parallele Prozesse, um Daten in ein lokales Ziel zu kopieren. Sie können die maximale Anzahl paralleler Prozesse ändern, indem Sie den Containerkopierspeicherpool aktualisieren, der das Ziel ist. Verwenden Sie den Befehl UPDATE STGPOOL mit dem Parameter PROTECTPROCESS.

#### FORCEREconcile

Gibt an, ob die Unterschiede zwischen Datenbereichen in dem Verzeichniscontainerspeicherpool auf dem Quellenserver und dem Zielservers abgeglichen werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Geben Sie einen der folgenden Werte an:

##### No



Gibt an, dass bei der Datensicherung nicht alle Datenbereiche in dem Verzeichniscontainerspeicherpool auf dem Quellenserver mit Datenbereichen auf dem Zielserver verglichen werden. Stattdessen werden bei der Datensicherung Änderungen an den Datenbereichen auf dem Quellenserver seit der letzten Sicherung verfolgt und diese Änderungen auf dem Zielserver synchronisiert.

##### Yes

Gibt an, dass bei der Datensicherung alle Datenbereiche auf dem Quellenserver mit Datenbereichen auf dem Zielserver verglichen und die Datenbereiche auf dem Zielserver mit den Datenbereichen auf dem Quellenserver synchronisiert werden.

#### MAXSESSions

Gibt die maximale Anzahl der Datensitzungen an, die Daten an einen Zielserver senden können. Dieser Parameter ist wahlfrei. Der angegebene Wert kann im Bereich 1 - 100 liegen.

 AIX-Betriebssysteme  Windows-Betriebssysteme Der Standardwert ist 10.

 Linux-Betriebssysteme Der Standardwert variiert:

- Bei TRANSFERMETHOD=TCPIP ist der Standardwert des Parameters MAXSESSIONS 10.
- Bei TRANSFERMETHOD=FASP ist der Standardwert des Parameters MAXSESSIONS 2.

Wenn Sie die Anzahl der Sitzungen erhöhen, können Sie den Durchsatz für den Speicherpool verbessern.

Wenn Sie einen Wert für den Parameter MAXSESSIONS definieren, stellen Sie sicher, dass die verfügbare Bandbreite und die Prozessorkapazität des Quellen- und Zielservers ausreichend sind.

#### Tipps:

- Wird ein Befehl QUERY SESSION ausgegeben, kann die Gesamtzahl der Sitzungen die Anzahl der Datensitzungen überschreiten. Die Differenz resultiert aus kurzen Steuersitzungen, die zum Abfragen und Definieren von Operationen verwendet werden.
- Die Anzahl der Sitzungen, die für den Schutz verwendet werden, hängt vom Datenvolumen ab, das gesichert wird. Wird nur ein geringes Datenvolumen gesichert, wird durch die Erhöhung der Anzahl Sitzungen kein Vorteil erzielt.

#### Preview

Gibt an, ob eine Voranzeige der Daten aufgerufen werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Geben Sie einen der folgenden Werte an:

##### No

Gibt an, dass die Daten auf dem Zielserver gesichert, aber nicht vorangezeigt werden.

##### Yes

Gibt an, dass die Daten vorangezeigt, aber nicht gesichert werden.

#### PURGEdata

Gibt an, dass Datenbereiche auf dem Zielserver gelöscht werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

##### No

Gibt an, dass Datenbereiche auf dem Zielserver nicht gelöscht werden.

##### All

Gibt an, dass alle Datenbereiche auf dem Zielserver gelöscht werden. Datenbereiche, die von anderen Daten im Zielspeicherpool referenziert werden, werden nicht gelöscht.

##### Deleted

Gibt an, dass Datenbereiche, die auf dem Quellenserver gelöscht wurden, vom Zielserver gelöscht werden. Neue Datenbereiche werden nicht geschützt.

## RECLaim

Gibt an, ob die Konsolidierung ausgeführt wird, wenn der Befehl PROTECT STGPOOL verarbeitet wird. Die Konsolidierung wird für den lokalen Containerkopierspeicherpool ausgeführt, der das Ziel der Schutzoperation ist. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

### Yes

Gibt an, dass die Konsolidierung zusammen mit der Speicherpoolschutzoperation ausgeführt wird, wenn der Befehl ausgegeben wird. Die Konsolidierung wird vollständig ausgeführt; die Anzahl der Datenträger im Speicherpool, die für die Konsolidierung verarbeitet werden, ist hierbei nicht begrenzt.

### No

Gibt an, dass die Konsolidierung nicht ausgeführt wird, wenn der Befehl ausgegeben wird. Nur die Speicherpoolschutzoperation wird ausgeführt.

### Only

Gibt an, dass ausschließlich die Konsolidierung ausgeführt wird, wenn der Befehl ausgegeben wird. Die Speicherpoolschutzoperation wird nicht ausgeführt. Daten im Verzeichniscontainerspeicherpool, die seit der letzten Schutzoperation aktualisiert wurden, werden daher nicht geschützt. Die Konsolidierung wird vollständig ausgeführt; die Anzahl der Datenträger im Speicherpool, die für die Konsolidierung verarbeitet werden, ist hierbei nicht begrenzt.

### YESLIMited

Gibt an, dass die Konsolidierung zusammen mit der Speicherpoolschutzoperation ausgeführt wird, wenn der Befehl ausgegeben wird. Die Konsolidierung wird ausgeführt, bis sie den Konsolidierungsgrenzwert erreicht, der für den Containerkopierspeicherpool definiert ist. Der Konsolidierungsgrenzwert wird mit dem Parameter RECLAIMLIMIT im Befehl DEFINE STGPOOL oder UPDATE STGPOOL definiert.

### ONLYLIMited

Gibt an, dass ausschließlich die Konsolidierung ausgeführt wird, wenn der Befehl ausgegeben wird. Die Speicherpoolschutzoperation wird nicht ausgeführt. Daten im Verzeichniscontainerspeicherpool, die seit der letzten Schutzoperation aktualisiert wurden, werden daher nicht geschützt. Die Konsolidierung wird ausgeführt, bis sie den Konsolidierungsgrenzwert erreicht, der für den Containerkopierspeicherpool definiert ist. Der Konsolidierungsgrenzwert wird mit dem Parameter RECLAIMLIMIT im Befehl DEFINE STGPOOL oder UPDATE STGPOOL definiert.

## Wait

Gibt an, ob darauf gewartet werden soll, dass der Server diesen Befehl im Vordergrund verarbeitet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

### No


Gibt an, dass der Befehl im Hintergrund verarbeitet wird. Um die Hintergrundprozesse dieses Befehls zu überwachen, geben Sie den Befehl QUERY PROCESS aus.

### Yes

Gibt an, dass der Befehl im Vordergrund verarbeitet wird. Nachrichten werden erst angezeigt, wenn die Verarbeitung des Befehls beendet ist.

Einschränkung: Sie können nicht `WAIT=YES` an der Serverkonsole angeben.

## Linux-BetriebssystemeTRANSFERMethod

 Linux-BetriebssystemeGibt die Methode an, die für die Datenübertragung zwischen Servern verwendet wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

### Tcpip

Gibt an, dass TCP/IP für die Übertragung von Daten verwendet wird. Dieser Wert ist der Standardwert.

### Fasp

Gibt an, dass die Aspera FASP-Technologie (Fast Adaptive Secure Protocol) für die Übertragung von Daten verwendet wird. Mit der Aspera FASP-Technologie kann die Datenübertragung in einem Weitverkehrsnetz (WAN) optimiert werden. Wenn Sie `TRANSFERMETHOD=FASP` angeben, werden alle Parameter `TRANSFERMETHOD` überschrieben, die Sie im Befehl `DEFINE SERVER` oder `UPDATE SERVER` angegeben haben.

Einschränkungen:

- Bevor Sie die Aspera FASP-Technologie aktivieren, müssen Sie bestimmen, ob die Technologie für Ihre Systemumgebung geeignet ist, und die entsprechenden Lizenzen installieren. Anweisungen finden Sie unter [Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann](#). Wenn die Lizenzen fehlen oder abgelaufen sind, schlagen Operationen zum Schützen von Speicherpools fehl.
- Wenn die WAN-Leistung Ihre Geschäftsanforderungen erfüllt, aktivieren Sie nicht die Aspera FASP-Technologie.

## Beispiel: Alle Datenbereiche auf dem Zielserver löschen

Löschen Sie alle Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Zielserver. Der Verzeichniscontainerspeicherpool mit dem Namen POOL1 auf dem Quellenserver wird nicht mehr durch den Verzeichniscontainerspeicherpool auf dem Zielserver geschützt. Sie können alle Bereiche löschen, um den Verzeichniscontainerspeicherpool auf dem Zielserver zu bereinigen, der den Quellenserver nicht mehr schützt.

```
protect stgpool pool1 purgedata=all
```

## Beispiel: Einen Speicherpool schützen und eine maximale Anzahl Datensitzungen angeben

Schützen Sie einen Speicherpool mit dem Namen SPOOL1 auf dem Quellenserver, indem Sie die Daten auf dem Zielserver TPOOL1 sichern. Geben Sie maximal 20 Datensitzungen an.

```
update stgpool spool1 protectstgpool=tpool1  
protect stgpool spool1 maxsessions=20
```

## Beispiel: Die Speicherpooldaten auf Band kopieren

Schützen Sie einen Verzeichniscontainerspeicherpool, indem Sie die Daten in einen Containerkopierspeicherpool auf demselben Server kopieren. In diesem Beispiel hat der Verzeichniscontainerspeicherpool den Namen SPOOL1 und der Containerkopierspeicherpool, der Band für die Speicherung verwendet, den Namen TAPES1.

1. Aktualisieren Sie den Verzeichniscontainerspeicherpool, um TAPES1 als lokalen Speicherpool für den Schutz hinzuzufügen. Der Speicherpool TAPES1 muss ein Containerkopierspeicherpool sein. Geben Sie den folgenden Befehl aus:

```
update stgpool spool1 protectlocalstgpools=tapes1
```

2. Schützen Sie die Daten in dem Verzeichniscontainerspeicherpool mit einer lokalen Kopie, indem Sie den folgenden Befehl ausgeben:

```
protect stgpool type=local spool1
```

Die Daten werden in den Speicherpool TAPES1 kopiert.

## Beispiel: Speicherbereich auf Banddatenträgern vor dem Schutz eines Speicherpools konsolidieren

Konsolidieren Sie Speicherbereich auf den Banddatenträgern, die zum Schutz eines Verzeichniscontainerspeicherpools verwendet werden. Schützen Sie anschließend die Daten im Verzeichniscontainerspeicherpool. In diesem Beispiel hat der Verzeichniscontainerspeicherpool den Namen SPOOL1.

1. Konsolidieren Sie Speicherbereich im lokalen Containerkopierspeicherpool, der als Zielschutzpool für SPOOL1 definiert ist.

```
protect stgpool spool1 type=local reclaim=only
```

2. Schützen Sie die Daten im Verzeichniscontainerspeicherpool namens SPOOL1, ohne eine Konsolidierung auszuführen.

```
protect stgpool spool1 type=local reclaim=no
```

Tabelle 1. Zugehörige Befehle für PROTECT STGPOOL

| Befehl                                | Beschreibung   |
|---------------------------------------|--|
| CANCEL PROCESS                        | Bricht einen Serverhintergrundprozess ab.  |
| DEFINE STGPOOL (Containerkopie)       | Definiert einen Containerkopierspeicherpool, in dem Kopien von Daten aus einem Verzeichniscontainerspeicherpool gespeichert werden.    |
| DEFINE STGPOOL (Verzeichniscontainer) | Definiert einen Verzeichniscontainerspeicherpool.  |
| DEFINE STGPOOLDIRECTORY               | Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool.                                |
| REPAIR STGPOOL                        | Repariert einen Verzeichniscontainerspeicherpool.  |
| REPLICATE NODE                        | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |
| SET REPLSERVER                        | Gibt einen Zielreplikationsserver an.  |
| UPDATE STGPOOL (Containerkopie)       | Aktualisiert einen Containerkopierspeicherpool, in dem Kopien von Daten aus einem Verzeichniscontainerspeicherpool gespeichert werden. |

## QUERY-Befehle

Mit den QUERY-Befehlen können Informationen zu IBM Spectrum Protect-Objekten angefordert oder angezeigt werden.

- QUERY ACTLOG (Aktivitätenprotokoll abfragen)
- QUERY ADMIN (Administratorinformationen anzeigen)
- QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)
- QUERY ALERTSTATUS (Status eines Alert abfragen)
- QUERY ASSOCIATION (Zuordnung zwischen Clientknoten und Zeitplan abfragen)
- QUERY AUDITOCUPANCY (Speicherauslastung des Clientknotens abfragen)
- QUERY BACKUPSET (Sicherungsgruppe abfragen)
- QUERY BACKUPSETCONTENTS (Inhalt einer Sicherungsgruppe abfragen)
-    QUERY CLEANUP (Bereinigung abfragen, die in einem Quellenspeicherpool erforderlich ist)
- QUERY CLOPTSET (Clientoptionsgruppe abfragen)
- QUERY COLLOGROUP (Kollokationsgruppe abfragen)
- QUERY CONTENT (Inhalt eines Speicherpooldatenträgers abfragen)
-    QUERY CONTAINER (Container abfragen)
-    QUERY CONVERSION (Konvertierungsstatus eines Speicherpools abfragen)
- QUERY COPYGROUP (Kopiengruppen abfragen)
- QUERY DATAMOVER (Definitionen der Einheit zum Versetzen von Daten anzeigen)
-    QUERY DAMAGED (Beschädigte Daten in einem Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool abfragen)
- QUERY DB (Datenbankinformationen anzeigen)
- QUERY DBSPACE (Datenbankspeicherbereich anzeigen)
-    QUERY DEDUPSTATS (Dateneduplizierungsstatistikdaten abfragen)
- QUERY DEVCLASS (Informationen über Einheitenklassen anzeigen)
- QUERY DIRSPACE (Speichernutzung von FILE-Verzeichnissen abfragen)
- QUERY DOMAIN (Maßnahmendomäne abfragen)
- QUERY DRIVE (Informationen über ein Laufwerk abfragen)
- QUERY DRMEDIA (Fehlerbehebungsdatenträger abfragen)
- QUERY DRMSTATUS (Disaster Recovery Manager-Systemparameter abfragen)
- QUERY ENABLED (Aktivierte Ereignisse abfragen)
- QUERY EVENT (Geplante und abgeschlossene Ereignisse abfragen)
- QUERY EVENTRULES (Regeln für Server- oder Clientereignisse abfragen)
- QUERY EVENTSERVER (Ereignisserver abfragen)
- QUERY EXPORT (Aktive oder ausgesetzte Exportoperationen abfragen)
-    QUERY EXTENTUPDATES (Aktualisierte Datenbereiche abfragen)
- QUERY FILESPACE (Dateibereiche abfragen)
- QUERY LIBRARY (Kassettenarchiv abfragen)
- QUERY LIBVOLUME (Datenträger im Kassettenarchiv abfragen)
- QUERY LICENSE (Lizenzinformationen anzeigen)
- QUERY LOG (Informationen zum Wiederherstellungsprotokoll anzeigen)
- QUERY MACHINE (Maschineninformationen abfragen)
- QUERY MEDIA (Speicherpooldatenträger mit sequenziellem Zugriff abfragen)
- QUERY MGMTCLASS (Verwaltungsklasse abfragen)
- QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)
- QUERY MONITORSTATUS (Überwachungsstatus abfragen)
- QUERY MOUNT (Informationen zu bereitgestellten Datenträgern mit sequenziellem Zugriff anzeigen)
-    QUERY NASBACKUP (NAS-Sicherungsimages abfragen)
- QUERY NODE (Knoten abfragen)
- QUERY NODEDATA (Clientdaten auf Datenträgern abfragen)
- QUERY NODEGROUP (Knotengruppe abfragen)
- QUERY OCCUPANCY (Clientdateibereiche in Speicherpools abfragen)
- QUERY OPTION (Serveroptionen abfragen)
- QUERY PATH (Pfaddefinition anzeigen)
- QUERY POLICYSET (Maßnahmengruppe abfragen)
- QUERY PROCESS (Serverprozesse abfragen)
- QUERY PROFILE (Profil abfragen)
- QUERY PROTECTSTATUS (Status des Speicherpoolschutzes abfragen)
- QUERY PROXYNODE (Proxyberechtigung für einen Clientknoten abfragen)
- QUERY PVUESTIMATE (Prozessor-Value-Unit-Schätzung anzeigen)
- QUERY RECOVERYMEDIA (Wiederherstellungsdatenträger abfragen)
- QUERY REPLICATION (Knotenreplikationsprozesse abfragen)
- QUERY REPLNODE (Informationen zum Replikationsstatus für einen Clientknoten anzeigen)



```

>----->
  '-MSGno-----Nachrichtennummer-'

>----->
  '-Search-----Zeichenfolge-'  '-NODEname-----Knotenname-'

  .-Originator-----ALL-----
>-----<
  '-ORiginator-----+--ALL-----+-'
                    +-Server-----+
                    '-CLient--| A |- '

A

|----->
  '-OWNERname-----Eignername-'

>----->
  '-SCHedname-----Zeitplanname-'

>----->
  '-Dmainname-----Domänenname-'

>-----|
  '-SESSnum-----Sitzungsnummer-'

```

## Parameter

### BEGINDate

Gibt das Anfangsdatum des Bereichs an, für den Nachrichten angezeigt werden sollen. Es werden alle Nachrichten angezeigt, die die Zeitkriterien erfüllen und nach diesem Datum aufgetreten sind. Standardwert ist das aktuelle Datum. Dieser Parameter ist wahlfrei.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 09/15/1998   |
| TODAY                          | Das aktuelle Datum   | TODAY  |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY-7 <i>oder</i> -7.<br><br>Sollen Informationen beginnend mit den Nachrichten angezeigt werden, die vor einer Woche erstellt wurden, kann BEGINDATE=TODAY-7 oder BEGINDATE= -7 angegeben werden. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.   |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.  |

### BEGINTime

Gibt die Anfangszeit des Bereichs an, für den Nachrichten angezeigt werden sollen. Es werden alle Nachrichten angezeigt, die die Zeitkriterien erfüllen und nach dieser Uhrzeit aufgetreten sind. Wird keine Zeit angegeben, werden alle Nachrichten angezeigt, die in der letzten Stunde aufgetreten sind.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert     | Beschreibung                                       | Beispiel |
|----------|--|----------|
| HH:MM:SS | Eine bestimmte Uhrzeit am angegebenen Anfangsdatum | 10:30:08 |



| Wert                         | Beschreibung   | Beispiel   |
|------------------------------|--|--|
| NOW                          | Die aktuelle Uhrzeit am angegebenen Anfangsdatum                               | NOW  |
| NOW+HH:MM <i>oder</i> +HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Anfangsdatum  | NOW+03:00 <i>oder</i> +03:00.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTIME=NOW+3 <i>oder</i> BEGINTIME=+3 ausgegeben, zeigt IBM Spectrum Protect Nachrichten mit der Uhrzeit 12:00 Uhr oder später am Anfangsdatum an.                 |
| NOW-HH:MM <i>oder</i> -HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Anfangsdatum | NOW-04:00 <i>oder</i> -04:00.<br><br>Wird der Befehl QUERY ACTLOG um 9:00 Uhr mit der Angabe BEGINTime=NOW-3:30 <i>oder</i> BEGINTime= -3:30 ausgegeben, zeigt IBM Spectrum Protect Nachrichten mit der Uhrzeit 5:30 Uhr oder später am Anfangsdatum an. |

#### ENDDate

Gibt das Enddatum des Bereichs an, für den Nachrichten angezeigt werden sollen. Es werden alle Nachrichten angezeigt, die die Zeitkriterien erfüllen und vor dem Enddatum aufgetreten sind. Wird kein Wert angegeben, wird das aktuelle Datum verwendet.

Dieser Parameter ist wahlfrei.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                           | Beschreibung   | Beispiel  |
|--------------------------------|--|---|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 09/15/1998  |
| TODAY                          | Das aktuelle Datum   | TODAY   |
| TODAY-Tage <i>oder</i> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY-1 <i>oder</i> -1.<br><br>Sollen Informationen angezeigt werden, die bis gestern erstellt wurden, kann ENDDATE=TODAY-1 <i>oder</i> einfach ENDDATE= -1 angegeben werden. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM  |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.  |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM  |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.   |

#### ENDTime

Gibt die Endzeit des Bereichs an, für den Nachrichten angezeigt werden sollen. Es werden alle Nachrichten angezeigt, die die Zeitkriterien erfüllen und vor dieser Uhrzeit aufgetreten sind. Wird kein Wert angegeben, werden alle Nachrichten angezeigt, die bis zum Zeitpunkt der Ausgabe dieses Befehls aufgetreten sind. Dieser Parameter ist wahlfrei.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert     | Beschreibung                                   | Beispiel |
|----------|--|----------|
| HH:MM:SS | Eine bestimmte Uhrzeit am angegebenen Enddatum | 10:30:08 |
| NOW      | Die aktuelle Uhrzeit am angegebenen Enddatum   | NOW      |

| Wert                            | Beschreibung   | Beispiel   |
|---------------------------------|--|--|
| NOW+HH:MM <i>oder</i><br>+HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum  | NOW+03:00 <i>oder</i> +03:00.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW+3:00 oder ENDTIME= +3:00 ausgegeben, zeigt IBM Spectrum Protect Nachrichten mit der Uhrzeit 12:00 Uhr oder früher am angegebenen Enddatum an. |
| NOW-HH:MM <i>oder</i> -HH:MM    | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum | NOW-03:30 <i>oder</i> -03:30.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW-3:30 oder ENDTIME= -3:30 ausgegeben, zeigt IBM Spectrum Protect Nachrichten mit der Uhrzeit 5:30 Uhr oder früher am angegebenen Enddatum an.  |

#### MSGno

Gibt eine ganze Zahl an, die die Nachrichtennummer der aus dem Aktivitätenprotokoll anzuzeigenden Nachricht definiert. Diese ganze Zahl ist nur der numerische Teil der Nachricht. Dieser Parameter ist wahlfrei.

#### Search

Gibt eine Zeichenfolge an, nach der im Aktivitätenprotokoll gesucht werden soll. Die Zeichenfolge in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Sie können Text und ein Platzhalterzeichen verwenden, um diese Zeichenfolge anzugeben. Dieser Parameter ist wahlfrei.

Anmerkung: Geben Sie als Zeichenfolge nicht den IBM Spectrum Protect-Servernamen oder Text und ein Platzhalterzeichen an, mit dem der Servername gefunden würde. Die Ausgabe enthält sonst Nachrichten, die den Suchbegriff nicht enthalten.

#### NODENAME

Gibt an, dass die Abfrage Nachrichten anzeigt, die für diesen Knoten protokolliert wurden. Wird kein Wert für diesen Parameter angegeben, werden Nachrichten für alle Knoten angezeigt.

#### ORIGINATOR

Gibt an, dass die Abfrage Nachrichten anzeigt, die vom Server und/oder Client protokolliert wurden. Standardwert ist ALL. Gültige Werte:

#### ALL

Gibt an, dass die Abfrage Nachrichten anzeigt, die vom Client und vom Server stammen.

#### SERVER

Gibt an, dass die Abfrage Nachrichten anzeigt, die vom Server stammen.

#### CLIENT

Gibt an, dass die Abfrage Nachrichten anzeigt, die vom Client stammen.

Es kann einer der folgenden Werte angegeben werden, um die Verarbeitungszeit zu minimieren, wenn das Aktivitätenprotokoll nach Nachrichten abgefragt wird, die vom Client protokolliert wurden:

#### OWNERNAME

Gibt an, dass die Abfrage Nachrichten anzeigt, die für einen bestimmten Eigner protokolliert wurden. Wird kein Wert für diesen Parameter angegeben, werden Nachrichten für alle Eigner angezeigt.

#### SCHEDNAME

Gibt an, dass die Abfrage Nachrichten anzeigt, die für eine bestimmte geplante Clientaktivität protokolliert wurden. Wird kein Wert für diesen Parameter angegeben, werden Nachrichten für alle Zeitpläne angezeigt.

#### DOMAINNAME

Gibt an, dass die Abfrage Nachrichten anzeigt, die für eine bestimmte Maßnahmendomäne protokolliert wurden, zu der ein angegebener Zeitplan gehört. Dieser Parameter ist wahlfrei, es sei denn, es wird ein Zeitplanname angegeben.

#### SESSNUM

Gibt an, dass die Abfrage Nachrichten anzeigt, die aus einer bestimmten Clientsitzung protokolliert wurden. Wird kein Wert für diesen Parameter angegeben, werden Nachrichten für alle Clientsitzungen angezeigt.

## Beispiel: Das Aktivitätenprotokoll nach Nachrichten mit bestimmtem Text durchsuchen

Das Aktivitätenprotokoll nach allen Nachrichten durchsuchen, die die Zeichenfolge "löschen" enthalten. Die Ausgabe schließt nur die Nachrichten mit ein, die während der letzten Stunde ausgegeben wurden. Den folgenden Befehl ausgeben:

```
query actlog search=löschen
```

```
Datum/Uhrzeit      Nachricht
-----
08/27/1998 15:19:43 ANR0812I Verfallsprozess für Bestandsdateien
                    abgeschlossen: 0 Dateien wurden gelöscht.
```

## Beispiel: Das Aktivitätenprotokoll nach Nachrichten innerhalb eines bestimmten Zeitrahmens durchsuchen

---

Nachrichten anzeigen, die gestern zwischen 9:30 Uhr und 12:30 Uhr aufgetreten sind. Den folgenden Befehl ausgeben:

```
query actlog begindate=today-1
begintime=09:30:00 endtime=12:30:00
```

| Datum/Uhrzeit       | Nachricht   |
|---------------------|---|
| 10/21/1998 10:52:36 | ANR0407I Sitzung 3921 für Administrator ADMIN gestartet (WebBrowser) (HTTP 9.115.20.100(2315)). |
| 10/21/1998 11:06:08 | ANR0405I Sitzung 3922 für Administrator ADMIN beendet (WebBrowser).                             |
| 10/21/1998 12:16:50 | ANR0405I Sitzung 3934 für Administrator ADMIN beendet (WebBrowser).                             |

## Beispiel: Das Aktivitätenprotokoll nach Nachrichten von einem bestimmten Clientknoten durchsuchen

---

Das Aktivitätenprotokoll nach IBM Spectrum Protect-Nachrichten vom Client für Knoten JEE durchsuchen. Den folgenden Befehl ausgeben:

```
query actlog originator=client node=jee
```

| Datum/Uhrzeit       | Nachricht  |
|---------------------|--|
| 06/10/1998 15:46:22 | ANE4007E (Sitzungsnummer: 3 Knoten: JEE) Fehler beim Verarbeiten von '/jee/report.out': Zugriff auf Objekt wird verweigert |
| 06/11/1998 15:56:56 | ANE4009E (Sitzungsnummer: 4 Knoten: JEE) Fehler beim Verarbeiten von '/jee/work.lst': Platte vollständig belegt.           |

## Beispiel: Das Aktivitätenprotokoll nach Client- und Servernachrichten von einem bestimmten Clientknoten und einer bestimmten Sitzung durchsuchen

---

Das Aktivitätenprotokoll nach IBM Spectrum Protect-Nachrichten vom Client und Server für Knoten A, der der Sitzung 1 zugeordnet ist, durchsuchen. Die Ausgabe umfasst alle Nachrichten mit der definierten Zeichenfolge "SITZUNG: 1". Den folgenden Befehl ausgeben:

```
query actlog search="(SITZUNG:1)"
```

| Datum/Uhrzeit       | Nachricht   |
|---------------------|---|
| 02/13/2012 12:13:42 | ANR0406I Sitzung 1 für Knoten A gestartet (WinNT) (Tcp/Ip colind(2463)). (SITZUNG: 1)                   |
| 02/13/2012 12:13:56 | ANE4952I (ANE4985I Sitzung: 1, ANE4986I Knoten: A) Gesamtzahl geprüfter Objekte: 34 (SITZUNG: 1)        |
| 02/13/2012 12:13:56 | ANE4954I (ANE4985I Sitzung: 1, ANE4986I Knoten: A) Gesamtzahl gesicherter Objekte: 34 (SITZUNG: 1)      |
| 02/13/2012 12:13:56 | ANE4958I (ANE4985I Sitzung: 1, ANE4986I Knoten: A) Gesamtzahl aktualisierter Objekte: 0 (SITZUNG: 1)    |
| 02/13/2012 12:13:56 | ANE4964I (ANE4985I Sitzung: 1, ANE4986I Knoten: A) Abgelaufene Verarbeitungszeit: 00:00:02 (SITZUNG: 1) |
| 02/13/2012 12:13:59 | ANR0403I Sitzung 1 für Knoten A beendet (WinNT). (SITZUNG: 1)   |

## Beispiel: Das Aktivitätenprotokoll nach Clientnachrichten aus einer Clientsitzung durchsuchen

---

Das Aktivitätenprotokoll nach IBM Spectrum Protect-Nachrichten aus einer bestimmten Clientsitzung durchsuchen. Die Ausgabe umfasst nur Nachrichten, die vom Client generiert wurden. Den folgenden Befehl ausgeben:

```
query actlog sessnum=1
```

| Datum/Uhrzeit       | Nachricht   |
|---------------------|---|
| 02/13/2012 12:13:56 | ANE4952I (ANE4985I Sitzung: 1, ANE4986I Knoten: A) Gesamtzahl geprüfter Objekte: 34 |

```

(SITZUNG: 1)
02/13/2012 12:13:56 ANE4954I (ANE4985I Sitzung: 1, ANE4986I Knoten: A)
Gesamtzahl gesicherter Objekte: 34
(SITZUNG: 1)
02/13/2012 12:13:56 ANE4958I (ANE4985I Sitzung: 1, ANE4986I Knoten: A)
Gesamtzahl aktualisierter Objekte: 0
(SITZUNG: 1)
02/13/2012 12:13:56 ANE4964I (ANE4985I Sitzung: 1, ANE4986I Knoten: A)
Abgelaufene Verarbeitungszeit: 00:00:02
(SITZUNG: 1)

```

## Feldbeschreibungen

### Datum/Uhrzeit

Gibt das Datum und die Uhrzeit an, an dem bzw. zu der die Nachricht vom Server oder Client generiert wurde.

### Nachricht

Gibt die Nachricht an, die vom Server oder Client generiert wurde.

## Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für QUERY ACTLOG

| Befehl              | Beschreibung  |
|---------------------|---|
| SET ACTLOGRETENTION | Gibt die Anzahl Tage an, die Protokollsätze im Aktivitätenprotokoll aufbewahrt werden sollen. |

## QUERY ADMIN (Administratorinformationen anzeigen)

Mit diesem Befehl können Informationen zu einem oder zu mehreren Administratoren angezeigt werden.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```

. -*----- .
>>-Query Admin----->
      '-Administratorname-'

>+----->
|          .-,----- . |
|          v              | |
| '-Classes-----+System-----+'
|          +-Policy---+
|          +-Storage---+
|          +-Operator--+
|          '-Node-----'

.-Format-----Standard----- .
>+----->
| '-Format-----+Standard-+-'
|          '-Detailed-'

>+----->
| '-AUTHentication--++-Local-+-' | '-Alerts-----+Yes-+-'
|          '-Ldap--' |          '-No--'

```

## Parameter

### Administratorname

Gibt den Namen des Administrators an, für den Informationen angezeigt werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird für diesen Parameter kein Wert angegeben, werden alle Administratoren angezeigt.

### Classes

Gibt an, dass die Ausgabe auf Administratoren beschränkt werden soll, die über die angegebenen Berechtigungsklassen verfügen. Dieser Parameter ist wahlfrei. Es können mehrere Berechtigungsklassen in einer Liste angegeben werden, indem die Namen ohne

Leerzeichen durch Kommas voneinander getrennt werden. Wird kein Wert für diesen Parameter angegeben, werden unabhängig von der Berechtigungsklasse Informationen zu allen Administratoren angezeigt. Gültige Werte:

#### System

Informationen über Administratoren mit Systemberechtigung anzeigen.

#### Policy

Informationen über Administratoren mit Maßnahmenberechtigung anzeigen.

#### STorage

Informationen über Administratoren mit Speicherberechtigung anzeigen.

#### Operator

Informationen über Administratoren mit Bedienerberechtigung anzeigen.

#### Node

Informationen über Benutzer mit Client-Knotenberechtigung anzeigen.

#### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

##### Standard

Gibt an, dass Teilinformationen für die angegebenen Administratoren angezeigt werden.

##### Detailed

Gibt an, dass die gesamten Informationen für die angegebenen Administratoren angezeigt werden.

#### Authentication

Gibt die Kennwortauthentifizierungsmethode für den Administrator an.

##### Local

Zeigt die Administratoren an, die sich mit dem IBM Spectrum Protect-Server authentifizieren.

##### LDap

Zeigt die Administratoren an, die sich mit einem LDAP-Verzeichnisserver authentifizieren. Bei dem Administratorkennwort muss die Groß-/Kleinschreibung beachtet werden.

#### Alert

Gibt an, ob Alerts an die E-Mail-Adresse eines Administrators gesendet werden.

##### Yes

Gibt an, dass Alerts an die E-Mail-Adresse des angegebenen Administrators gesendet werden.

##### No

Gibt an, dass Alerts nicht an die E-Mail-Adresse des angegebenen Administrators gesendet werden. Dies ist der Standardwert.

Tipp: Die Alertüberwachung muss aktiviert sein und die E-Mail-Einstellungen müssen korrekt definiert sein, damit Alerts erfolgreich als E-Mail empfangen werden können. Um die aktuellen Einstellungen anzuzeigen, geben Sie den Befehl QUERY MONITORSETTINGS aus.

## Beispiel: Informationen zu allen Administratoren anzeigen

---

Teilinformationen zu allen Administratoren anzeigen. Den folgenden Befehl ausgeben:

```
query admin
```

| Administrator-<br>name | Tage seit<br>ltzt. Zugriff | Tage seit<br>Kennwort-<br>vergabe | Gesperrt | Berechtigungs-<br>klasse |
|------------------------|----------------------------|-----------------------------------|----------|--------------------------|
| ADMIN                  | <1                         | <1                                | No       | System                   |
| SERVER_CONSOLE         |                            |                                   | No       | System                   |

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Beispiel: Vollständige Informationen zu einem Administrator anzeigen

---

Von einem verwalteten Server aus vollständige Informationen für den Administrator ADMIN anzeigen. Den folgenden Befehl ausgeben:

```
query admin admin format=detailed
```

```
Administratorname: ADMIN
Letzter Zugriff: 1998.06.04 17.10.52
Tage seit letztem Zugriff: <1
Datum/Zeit der Kennwortvergabe: 1998.06.04 17.10.52
Tage seit Kennwortvergabe: 26
```

```

Zahl der ungültigen Anmeldeversuche: 0
      Gesperrt?: No
      Kontaktinformationen:
        Systemberechtigung: Yes
        Maßnahmenberechtigung: **Enthalten in Systember.**
        Speicherberechtigung: **Enthalten in Systember.**
        Bedienerberechtigung: **Enthalten in Systember.**
      Client-Zugriffsberechtigung: **Enthalten in Systember.**
      Client-Eigenerberechtigung: **Enthalten in Systember.**
      Registriert am: 05/09/1998 23:54:20
      Registriert durch: SERVER_CONSOLE
      Verwaltendes Profil:
        Kennwortablaufdauer: 90 Tag(e)
        E-Mail-Adresse:
      Alerts als E-Mail senden: Yes
      Authentifizierung: Local
      SSL erforderlich: No
      Sitzungssicherheit: Strict
      Transportmethode: TLS 1.2

```

Für Felddesreibungen siehe Felddesreibungen.

## Felddesreibungen

---

### Administratorname

Gibt den Namen des Administrators an.

### Letzter Zugriff

Gibt an, wann der Administrator zuletzt auf den Server zugegriffen hat (Datum und Uhrzeit).

### Tage seit letztem Zugriff

Gibt die Anzahl Tage seit des letzten Zugriffs des Administrators auf den Server an.

### Datum/Zeit der Kennwortvergabe

Gibt an, wann das Kennwort des Administrators definiert bzw. zuletzt aktualisiert wurde (Datum und Uhrzeit).

### Tage seit Kennwortvergabe

Gibt die Anzahl Tage seit der Definition oder der letzten Aktualisierung des Administratorkennworts an.

### Zahl der ungültigen Anmeldeversuche

Gibt die Anzahl der ungültigen Anmeldeversuche an, die seit der letzten erfolgreichen Anmeldung unternommen wurden. Diese Anzahl kann nur ungleich Null sein, wenn das Limit für ungültige Kennworteingaben (SET INVALIDPWLIMIT) größer Null ist. Entspricht die Anzahl der ungültigen Versuche dem durch den Befehl SET INVALIDPWLIMIT definierten Limit, wird der betreffende Administrator gesperrt.

### Gesperrt?

Gibt an, ob der Administrator für das System gesperrt ist.

### Kontaktinformationen

Gibt Kontaktinformationen für den Administrator an.

### Systemberechtigung

Gibt an, ob dem Administrator Systemberechtigung erteilt wurde.

### Maßnahmenberechtigung

Gibt an, ob dem Administrator uneingeschränkte Maßnahmenberechtigung erteilt wurde, oder gibt die Namen der Maßnahmendomänen an, die der Administrator mit eingeschränkter Maßnahmenberechtigung verwalten kann.

### Speicherberechtigung

Gibt an, ob dem Administrator uneingeschränkte Speicherberechtigung erteilt wurde, oder gibt die Namen der Speicherpools an, die der Administrator mit eingeschränkter Speicherberechtigung verwalten kann.

### Bedienerberechtigung

Gibt an, ob dem Administrator Bedienerberechtigung erteilt wurde.

### Clientzugriffsberechtigung

Gibt an, dass einem Benutzer mit Knotenberechtigung Clientzugriffsberechtigung erteilt wurde.

### Clienteigenerberechtigung

Gibt an, dass einem Benutzer mit Knotenberechtigung Clienteigenerberechtigung erteilt wurde.

### Registriert am

Gibt an, wann der Administrator registriert wurde (Datum und Uhrzeit).

### Registriert durch

Gibt den Namen des Administrators an, der den Administrator registriert hat. Enthält dieses Feld \$\$CONFIG\_MANAGER\$\$, ist der Administrator einem Profil zugeordnet, das von dem Konfigurationsmanager verwaltet wird.

### Verwaltendes Profil

Gibt die Profile an, für die der verwaltete Server subskribiert hat, um die Definition dieses Administrators zu erhalten.

### Kennwortablaufdauer

Gibt die Ablaufdauer des Administratorkennworts an.

### E-Mail-Adresse

Gibt die E-Mail-Adresse für den Administrator an.

Alerts als E-Mail senden

Gibt an, ob Alerts als E-Mail an den angegebenen Administrator gesendet werden.

Authentifizierung

Gibt die Kennwortauthentifizierungsmethode an: LOCAL, LDAP oder LDAP (künftig).

| Authentifizierungsziel   | Authentifizierungsmethode |
|--|---------------------------|
| IBM Spectrum Protect-Server  | LOCAL                     |
| LDAP-Verzeichnissever  | LDAP                      |
| Dieser Administrator ist für die Authentifizierung mit einem LDAP-Verzeichnissever konfiguriert, aber der Administrator hat sich noch nicht über einen Clientknoten authentifiziert. | LDAP (künftig)            |

SSL erforderlich (veraltet)

Gibt an, ob die Sicherheitseinstellung für die Administrator-ID das Protokoll Secure Sockets Layer (SSL) erfordert. Die gültigen Werte sind YES, NO oder Default. Sie müssen über die Berechtigung auf Systemebene verfügen, um die Einstellung von SSLREQUIRED für den Administrator zu aktualisieren. Dieser Parameter wird nicht mehr verwendet.

Sitzungssicherheit

Gibt die Stufe der Sitzungssicherheit an, die für die Administrator-ID durchgesetzt wird. Die gültigen Werte sind STRICT und TRANSITIONAL.

Transportmethode

Gibt die Transportmethode an, die zuletzt für den angegebenen Administrator verwendet wurde. Die gültigen Werte sind TLS 1.2, TLS 1.1 und NONE. Ein Fragezeichen (?) wird angezeigt, bis eine erfolgreiche Authentifizierung ausgeführt wird.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY ADMIN

| Befehl             | Beschreibung   |
|--------------------|--|
| GRANT AUTHORITY    | Ordnet einem Administrator Berechtigungsklassen zu.  |
| QUERY NODE         | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.                                      |
| QUERY STATUS       | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.   |
| REGISTER ADMIN     | Definiert einen neuen Administrator, ohne Administratorberechtigung zu erteilen.                                       |
| REMOVE ADMIN       | Löscht einen Administrator aus der Liste der registrierten Administratoren.  |
| RENAME ADMIN       | Ändert den Namen eines IBM Spectrum Protect-Administrators.  |
| RESET PASSEXP      | Setzt die Kennwortablaufdauer für Knoten oder Administratoren zurück.  |
| REVOKE AUTHORITY   | Widerruft eine oder mehrere Berechtigungsklassen oder schränkt den Zugriff auf Maßnahmendomänen und Speicherpools ein. |
| SET INVALIDPWLIMIT | Definiert die Anzahl ungültiger Anmeldeversuche, die zulässig sind, bevor ein Knoten gesperrt wird.                    |
| SET MINPWLENGTH    | Legt die Mindestlänge für Clientkennwörter fest.   |
| SET PASSEXP        | Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.                                     |

## QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)

Verwenden Sie diesen Befehl, um die Servernachrichten anzuzeigen, die als Alerts definiert sind.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-Query ALERTTrigger-----+-----<
      .-*-----+
      '---Nachrichtenummer---'
```

## Parameter

### Nachrichtenummer

Gibt die Nachrichtenummer an, die abgefragt werden soll. Geben Sie mehrere Nachrichtenummern durch Kommas getrennt und ohne Leerzeichen an. Nachrichtenummern haben eine maximale Länge von acht Zeichen. Platzhalterzeichen können verwendet werden, um Nachrichtenummern anzugeben. Wenn Sie keine Nachrichtenummer angeben, werden alle Alertauslöser angezeigt.

## Alertauslöser abfragen, um die Nachrichten anzuzeigen, die als Alerts angegeben sind

Mit dem folgenden Befehl alle Nachrichten anzeigen, die als Alerts angegeben sind:

```
query alerttrigger
```

### Beispielausgabe:

| Alertauslöser | Kategorie | Administrator                    |
|---------------|-----------|----------------------------------|
| ANR1067E      | SERVER    | HARRYH                           |
| ANR1073E      | SERVER    | CSDADMIN, DJADMIN, HARRYH        |
| ANR1074E      | STORAGE   | CSDADMIN, DJADMIN, HARRYH        |
| ANR1096E      | STORAGE   | CSDADMIN, DJADMIN, HARRYH, MHAYE |

## Alertauslöser nach einer bestimmten Nachrichtenummer abfragen

Den folgenden Befehl ausgeben, um alle Alertauslöser anzuzeigen, für die die Nachrichtenummer ANR1067E angegeben ist:

```
query alerttrigger ANR1067E
```

### Beispielausgabe:

| Alertauslöser | Kategorie | Administrator |
|---------------|-----------|---------------|
| ANR1067E      | SERVER    | HARRYH        |

## Feldbeschreibungen

### Alertauslöser

Die Nachrichtenummer für den Alertauslöser.

### Kategorie

Die Kategorie des Alertauslösers.

### Administrator

Der Name des Administrators, der Alerts von diesem Alertauslöser empfängt.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY ALERTTRIGGER

| Befehl  | Beschreibung  |
|---|---|
| DEFINE ALERTTRIGGER (Alertauslöser definieren)                    | Ordnet angegebene Nachrichten einem Alertauslöser zu.                   |
| DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen) | Entfernt eine Nachrichtenummer, die einen Alert auslösen kann.          |
| QUERY ALERTSTATUS (Status eines Alert abfragen)                   | Zeigt Informationen zu Alerts an, die auf dem Server ausgegeben wurden. |
| UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)     | Aktualisiert die Attribute eines oder mehrerer Alertauslöser.           |
| UPDATE ALERTSTATUS (Status eines Alert aktualisieren)             | Aktualisiert den Status eines zurückgemeldeten Alert.                   |

## QUERY ALERTSTATUS (Status eines Alert abfragen)





Der Alert wird als Bestandskategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die der Datenbank, der aktiven Protokolldatei oder der Archivprotokolldatei zugeordnet sind.

Anmerkung: Die Kategorie `CATalog` wird anstelle von `INventory` in Alerts von Servern verwendet, für die kein Upgrade auf IBM Spectrum Protect 7.1.0 oder höher durchgeführt wurde.

#### Client

Der Alert wird als Clientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die allgemeinen Clientaktivitäten zugeordnet sind.

#### DEvice

Der Alert wird als Einheitenkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Einheitenklassen, Kassettenarchiven, Laufwerken oder Pfaden zugeordnet sind.

#### SErver

Der Alert wird als allgemeine Serverkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die allgemeinen Serveraktivitäten oder -ereignissen zugeordnet sind.

#### STorage

Der Alert wird als Speicherkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Speicherpools zugeordnet sind.

#### SYstems

Der Alert wird als Systemclientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Systemsicherungs- und -archivierungsclients oder HSM-Clients zugeordnet sind.

#### VMclient

Der Alert wird als VM-Clientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die VM-Clients zugeordnet sind.

#### SOURCEType

Gibt den Quellentyp an, der abgefragt wird. Geben Sie einen der folgenden Werte an:

##### Local

Zeigt Alerts an, die von dem lokalen IBM Spectrum Protect-Server stammen.

##### Client

Zeigt Alerts an, die von dem IBM Spectrum Protect-Client stammen.

##### REmote

Zeigt Alerts an, die von einem anderen IBM Spectrum Protect-Server stammen.

#### SOURCENAME

Gibt den Namen der Quelle an, von der der Alert stammt. SOURCENAME kann der Name eines lokalen oder fernen IBM Spectrum Protect-Servers oder eines IBM Spectrum Protect-Clients sein.

#### ID

Dieser optionale Parameter gibt die eindeutige ID des Alert an, der angezeigt werden soll. Geben Sie einen Wert von 1 bis 9223372036854775807 an.

#### ASSigned

Gibt den Namen des Administrators an, dem der Alert zugeordnet ist, der abgefragt werden soll.

#### RESolvedby

Gibt den Namen des Administrators an, der den Alert behoben hat, der abgefragt werden soll.

## Aktive Alerts abfragen

---

Den folgenden Befehl ausgeben, um nur Alerts anzuzeigen, die in der Serverdatenbank aktiv sind:

```
query alertstatus status=active
```

## Aktive Alerts für zwei Nachrichten abfragen, die vom lokalen Server ausgegeben wurden

---

Den folgenden Befehl ausgeben, um nur aktive Alerts für die Nachrichtennummern ANE4958I und ANR4952E anzuzeigen, die vom lokalen Server ausgegeben wurden:

```
query alertstatus msgnum=4958,4952 status=active sourcetype=local
```

## Aktive Alerts für die Nachrichten ANR4958I und ANR4952E abfragen, die von einem Client ausgegeben wurden

---

Den folgenden Befehl ausgeben, um nur aktive Alerts für die Nachrichtennummern ANE4958I und ANE4952I anzuzeigen, die von einem Client ausgegeben wurden:

```
query alertstatus msgnum=4958,4952 status=active sourcetype=client
```

## Alle Alerts auf einem Server abfragen

---

Den folgenden Befehl ausgeben, um alle Alerts auf dem Server anzuzeigen:

```
query alertstatus
```

Beispielausgabe: Alle Alerts auf dem Server anzeigen

```
Alert-ID: 83
Alertnachrichtenummer: 293
  Quellename: SEDONA
  Quellentyp: LOCAL
  Erstes Auftreten: 03/07/2013 17:08:35
  Letztes Auftreten: 03/07/2013 17:08:35
    Anzahl: 1
    Status: ACTIVE
  Letzte Statusänderung: 12/31/1969 17:00:00
  Kategorie: INVENTORY
  Nachricht: ANR0293I Reorganisation für Tabelle AF_BITFILES gestartet.
  Zugeordnet:
  Behoben von:
  Anmerkung:

Alert-ID: 85
Alertnachrichtenummer: 293
  Quellename: SEDONA
  Quellentyp: LOCAL
  Erstes Auftreten: 03/08/2013 05:45:00
  Letztes Auftreten: 03/08/2013 05:45:00
    Anzahl: 1
    Status: ACTIVE
  Letzte Statusänderung: 12/31/1969 17:00:00
  Kategorie: INVENTORY
  Nachricht: ANR0293I Reorganisation für Tabelle BF_AGGREGATED_BITFILES gestartet.
  Zugeordnet:
  Behoben von:
  Anmerkung:

Alert-ID: 1282
Alertnachrichtenummer: 293
  Quellename: ALPINE
  Quellentyp: LOCAL
  Erstes Auftreten: 02/13/2013 15:47:50
  Letztes Auftreten: 02/13/2013 15:47:50
    Anzahl: 1
    Status: CLOSED
  Letzte Statusänderung: 02/26/2013 09:46:39
  Kategorie: INVENTORY
  Nachricht: ANR0293I Reorganisation für Tabelle TSMON_ALERT gestartet.
  Zugeordnet:
  Behoben von:
  Anmerkung:

Alert-ID: 1792
Alertnachrichtenummer: 293
  Quellename: ALPINE
  Quellentyp: LOCAL
  Erstes Auftreten: 02/19/2013 08:58:14
  Letztes Auftreten: 02/19/2013 08:58:14
    Anzahl: 1
    Status: CLOSED
  Letzte Statusänderung: 03/01/2013 12:39:21
  Kategorie: INVENTORY
  Nachricht: ANR0293I Reorganisation für Tabelle ACTIVITY_LOG gestartet.
  Zugeordnet:
  Behoben von:
  Anmerkung:
```

## Feldbeschreibungen

---

### Alert-ID

Die eindeutige ID für den Alert.

### Alertnachrichtenummer

Die Nachrichtenummer für den Alert.

### Quellename

Der Name der Quelle, aus der der Alert stammte.

### Quellentyp



Gibt den Namen der Maßnahmendomäne an, die angezeigt werden soll. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben. Alle übereinstimmenden Maßnahmendomännennamen werden angezeigt. Wird kein Wert für diesen Parameter angegeben, werden alle vorhandenen Maßnahmendomänen abgefragt. Wird ein Domänenname angegeben, ist kein Zeitplanname erforderlich.

**Zeitplanname**

Gibt den Namen des Zeitplans an, der angezeigt werden soll. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben. Alle übereinstimmenden Zeitplannamen werden angezeigt. Wird kein Wert für diesen Parameter angegeben, werden alle vorhandenen Zeitpläne abgefragt. Wird ein Zeitplanname angegeben, ist gleichzeitig auch ein Domänenname erforderlich.

## Beispiel: Clientknoten anzeigen, die einem Zeitplan zugeordnet sind

Alle Client-Knoten anzeigen, die allen Zeitplänen zugeordnet sind, die zu der Maßnahmendomäne EMPLOYEE\_RECORDS gehören. Den folgenden Befehl ausgeben:

```
query association employee_records *

      Name der Maßnahmendomäne: EMPLOYEE_RECORDS
      Zeitplanname: WEEKLY_BACKUP
      Zugeordnete Knoten: JOE JOHNSON LARRY SMITH SMITHERS TOM
```

Für Felddesreibungen siehe Felddesreibungen.

## Felddesreibungen

**Name der Maßnahmendomäne**

Gibt den Namen der Maßnahmendomäne an, zu der der Zeitplan gehört.

**Zeitplanname**

Gibt den Namen des Zeitplans an.

**Zugeordnete Knoten**

Gibt die Namen der Client-Knoten an, die dem angegebenen Zeitplan zugeordnet sind.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY ASSOCIATION

| Befehl             | Beschreibung  |
|--------------------|---|
| DEFINE ASSOCIATION | Ordnet Clients einem Zeitplan zu.                         |
| DELETE ASSOCIATION | Löscht die Zuordnung zwischen Clients und einem Zeitplan. |

## QUERY AUDITOCUPANCY (Speicherauslastung des Clientknotens abfragen)

Mit diesem Befehl können Informationen über die Server-Speicherauslastung des Client-Knotens angezeigt werden. Sollen aktuelle Lizenzprüfungsinformationen vom Server angezeigt werden, den Befehl AUDIT LICENSE verwenden, bevor der Befehl QUERY AUDITOCUPANCY ausgegeben wird.

Als Teil einer Lizenzprüfung berechnet der Server den Umfang des belegten Sicherungs-, Archivierungs- und Speicherverwaltungsspeichers nach Knoten. Bei Servern, die umfangreiche Datenmengen verwalten, kann diese Berechnung sehr viel Prozessorzeit beanspruchen und andere Serveraktivitäten blockieren. Mit der Serveroption AUDITSTORAGE kann angegeben werden, dass bei der Lizenzprüfung der Speicher nicht berechnet werden soll.

Mit Hilfe der Informationen aus dieser Abfrage kann festgestellt werden, ob und wo die Speicherauslastung des Clientknotens ausgeglichen werden muss. Diese Informationen können auch für die Berechnung der Speicherbelegungskosten für Clients verwendet werden.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-Query AUDITOccupancy-+-+-----+----->
      | .,------. |
      | v           | |
      |---Knotename-+-'
```





## Parameter

### Knotenname oder Knotengruppenname

Gibt den Namen des Clientknotens und der Knotengruppen an, dessen bzw. deren Daten in der Sicherungsgruppe enthalten sind, die angezeigt werden soll. Sollen mehrere Knotennamen und Knotengruppenamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Sie können Platzhalterzeichen für Knotennamen, aber nicht für Knotengruppenamen verwenden.

### Sicherungsgruppenname

Gibt den Namen der Sicherungsgruppe an, deren Informationen angezeigt werden sollen. Der angegebene Sicherungsgruppenname kann Platzhalterzeichen enthalten. Es können mehrere Sicherungsgruppenamen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden.

### BEGINDate

Gibt das Anfangsdatum des Bereichs an, in den das zeitpunktgesteuerte Datum der Sicherungsgruppe, die angezeigt werden soll, fallen muss. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter BEGINTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird ein Anfangsdatum ohne eine Anfangszeit angegeben, lautet die Zeit 24:00 (Mitternacht) an dem angegebenen Datum.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                           | Beschreibung  | Beispiel   |
|--------------------------------|---|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum                                      | 09/15/1999   |
| TODAY                          | Das aktuelle Datum  | TODAY  |
| TODAY+Tage oder +Tage          | Das aktuelle Datum plus der Anzahl der angegebenen Tage.  | TODAY +3 oder +3.  |
| TODAY-Tage oder -Tage          | Das aktuelle Datum minus der Anzahl der angegebenen Tage. | TODAY -3 oder -3.  |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.                             | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.       | EOLM-1<br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.                       | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.  | BOTM+9<br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

### BEGINTime

Gibt die Anfangszeit des Bereichs an, in den das zeitpunktgesteuerte Datum der Sicherungsgruppe, die angezeigt werden soll, fallen muss. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter BEGINDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird eine Anfangszeit ohne ein Anfangsdatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Uhrzeit.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert                  | Beschreibung   | Beispiel               |
|-----------------------|--|------------------------|
| HH:MM:SS              | Eine bestimmte Uhrzeit   | 10:30:08               |
| NOW                   | Die aktuelle Uhrzeit   | NOW                    |
| NOW+HH:MM oder +HH:MM | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten  | NOW+02:00 oder +02:00. |
| NOW-HH:MM oder -HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten | NOW-02:00 oder -02:00. |

### ENDDate

Gibt das Enddatum des Bereichs an, in den das zeitpunktgesteuerte Datum der Sicherungsgruppe, die angezeigt werden soll, fallen muss. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter ENDTIME verwendet werden, um ein Enddatum und eine Endzeit anzugeben. Wird ein Enddatum ohne eine Endzeit angegeben, lautet die Zeit 23:59:59 am angegebenen Enddatum.

Sie können das Datum mit einem der folgenden Werte angeben:



| Wert                              | Beschreibung  | Beispiel   |
|-----------------------------------|---|--|
| MM/TT/JJJJ                        | Ein bestimmtes Datum  | 09/15/1999   |
| TODAY                             | Das aktuelle Datum  | TODAY  |
| TODAY+Tage <i>oder</i><br>+Tage   | Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY +3 <i>oder</i> +3.   |
| TODAY-Tage <i>oder</i> -<br>Tage  | Das aktuelle Datum minus der Anzahl der angegebenen Tage.   | TODAY -3 <i>oder</i> -3.   |
| EOLM (Ende des<br>letzten Monats) | Der letzte Tag des Vormonats.   | EOLM   |
| EOLM-Tage                         | Der letzte Tag des Vormonats minus angegebene Tage.   | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses<br>Monats)    | Der erste Tag des aktuellen Monats.   | BOTM   |
| BOTM+Tage                         | Der erste Tag des aktuellen Monats plus angegebene Tage.  | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

#### ENDTime

Gibt die Endzeit des Bereichs an, in den das zeitpunktgesteuerte Datum der Sicherungsgruppe, die angezeigt werden soll, fallen muss. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter ENDDATE verwendet werden, um ein Datum und eine Uhrzeit anzugeben. Wird eine Endzeit ohne ein Enddatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Zeit.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert                             | Beschreibung   | Beispiel                      |
|----------------------------------|--|-------------------------------|
| HH:MM:SS                         | Eine bestimmte Uhrzeit   | 10:30:08                      |
| NOW                              | Die aktuelle Uhrzeit   | NOW                           |
| NOW+HH:MM <i>oder</i><br>+HH:MM  | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten  | NOW+02:00 <i>oder</i> +02:00. |
| NOW-HH:MM <i>oder</i> -<br>HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten | NOW-02:00 <i>oder</i> -02:00. |

#### WHERERetention

Gibt den Aufbewahrungszeitraum in Tagen an, der den Sicherungsgruppen zugeordnet sein muss, die angezeigt werden sollen. Sie können eine ganze Zahl von 0 bis 30000 angeben. Gültige Werte:

##### Tage

Gibt an, dass Sicherungsgruppen, die diese Anzahl Tage aufbewahrt werden, angezeigt werden.

##### NOLimit

Gibt an, dass Sicherungsgruppen, die unbegrenzt aufbewahrt werden, angezeigt werden.

#### WHEREDescription

Gibt die Beschreibung an, die der Sicherungsgruppe zugeordnet sein muss, die angezeigt werden soll. Die angegebene Beschreibung kann Platzhalterzeichen enthalten. Dieser Parameter ist wahlfrei. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

#### WHEREDEVclass

Gibt den Namen der Einheitenklasse an, die der Sicherungsgruppe zugeordnet sein muss, die angezeigt werden soll. Es können Platzhalterzeichen verwendet werden, um einen Einheitenklassennamen anzugeben. Dieser Parameter ist wahlfrei.

#### WHERECexists

Gibt an, ob eine Sicherungsgruppe ein Inhaltsverzeichnis haben muss, damit sie angezeigt wird. Dieser Parameter ist wahlfrei. Der Standardwert gibt an, dass alle Sicherungsgruppen angezeigt werden sollen, unabhängig davon, ob sie ein Inhaltsverzeichnis haben.

#### WHEREDATType

Gibt den Datentyp einer Sicherungsgruppe an, der angezeigt werden soll. Dieser Parameter ist wahlfrei. Der Standardwert gibt an, dass alle Typen von Sicherungsgruppen angezeigt werden sollen. Bei der Angabe mehrerer Datentypen müssen die Datentypen durch Kommas und ohne Leerzeichen voneinander getrennt werden.

## FILE

Gibt an, dass eine Sicherungsgruppe auf Dateiebene angezeigt werden soll. Sicherungsgruppen auf Dateiebene enthalten Dateien und Verzeichnisse, die vom Client für Sichern/Archivieren gesichert wurden.

## IMAGE

Gibt an, dass eine Imagesicherungsgruppe angezeigt werden soll. Imagesicherungsgruppen enthalten Images, die mit dem Befehl BACKUP IMAGE des Clients für Sichern/Archivieren erstellt wurden.

## Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

### Standard

Gibt an, dass Teilinformationen für die angegebenen Sicherungsgruppen angezeigt werden.

### Detailed

Gibt an, dass die gesamten Informationen für die angegebenen Sicherungsgruppen angezeigt werden.

## Beispiel: Eine Sicherungsgruppe abfragen

Informationen zu Sicherungsgruppen anzeigen, deren Namen mit PERS\_DATA beginnen. Die Sicherungsgruppen gehören zum Knoten JANE und sind der Einheitenklasse DVLMENT zugeordnet.

```
query backupset jane pers_data*
```

```
                Knotenname: JANE
Sicherungsgruppenname: PERS_DATA.3089
                Datentyp: File
                Datum/Uhrzeit: 03/17/2007 16:17:47
Aufbewahrungszeitraum: 60
                Einheitenklassenname: DVLMENT
                Beschreibung: backupset created from /srvr
Hat Inhaltsverzeichnis?: Yes
```

## Feldbeschreibungen

### Knotenname

Gibt den Namen des Clientknotens an, dessen Daten in der Sicherungsgruppe enthalten sind.

### Sicherungsgruppenname

Gibt den Namen der Sicherungsgruppe an.

### Datentyp

Zeigt den Datentyp der Sicherungsgruppen. Mögliche Typen sind file (Datei), image (Image) und application (Anwendung).

### Datum/Uhrzeit

Gibt das Datum und die Uhrzeit (PITDate und PITTime) des Befehls GENERATE BACKUPSET an. PITDate und PITTime geben an, dass Dateien, die an dem angegebenen Datum und zu der angegebenen Zeit aktiv waren und die noch auf dem IBM Spectrum Protect-Server gespeichert sind, in die Sicherungsgruppe eingeschlossen werden sollen, auch wenn sie zum Zeitpunkt der Ausgabe des Befehls GENERATE BACKUPSET inaktiv sind. Der Standardwert ist das Datum, an dem der Befehl GENERATE BACKUPSET ausgeführt wird.

### Aufbewahrungszeitraum

Gibt die Anzahl Tage an, die die Sicherungsgruppe auf dem Server aufbewahrt wird.

### Einheitenklassenname

Gibt den Namen der Einheitenklasse an, der die Datenträger, die die Sicherungsgruppe enthalten, zugeordnet sind.

### Beschreibung

Gibt die Beschreibung an, die der Sicherungsgruppe zugeordnet ist.

### Hat Inhaltsverzeichnis?

Gibt an, ob die Sicherungsgruppe ein Inhaltsverzeichnis hat.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY BACKUPSET

| Befehl                 | Beschreibung   |
|------------------------|--|
| DEFINE BACKUPSET       | Definiert eine zuvor generierte Sicherungsgruppe für einen Server. |
| DEFINE NODEGROUP       | Definiert eine Gruppe von Knoten.                                  |
| DEFINE NODEGROUPMEMBER | Fügt einer Knotengruppe einen Clientknoten hinzu.                  |
| GENERATE BACKUPSET     | Generiert eine Sicherungsgruppe mit den Daten eines Clients.       |
| GENERATE BACKUPSETTOC  | Generiert ein Inhaltsverzeichnis für eine Sicherungsgruppe.        |



```
JANE          /srvr      /deblock.c
JANE          /srvr      /dsmerror.log
JANE          /srvr      /dsmxxxxx.log
JANE          ...          .....
```

## Feldbeschreibungen

### Knotenname

Gibt den Namen des Clientknotens an, dessen Daten in der Sicherungsgruppe enthalten sind.

### Dateibereichsname

Gibt den Namen des Dateibereichs an, zu dem die angegebene Datei gehört.

Dateibereichsnamen können eine andere Zeichenumsetzungstabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetzungstabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetzungstabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetzungstabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

### Dateiname des Clients

Gibt den Namen der Datei an.

Dateibereichsnamen und Dateinamen, die eine andere Zeichenumsetzungstabelle oder Locale als der Server haben können, werden im Operations Center oder in der Verwaltungsbefehlszeilenschnittstelle nicht korrekt angezeigt. Die Daten selbst werden korrekt gesichert und können korrekt zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

Ist der Dateibereichsname in Unicode, wird der Name zur Anzeige in die Zeichenumsetzungstabelle des Servers konvertiert. Die Ergebnisse der Konvertierung für Zeichen, die von der aktuellen Zeichenumsetzungstabelle nicht unterstützt werden, hängen von dem Betriebssystem ab. Bei Namen, die IBM Spectrum Protect teilweise konvertieren kann, werden möglicherweise Fragezeichen (??), Leerzeichen, nicht druckbare Zeichen oder "..." angezeigt. Diese Zeichen zeigen dem Administrator, dass Dateien vorhanden sind. Ist die Konvertierung nicht erfolgreich, wird der Name als "..." angezeigt. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetzungstabelle nicht verfügbar sind oder wenn der Server Probleme beim Zugriff auf die Systemkonvertierungsroutinen hat.

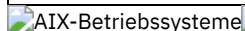
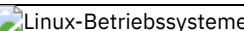
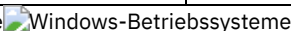
Ein Dateiname, der als "....." angezeigt wird, gibt an, dass sowohl der Dateipfad als auch der Dateiname nicht erfolgreich konvertiert wurden. Ein Beispiel für den Pfad und Namen ist:

```
my\dir\...
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY BACKUPSETCONTENTS

| Befehl                | Beschreibung  |
|-----------------------|---|
| DEFINE BACKUPSET      | Definiert eine zuvor generierte Sicherungsgruppe für einen Server.          |
| GENERATE BACKUPSET    | Generiert eine Sicherungsgruppe mit den Daten eines Clients.                |
| GENERATE BACKUPSETTOC | Generiert ein Inhaltsverzeichnis für eine Sicherungsgruppe.                 |
| DELETE BACKUPSET      | Löscht eine Sicherungsgruppe.   |
| QUERY BACKUPSET       | Zeigt Sicherungsgruppen an.   |
| UPDATE BACKUPSET      | Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum. |

## QUERY CLEANUP (Bereinigung abfragen, die in einem Quellenspeicherpool erforderlich ist)

Mit diesem Befehl können Informationen zu beschädigten Dateien angezeigt werden, die während eines Speicherpoolkonvertierungsprozesses identifiziert werden.

Wenn Sie den Befehl CONVERT STGPOOL ausgeben, um eine Einheitenklasse FILE, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) in einen Verzeichniscontainerspeicherpool zu konvertieren, werden einige Dateien in dem Quellenspeicherpool aufgrund von beschädigten Daten möglicherweise nicht konvertiert. Geben Sie den Befehl QUERY CLEANUP für einen Quellenspeicherpool aus, um beschädigte Daten anzuzeigen, die während des Konvertierungsprozesses identifiziert werden.

Um eine unbeschädigte Version der Daten aus einem Kopierspeicherpool oder Speicherpool für aktive Daten wiederherzustellen, geben Sie den Befehl RESTORE STGPOOL aus. Um eine unbeschädigte Version der Daten von einem Zielreplikationsserver wiederherzustellen, geben Sie den Befehl REPLICATE NODE aus und geben Sie den Parameter RECOVERDAMAGED=YES an.

## Berechtigungsklasse

---

Für diesen Befehl ist die eingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
>>-Query CLeanup--PoolName-----><
```

## Parameter

---

Poolname (Erforderlich)  
Gibt den Speicherpool an, der abgefragt werden soll.

## Beispiel: Beschädigte Dateien anzeigen, die bei einem Speicherpoolkonvertierungsprozess identifiziert werden

---

Beschädigte Dateien in einem Speicherpool mit dem Namen POOL1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query cleanup pool1

      Dateiname: \RTC\BDAT\GIGFILES\BF1.GB
      Status: Aktiv
Gespeicherte Größe: 1 GB
Dateibereichsname: \\ibm838-r90gf0gx\c$
      Typ: Backup
      Clientname: CAKINProtection
Datum des Schutzes: 03/25/2016 16:47:57
```

## Feldbeschreibungen

---

### Dateiname

Der Name der beschädigten Datei.

### Status

Der Status der Daten im Bestand. Die folgenden Status sind gültig:

#### Aktiv

Die Version der Datei im Bestand ist aktiv. Es kann nur eine aktive Version der Datei im Bestand vorhanden sein.

#### Inaktiv

Die Version der Datei im Bestand ist inaktiv. Es können mehrere inaktive Versionen der Datei im Bestand vorhanden sein.

### Gespeicherte Größe

Die Größe der Daten in Megabyte (MB) oder Gigabyte (GB), die in dem Speicherpool gespeichert werden.

### Dateibereichsname

Der Name des Dateibereichs, dem die Datei zugeordnet ist.

### Typ

Der Typ der Operation, die zum Speichern der Datei verwendet wurde. Die folgenden Typen sind gültig:

#### Backup

Dateien, die gesichert werden.

#### Archive

Dateien, die archiviert werden.

## SpaceMg

Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert werden.

### Clientname

Der Name des Clients, der Eigner der Datei ist.

### Datum des Schutzes

Die Uhrzeit und das Datum, zu der bzw. an dem die Datei von einem IBM Spectrum Protect for Space Management-Client gesichert, archiviert oder umgelagert wurde.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY CLEANUP

| Befehl           | Beschreibung  |
|------------------|---|
| CONVERT STGPOOL  | Konvertiert einen Speicherpool in einen Verzeichniscontainerspeicherpool.       |
| PROTECT STGPOOL  | Schützt einen Verzeichniscontainerspeicherpool.                                 |
| QUERY CONVERSION | Fragt den Konvertierungsstatus eines Speicherpools ab.                          |
| REMOVE DAMAGED   | Entfernt beschädigte Daten aus einem Quellenspeicherpool.                       |
| REPAIR STGPOOL   | Repariert einen Verzeichniscontainerspeicherpool.                               |
| REPLICATE NODE   | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.          |
| RESTORE STGPOOL  | Schreibt Dateien aus Kopierspeicherpools in einen primären Speicherpool zurück. |

## QUERY CLOPTSET (Clientoptionsgruppe abfragen)

Mit diesem Befehl kann eine Clientoptionsgruppe abgefragt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
.- *-----  
>>-Query CLOptset--+-----+----->  
                    '-Optionsgruppenname-'  
  
>+-----+-----<  
    '-DESCription-----Beschreibung-'
```

### Parameter

#### Optionsgruppenname

Gibt den Namen der Clientoptionsgruppe an, die abgefragt werden soll. Dieser Name kann mithilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert lautet Optionsgruppennamen.

#### DESCription

Gibt die im Befehl DEFINE oder UPDATE CLOPTSET verwendete Beschreibung an, die als Filter verwendet werden soll. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Dieser Parameter ist wahlfrei.

## Beispiel: Eine Clientoptionsgruppe abfragen

Von einem verwalteten Server die Clientoptionsgruppe ENG abfragen. Geben Sie den folgenden Befehl aus:

```
query cloptset eng
```

```
Optionsgruppe: ENG  
Beschreibung:  
Letzte Aktualisierung durch  
(Administrator): $$CONFIG_MANAGER$$
```

Verwaltendes Profil:

Replikatoptionsgruppe: Yes

Option: SCROLLINES  
Folgenummer: 0  
Optionsgruppenwert verwenden (FORCE): No  
Optionswert: 40

Option: SCROLLPROMPT  
Folgenummer: 0  
Optionsgruppenwert verwenden (FORCE): No  
Optionswert: yes

## Feldbeschreibungen

### Optionsgruppe

Gibt den Namen der Optionsgruppe an.

### Beschreibung

Gibt die Beschreibung der Clientoptionsgruppe an.

### Letzte Aktualisierung durch (Administrator)

Gibt den Namen des Administrators an, der die Optionsgruppe zuletzt aktualisiert hat. Enthält dieses Feld \$\$CONFIG\_MANAGER\$\$, ist die Clientoptionsgruppe einem Profil zugeordnet, das von dem Konfigurationsmanager verwaltet wird.

### Verwaltendes Profil

Gibt das Profil an, für das der verwaltete Server subskribiert hat, um die Definition der Clientoptionsgruppe zu erhalten.

### Replikatoptionsgruppe

Gibt an, dass die Replikatoptionsgruppe durch den Quellenreplikationsserver repliziert wird.

### Option

Gibt den Namen der Option an.

### Folgenummer

Gibt die Folgenummer der Option an.

### Optionsgruppenwert verwenden (FORCE)

Gibt an, ob die Serveroptionseinstellung die Optionseinstellung für den Client überschreibt. NO gibt an, dass die Serveroptionseinstellung die Clientoption nicht überschreibt. YES gibt an, dass die Serveroptionseinstellung die Clientoptionseinstellung überschreibt. Diese Option wird mit dem Parameter FORCE im Befehl DEFINE CLIENTOPT definiert.

### Optionswert

Gibt den Wert der Option an.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY CLOPTSET

| Befehl                 | Beschreibung  |
|------------------------|---|
| COPY CLOPTSET          | Kopiert eine Clientoptionsgruppe.   |
| DEFINE CLIENTOPT       | Fügt einer Clientoptionsgruppe eine Clientoption hinzu.                       |
| DEFINE CLOPTSET        | Definiert eine Clientoptionsgruppe.   |
| DELETE CLIENTOPT       | Löscht eine Clientoption aus einer Clientoptionsgruppe.                       |
| DELETE CLOPTSET        | Löscht eine Clientoptionsgruppe.  |
| UPDATE CLIENTOPT       | Aktualisiert die Folgenummer einer Clientoption in einer Clientoptionsgruppe. |
| UPDATE CLOPTSET        | Aktualisiert die Beschreibung einer Clientoptionsgruppe.                      |
| DEFINE PROFASSOCIATION | Ordnet Objekte einem Profil zu.   |

## QUERY COLLOGROUP (Kollokationsgruppe abfragen)

Verwenden Sie diesen Befehl, um die Kollokationsgruppen anzuzeigen, die auf dem Server definiert sind.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```

      .-*------.
>>-Query COLLOCGroup--+-----+----->
      '-Gruppenname-'

.-Format----Standard----.
>--+-----+-----><
      '-Format----+Standard-+-'
      '-Detailed-'

```

## Parameter

### Gruppenname

Gibt den Namen der Kollokationsgruppe an, die angezeigt werden soll. Sollen mehrere Namen angegeben werden, ein Platzhalterzeichen verwenden. Dieser Parameter ist wahlfrei. Standardmäßig werden alle Kollokationsgruppen angezeigt.

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

#### Standard

Gibt an, dass Teilm Informationen angezeigt werden.

#### Detailed

Gibt an, dass die gesamten Informationen angezeigt werden. Um die Clientknoten in der Kollokationsgruppe anzuzeigen, müssen Sie FORMAT=DETAILED angeben.

## Definierte Kollokationsgruppen anzeigen

Die Kollokationsgruppen anzeigen, die auf dem Server definiert sind. Den folgenden Befehl ausgeben:

```
query collogroup
```

| Name der Kollokationsgruppe | Beschreibung der Kollokationsgruppe |
|-----------------------------|-------------------------------------|
| DEPT_ED                     | Ausbildungsabteilung                |
| GROUP1                      | Clientknoten mit geringer Kap.      |

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Ausführliche Informationen zu Kollokationsgruppen anzeigen

Vollständige Informationen zu allen Kollokationsgruppen anzeigen und bestimmen, welche Clientknoten zu welchen Kollokationsgruppen gehören. Den folgenden Befehl ausgeben:

```
query collogroup format=detailed
```

```

      Name der Kollokationsgruppe: DEPT_ED
      Beschreibung der Kollokationsgruppe: Ausbildungsabteilung
      Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
      Datum/Zeit der letzten Aktualisierung: 04/21/2013 10:59:03
      Kollokationsgruppenmitglied(er): EDU_1 EDU_7
      Dateibereichsmitglied(er):

      Name der Kollokationsgruppe: GROUP1
      Beschreibung der Kollokationsgruppe: Knoten mit ger. Kap.
      Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
      Datum/Zeit der letzten Aktualisierung: 04/21/2013 10:59:16
      Kollokationsgruppenmitglied(er): CHESTER
      Dateibereichsmitglied(er): alpha

      Name der Kollokationsgruppe: GROUP1
      Beschreibung der Kollokationsgruppe: Knoten mit ger. Kap.
      Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
      Datum/Zeit der letzten Aktualisierung: 04/21/2013 10:59:16
      Kollokationsgruppenmitglied(er): CHESTER
      Dateibereichsmitglied(er): beta

      Name der Kollokationsgruppe: GROUP1
      Beschreibung der Kollokationsgruppe: Knoten mit ger. Kap.
      Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
      Datum/Zeit der letzten Aktualisierung: 04/21/2013 10:59:16
      Kollokationsgruppenmitglied(er): CHESTER
      Dateibereichsmitglied(er): gamma

```



Für Felddesreibungen siehe Felddesreibungen.

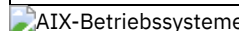
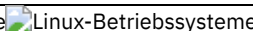
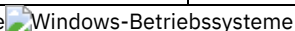
## Felddesreibungen

|   |  |
|---|--|
| Name der Kollokationsgruppe                 | Der Name der Kollokationsgruppe.   |
| Beschreibung der Kollokationsgruppe         | Die Beschreibung der Kollokationsgruppe.   |
| Letzte Aktualisierung durch (Administrator) | Der Name des Administrators, der die Kollokationsgruppe definiert oder zuletzt aktualisiert hat.   |
| Datum/Zeit der letzten Aktualisierung       | Das Datum und die Uhrzeit, an dem bzw. zu der ein Administrator die Kollokationsgruppe definiert oder zuletzt aktualisiert hat.                                    |
| Kollokationsgruppenmitglied(er)             | Die Mitglieder der Kollokationsgruppe.   |
| Dateibereichsmitglied(er)                   | Die Dateibereiche, die Mitglieder der Kollokationsgruppe sind. Sind mehrere Dateibereiche vorhanden, wird jeder Dateibereich in einem separaten Eintrag angezeigt. |

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY COLLOGROUP

| Befehl              | Beschreibung  |
|---------------------|---|
| DEFINE COLLOGROUP   | Definiert eine Kollokationsgruppe.  |
| DEFINE COLLOCMEMBER | Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.                                     |
| DEFINE STGPOOL      | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.                            |
| DELETE COLLOGROUP   | Löscht eine Kollokationsgruppe.   |
| DELETE COLLOCMEMBER | Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.                                     |
| MOVE NODEDATA       | Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen. |
| QUERY NODE          | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.                             |
| QUERY NODEDATA      | Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.                               |
| QUERY STGPOOL       | Zeigt Informationen zu Speicherpools an.  |
| REMOVE NODE         | Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.              |
| UPDATE COLLOGROUP   | Aktualisiert die Beschreibung einer Kollokationsgruppe.   |
| UPDATE STGPOOL      | Ändert die Attribute eines Speicherpools.   |

## QUERY CONTAINER (Container abfragen)

Mit diesem Befehl können Informationen zu einem oder zu mehreren Containern angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query CONTAINER-+-----+----->
                    .-*-----,
                    '-Containername-'
```



## Beispiel: Informationen zu einem Container anzeigen

---

Für Felddescriptions siehe Felddescriptions.

```
query container /Containers/09/0000000000000943.ncf
```

| Container                           | Speicher-<br>poolname | Container-<br>typ | Status    |
|-------------------------------------|-----------------------|-------------------|-----------|
| /Containers/09/0000000000000943.ncf | STGPOOL1              | Non Dedup         | Available |

 Windows-Betriebssysteme

## Beispiel: Informationen zu einem Container anzeigen

---

Für Felddescriptions siehe Felddescriptions.

```
query container C:\abc\00\0000000000000005.ncf
```

| Container                      | Speicher-<br>poolname | Container-<br>typ | Status    |
|--------------------------------|-----------------------|-------------------|-----------|
| C:\abc\00\0000000000000005.ncf | STGPOOL1              | Non Dedup         | Available |

 AIX-Betriebssysteme  Linux-Betriebssysteme

## Beispiel: Ausführliche Informationen zu einem Container anzeigen

---

Ausführliche Informationen zu Containern anzeigen, die deduplizierte Daten im Speicherpool STGPOOL1 enthalten:

```
query container stgpool=STGPOOL1 type=dedup format=detail
```

```
Container: /abc/00/0000000000000001.dcf
  Speicherpoolname: STGPOOL1
  Containertyp: Dedup
  Status: Available
  Maximale Größe (MB): 40.960
  Freier Speicherbereich (MB): 39.700
  Ungefähres Datum des letzten Schreibens: 11/10/2014 15:17:09
  Ungefähres Datum der letzten Prüfung:
    Cloudtyp:
    Cloud-URL:
  Cloudobjektgröße (MB):
  Belegter Speicherbereich (MB):
  Anzahl Datenbereiche:
```

 Windows-Betriebssysteme

## Beispiel: Ausführliche Informationen zu einem Container anzeigen

---

Ausführliche Informationen zu Containern anzeigen, die deduplizierte Daten im Speicherpool STGPOOL1 enthalten:

```
query container stgpool=STGPOOL1 type=dedup format=detail
```

```
Container: C:\abc\00\0000000000000001.dcf
  Speicherpoolname: STGPOOL1
  Containertyp: Dedup
  Status: Available
  Maximale Größe (MB): 40.960
  Freier Speicherbereich (MB): 39.700
  Ungefähres Datum des letzten Schreibens: 11/10/2014 15:17:09
  Ungefähres Datum der letzten Prüfung:
    Cloudtyp:
    Cloud-URL:
  Cloudobjektgröße (MB):
  Belegter Speicherbereich (MB):
  Anzahl Datenbereiche:
```

## Beispiel: Ausführliche Informationen zu Containern anzeigen, die in einem Cloudspeicherpool gespeichert sind

---

Ausführliche Informationen zu Containern anzeigen, die im Cloudspeicherpool CLOUDPOOL gespeichert sind:

```
query container stgpool=CLOUDPOOL format=detail
```

```
Container: 7-64a1261000c811e58e8f005056c00008
  Speicherpoolname: CLOUDPOOL
  Containertyp: Cloud
  Status:
  Freier Speicherbereich (MB):
  Maximale Größe (MB):
  Ungefähres Datum des letzten Schreibens: 05/22/2015 14:36:57
  Ungefähres Datum der letzten Prüfung:
  Cloudtyp: SWIFT
  Cloud-URL: http://cloudurl:5000/v2.0
Cloudobjektgröße (MB):
  Belegter Speicherbereich (MB): 27
  Anzahl Datenbereiche: 95
```

## Feldbeschreibungen

---

### Container

Der Name des Containers.

### Speicherpoolname

Der Name des Speicherpools.

### Containertyp

Der Typ des Containers.

### Status

Der Status der Daten in dem Container. Das Feld kann einen der folgenden Werte enthalten:

#### Available

Der Container ist für die Verwendung verfügbar.

#### Unavailable

Der Container kann nicht geöffnet oder geprüft werden.

Tipp: Geben Sie den Befehl `AUDIT CONTAINER` aus, um den Inhalt des Containers zu prüfen.

#### Read only

Der Container kann gelesen werden, aber es können keine Daten in den Container geschrieben werden.

#### Pending

Das Löschen des Containers ist anstehend. Wenn der für den Parameter `REUSEDELAY` im Befehl `DEFINE STGPOOL` oder `UPDATE STGPOOL` angegebene Wert abläuft, wird der Container gelöscht.

Dieses Feld gilt nicht für Container, die in Cloudspeicherpools gespeichert sind.

### Maximale Größe (MB)

Die maximale Größe des Containers in Megabyte.

Dieses Feld gilt nicht für Container, die in Cloudspeicherpools gespeichert sind.

### Freier Speicherbereich (MB)

Der Gesamtumfang des freien Speicherbereichs (in Megabyte), der im Container verfügbar ist.

Dieses Feld gilt nicht für Container, die in Cloudspeicherpools gespeichert sind.

### Ungefähres Datum des letzten Schreibens

Das ungefähre Datum und die Uhrzeit, an dem bzw. zu der Daten in den Container geschrieben wurden.

### Ungefähres Datum der letzten Prüfung

Das ungefähre Datum und die Uhrzeit, an dem bzw. zu der Daten in dem Container geprüft wurden.

### Cloudtyp

Wenn der Container in einem Cloudspeicherpool gespeichert ist, der Typ der Cloudplattform.

### Cloud-URL

Wenn der Container in einem Cloudspeicherpool gespeichert ist, die URL für den Zugriff auf die private On-Premises-Cloud oder die öffentliche Off-Premises-Cloud.

### Cloudobjektgröße (MB)

Die Größe des Cloudobjekts in Megabyte, wenn der Container durch ein einzelnes Objekt im Cloud-Containerspeicherpool dargestellt wird.

### Belegter Speicherbereich (MB)

Wenn der Container in einem Cloudspeicherpool gespeichert ist, der Umfang des Speicherbereichs, der von dem Container in der privaten On-Premises-Cloud oder der öffentlichen Off-Premises-Cloud belegt wird.

### Anzahl Datenbereiche

Wenn der Container in einem Cloud-Containerspeicherpool gespeichert ist, die Anzahl Datenbereiche, die von der privaten On-Premises-Cloud oder der öffentlichen Off-Premises-Cloud für den Container verwaltet wird.

Tabelle 1. Zugehörige Befehle für QUERY CONTAINER

| Befehl          | Beschreibung   |
|-----------------|--|
| AUDIT CONTAINER | Prüft einen Verzeichniscontainerspeicherpool.                                |
| MOVE CONTAINER  | Versetzt den Inhalt eines Speicherpoolcontainers in einen anderen Container. |
| QUERY DAMAGED   | Zeigt Informationen zu beschädigten Dateien an.                              |

## QUERY CONTENT (Inhalt eines Speicherpooldatenträgers abfragen)

Mit diesem Befehl können Informationen zu Dateien auf einem Speicherpooldatenträger und die Namen von Clientdateien angezeigt werden, die die Verknüpfung zu einer deduplizierten Gruppe von Dateien herstellen.

Mit diesem Befehl können Dateien identifiziert werden, die vom Server als beschädigt erkannt wurden, sowie Dateien bestimmt werden, die in einem Kopierspeicherpool gesichert oder in einen Pool für aktive Daten kopiert wurden. Dieser Befehl ist nützlich bei einem beschädigten Datenträger oder bevor

- eine Anforderung an den Server gesendet wird, Inkonsistenzen zwischen einem Datenträger und der Datenbank zu beseitigen.
- Dateien von einem Datenträger auf einen anderen Datenträger versetzt werden.
- ein Datenträger aus einem Speicherpool gelöscht wird.

Da die Ausführung dieses Befehls sehr lange dauern kann und die Ergebnisse umfangreich sein können, sollte der Parameter COUNT verwendet werden, um die Anzahl der angezeigten Dateien zu begrenzen.

Anmerkung: Cache-Dateien in einem Plattendatenträger, die als beschädigt markiert sind, sind in den Ergebnissen nicht enthalten.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-Query CONTENT--Datenträgername--+-+-----+----->
                                     '-NODE-----Knotenname-'
>+-----+-----+-----+-----+----->
  '-Filespace-----Dateibereichsname-' '-COUnt-----Anzahl-'
. -Type-----ANY----- . -Format-----Standard-----
>+-----+-----+-----+-----+----->
  '-Type-----+ANY-----+' '-Format-----+Standard+++'
      +-Backup-----+           '-Detailed-'
      +-Archive-----+
      '-SPacemanaged-'
                                     (1)
. -DAmaged-----ANY----- . -COPIed-----ANY-.
>+-----+-----+-----+-----+----->
  '-DAmaged-----+ANY+++' '-COPIed-----+ANY+++'
      +-Yes++           +-Yes++
      '-No--'           '-No--'
. -NAMEType-----SERVER-----
>+-----+-----+-----+-----+----->
  '-NAMEType-----+SERVER+++'
      +-UNICODE+
      '-FSID-----'
. -CODEType-----BOTH-----
>+-----+-----+-----+-----+----->
  '-CODEType-----+UNICODE+++'
      +-NONUNICODE+
      '-BOTH-----'
. -FOLLOWLinks-----No-----
>+-----+-----+-----+-----+----->
  '-FOLLOWLinks-----+No-----+'
      +-Yes-----+
```

Anmerkungen:

1. Dieser Parameter ist nur für Datenträger in primären Speicherpools zu verwenden.

## Parameter

---

Datenträgername (Erforderlich)

Gibt den Datenträger an, der abgefragt werden soll.

NODE

Gibt den Client für Sichern/Archivieren oder den IBM Spectrum Protect for Space Management an, der dem Dateibereich zugeordnet ist, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Name angegeben, werden alle Clients für Sichern/Archivieren und IBM Spectrum Protect for Space Management-Clients berücksichtigt.

Filespace

Gibt den Dateibereich an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Bei Dateibereichsnamen muss die Groß-/Kleinschreibung berücksichtigt werden. Wird kein Dateibereichsname angegeben, werden alle Dateibereiche berücksichtigt.

Ein Server, der über Clients mit Unicode-Unterstützung verfügt, muss möglicherweise den Dateibereichsnamen, den Sie eingeben, konvertieren. Beispielsweise muss der Server gegebenenfalls den Namen, den Sie eingeben, aus der Zeichenumsetzungstabelle des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich unter dem Parameter NAMETYPE. Geben Sie keinen Dateibereichsnamen an oder geben Sie nur ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter CODETYPE verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

COUnt

Gibt die Anzahl der Dateien an, die angezeigt werden sollen. Dieser Parameter ist wahlfrei. Zulässig ist die Angabe einer positiven ganzen Zahl oder einer negativen ganzen Zahl. Wird eine positive ganze Zahl *n* angegeben, werden die ersten *n* Dateien angezeigt. Wird eine negative ganze Zahl *-n* angegeben, werden die letzten *n* Dateien in umgekehrter Reihenfolge angezeigt. Sie dürfen COUNT=0 nicht angeben. Wird für diesen Parameter kein Wert angegeben, werden alle Dateien angezeigt.

Type

Gibt die Dateitypen an, die abgefragt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Ist der Datenträger, der abgefragt wird, einem Pool für aktive Daten zugeordnet, sind nur die Werte ANY und BACKUP gültig. Gültige Werte:

ANY

Gibt an, dass alle Dateitypen in dem Speicherpool datenträger abgefragt werden: Sicherungsversionen von Dateien, Archivierungskopien von Dateien und Dateien, die von IBM Spectrum Protect for Space Management-Clients aus Clientknoten umgelagert wurden.

Backup

Gibt an, dass nur Sicherungsdateien abgefragt werden.

Archive

Gibt an, dass nur Archivierungsdateien abgefragt werden. Dieser Wert ist für Pools für aktive Daten nicht gültig.

SPacemanaged

Gibt an, dass nur speicherverwaltete Dateien (Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden) abgefragt werden. Dieser Wert ist für Pools für aktive Daten nicht gültig.

Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

Standard

Gibt an, dass Teilm Informationen angezeigt werden. Unicode-Namen werden in die Server-Zeichenumsetzungstabelle konvertiert.

Detailed

Gibt an, dass die gesamten Informationen angezeigt werden. Unicode-Namen werden in hexadezimalen Zeichen angezeigt.

DAMaged

Gibt Kriterien an, um die Ausgabe der Abfrage auf der Basis von Dateien, die als beschädigt markiert werden, zu begrenzen. Zu diesem Zweck überprüft der Server nur physische Dateien (eine Datei, die eine einzelne logische Datei oder ein Aggregat aus logischen Dateien sein kann). Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Gültige Werte:

ANY

Gibt an, dass Dateien unabhängig davon angezeigt werden, ob der Server die Dateien als beschädigt festgestellt hat.

Yes

Gibt an, dass nur Dateien angezeigt werden, die als beschädigt markiert werden. Hierbei handelt es sich um Dateien, in denen der Server Fehler festgestellt hat, als versucht wurde, sie zurückzuschreiben, abzurufen oder zurückzurufen oder als ein Befehl AUDIT VOLUME ausgeführt wurde.

No

Gibt an, dass nur Dateien angezeigt werden, von denen nicht bekannt ist, dass sie beschädigt sind.

COPIED

Gibt Kriterien an, um die Ausgabe der Abfrage auf der Basis von Dateien, die in einem Kopierspeicherpool gesichert wurden, zu begrenzen. Ob Dateien in einem Pool für aktive Daten gespeichert werden, hat keinen Einfluss auf die Ausgabe. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Gültige Werte:

ANY

Gibt an, daß Dateien unabhängig davon angezeigt werden, ob sie in einem Kopierspeicherpool gesichert werden. Kopien von Primär- und Cache-Dateien werden angezeigt.

Yes

Gibt an, daß nur Dateien angezeigt werden, für die mindestens eine verwendbare Sicherungskopie in einem Kopierspeicherpool vorhanden ist. Eine Datei wird nicht angezeigt, wenn bei ihrer Kopie im Kopierspeicherpool Fehler festgestellt wurden. Kopien von Cache-Dateien werden nicht angezeigt, weil diese Dateien nie zurückgeschrieben werden.

Verwenden Sie COPIED=YES, um Primärdateien zu identifizieren, die mit dem Befehl RESTORE VOLUME oder RESTORE STGPOOL zurückgeschrieben werden können.

No

Gibt an, daß nur Dateien angezeigt werden, für die keine verwendbaren Sicherungskopien in einem Kopierspeicherpool vorhanden sind. Kopien von Cache-Dateien werden nicht angezeigt, weil diese Dateien nie zurückgeschrieben werden.

Verwenden Sie COPIED=NO, um Primärdateien zu identifizieren, die mit dem Befehl RESTORE VOLUME oder RESTORE STGPOOL nicht zurückgeschrieben werden können.

NAMETYPE

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unicode-Unterstützung verfügt. Ein Client für Sichern/Archivieren mit Unicode-Unterstützung ist gegenwärtig nur für Windows, Macintosh OS 9, Macintosh OS X und NetWare verfügbar. Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen angeben.

Der Standardwert lautet SERVER. Gültige Werte:

SERVER

Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren.

UNICODE

Der Server konvertiert die Dateibereichsnamen aus der Server-Codepage in die Codepage UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in den Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server Probleme beim Zugriff auf die Systemkonvertierungsroutinen hat.

FSID

Der Server interpretiert die Dateibereichsnamen als ihre Dateibereichs-IDs (FSIDs).

CODETYPE

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben.

Der Standardwert lautet BOTH. Dieser Standardwert bedeutet, dass die Dateibereiche unabhängig von der Art der Zeichenumsetztabelle eingeschlossen werden. Gültige Werte:

UNICODE

Nur Dateibereiche einschließen, die in Unicode sind.

NONUNICODE

Dateibereiche einschließen, die nicht nur in Unicode sind.

BOTH

Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen.

FOLLOWLINKS

Gibt an, ob nur die Dateien angezeigt werden sollen, die auf dem Datenträger gespeichert sind, oder nur Dateien angezeigt werden sollen, die mit dem Datenträger verknüpft sind. Sie können auch gespeicherte Dateien und verknüpfte Dateien anzeigen. Der Standardwert ist NO. Gültige Werte:

No

Nur die Dateien anzeigen, die auf dem Datenträger gespeichert sind. Keine Dateien anzeigen, die Verknüpfungen mit dem Datenträger haben.

Yes


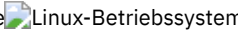
Alle Dateien anzeigen, einschließlich Dateien, die auf dem Datenträger gespeichert sind, und aller Dateien, die Verknüpfungen mit dem Datenträger haben.

#### JUSTLinks


Nur die Dateien anzeigen, die Verknüpfungen mit dem Datenträger haben. Keine Dateien anzeigen, die auf dem Datenträger gespeichert sind.

## Beispiel: Den Inhalt eines Datenträgers für einen bestimmten Clientknoten anzeigen

Den Inhalt eines Datenträgers abfragen und die Ergebnisse auf Dateien begrenzen, die auf dem Clientknoten PEGASUS gesichert wurden.

  Für den Datenträger /tsmstg/diskvoll1.dsm den folgenden Befehl ausgeben:

```
query content /tsmstg/diskvoll1.dsm node=pegasus
type=backup
```

 Für den Datenträger f:\tsmstg\diskvoll1.dsm den folgenden Befehl ausgeben:

```
query content f:\tsmstg\diskvoll1.dsm node=pegasus
type=backup
```

Die Ergebnisse des Befehls umfassen alle logischen Dateien, die ein beliebiges Aggregat auf dem Datenträger bilden, auch wenn das Aggregat auf mehreren Datenträgern gespeichert ist. Bei Aggregaten wird von der Abfrage nicht bestimmt, welche logischen Dateien tatsächlich auf dem Datenträger gespeichert sind, für den die Abfrage ausgeführt wird.

| Knotenname | Typ  | Dateibe-<br>klasse | FSID | Dateiname des Clients |
|------------|------|--------------------|------|-----------------------|
| PEGASUS    | Bkup | \\pegasus\e\$      | 1    | \UNI_TEST\ SM01.DAT   |
| PEGASUS    | Bkup | \\pegasus\e\$      | 1    | \UNI_TEST\ SM02.DAT   |

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Beispiel: Ausführliche Informationen zu einem Banddatenträger anzeigen

Den Inhalt des Banddatenträgers mit dem Namen WPD001 abfragen. Nur die Dateien anzeigen, die von dem Knoten MARK gesichert werden, und die Dateien anzeigen, die entweder auf dem Datenträger gespeichert oder mit dem Datenträger verknüpft sind. Nur die ersten vier Dateien auf dem Datenträger anzeigen.

```
query content wpd001 node=mark count=4 type=backup followlinks=yes
format=detailed
```

```

                Knotenname: MARK
                  Typ: Bkup
    Dateibereichsname: \\mark\e$
Hexadezimaler Dateibereichsname:
                FSID: 1
    Dateiname des Clients: \UNI_TEST\ SM01.DAT
Hexadezimaler Dateiname des Clients:
                Aggregat?: 1/3
    Gespeicherte Größe: 2.746
                Segmentnummer:
                Cache-Kopie?: No
                Verknüpft: No
                Fragmentnummer:

                Knotenname: MARK
                  Typ: Bkup
    Dateibereichsname: \\mark\e$
Hexadezimaler Dateibereichsname:
                FSID: 1
    Dateiname des Clients: \UNI_TEST\ SM02.DAT
Hexadezimaler Dateiname des Clients:
                Aggregat?: 2/3
    Gespeicherte Größe: 2.746
                Segmentnummer:
                Cache-Kopie?: No
                Verknüpft: No
                Fragmentnummer: 2

                Knotenname: MARK
                  Typ: Bkup
    Dateibereichsname: \\mark\e$
Hexadezimaler Dateibereichsname:
```



```
FSID: 1
Dateiname des Clients: \UNI_TEST\ SM03.DAT
Hexadezimaler Dateiname des Clients:
    Aggregat?: 3/3
    Gespeicherte Größe: 2.746
    Segmentnummer:
    Cache-Kopie?: No
    Verknüpft: No
    Fragmentnummer: 3
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Feldbeschreibungen

---

### Knotenname

Der Knoten, zu dem die Datei gehört.

### Type

Der Dateityp: archive (Arch), backup (Bkup) oder space-managed (SpMg) (durch einen IBM Spectrum Protect for Space Management-Client).

### Dateibereichsname

Der Dateibereich, zu dem die Datei gehört.

Dateibereichsnamen können eine andere Zeichenumsetzungstabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetzungstabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetzungstabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetzungstabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

### Hexadezimaler Dateibereichsname

Der Dateibereich, zu dem die Datei gehört. Ist der Dateibereichsname in Unicode, wird der Name in hexadezimalen Format angezeigt.

### FSID

Die Dateibereichs-ID (FSID) des Dateibereichs. Der Server ordnet eine eindeutige FSID zu, wenn ein Dateibereich zum ersten Mal auf dem Server gespeichert wird.

### Dateiname des Clients

Der Dateiname des Clients.

Dateibereichsnamen und Dateinamen, die eine andere Zeichenumsetzungstabelle oder Locale als der Server haben können, werden im Operations Center oder in der Verwaltungsbefehlszeilenschnittstelle nicht korrekt angezeigt. Die Daten selbst werden korrekt gesichert und können korrekt zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden. Die Ergebnisse der Konvertierung für Zeichen, die von der aktuellen Zeichenumsetzungstabelle nicht unterstützt werden, hängen von dem Betriebssystem ab. Bei Namen, die IBM Spectrum Protect teilweise konvertieren kann, werden möglicherweise Fragezeichen (??), Leerzeichen, nicht druckbare Zeichen oder "... " angezeigt. Diese Zeichen zeigen dem Administrator, dass Dateien vorhanden sind.

### Hexadezimaler Dateiname des Clients

Der Dateiname des Clients, der in hexadezimalen Format angezeigt wird.

### Aggregat?

Die Angabe, ob es sich um eine logische Datei handelt, die als Teil eines Aggregats gespeichert ist. Ist die Datei ein Teil eines Aggregats, werden die Folgenummer dieser Datei innerhalb des Aggregats und die Gesamtzahl der logischen Dateien in dem Aggregat angezeigt. Die Ergebnisse des Befehls umfassen alle logischen Dateien, die ein beliebiges Aggregat auf dem Datenträger bilden, auch wenn das Aggregat auf mehreren Datenträgern gespeichert ist. Die Abfrage bestimmt nicht, welche logischen Dateien tatsächlich auf dem Datenträger gespeichert sind, für den die Abfrage ausgeführt wird.

Ist die Datei nicht Teil eines Aggregats, zeigt dieses Feld "Nein" (No) an.

### Gespeicherte Größe

Die Größe der physischen Datei in Byte. Ist die Datei eine logische Datei, die als Teil eines Aggregats gespeichert ist, gibt dieser Wert die Größe des gesamten Aggregats an.

### Segmentnummer

Gibt bei Datenträgern in Speicherpools mit sequenziellen Zugriff an, ob die physische Datei (entweder eine einzelne logische Datei oder ein Aggregat aus logischen Dateien) auf mehreren Datenträgern gespeichert ist. Ist die logische Datei beispielsweise in einem Aggregat gespeichert, das sich über zwei Datenträger erstreckt, gibt die Segmentnummer 1/2 an (der erste Teil der

physischen Datei ist auf dem Datenträger gespeichert) oder 2/2 an (der zweite Teil der physischen Datei ist auf dem Datenträger gespeichert). Lautet die Segmentnummer 1/1, ist die physische Datei vollständig auf dem Datenträger gespeichert. Bei Datenträgern in Speicherpools mit wahlfreiem Zugriff wird für dieses Feld kein Wert angezeigt.

Cache-Kopie?

Die Angabe, ob die physische Datei eine Cache-Kopie einer Datei ist, die in den nächsten Speicherpool umgelagert wurde. Ist die Datei ein Teil eines Aggregats, bezieht sich dieser Wert auf das Aggregat.

Verknüpft

Gibt an, ob die Datei auf dem Datenträger gespeichert ist oder ob die Datei mit dem Datenträger verknüpft ist.

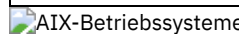
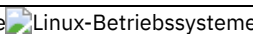
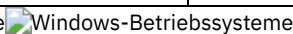
Fragmentnummer

Gibt die Fragmentnummer an. Ist die Fragmentnummer leer, ist das Fragment entweder das erste Fragment oder kein Fragment.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY CONTENT

| Befehl            | Beschreibung  |
|-------------------|---|
| BACKUP STGPOOL    | Sichert einen primären Speicherpool in einem Kopierspeicherpool.  |
| COPY ACTIVATEDATA | Kopiert aktive Sicherungsdaten.   |
| DEFINE VOLUME     | Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.                      |
| DELETE VOLUME     | Löscht einen Datenträger aus einem Speicherpool.  |
| RESTORE STGPOOL   | Schreibt Dateien aus Kopierspeicherpools in einen primären Speicherpool zurück.   |
| RESTORE VOLUME    | Schreibt Dateien, die auf angegebenen Datenträgern in einem primären Speicherpool gespeichert sind, aus Kopierspeicherpools zurück. |
| UPDATE VOLUME     | Aktualisiert die Attribute der Speicherpoolatenträger.  |

## QUERY CONVERSION (Konvertierungsstatus eines Speicherpools abfragen)

Verwenden Sie diesen Befehl, um Informationen zu einer Konvertierungsoperation anzuzeigen. Sie können einen primären Speicherpool, der eine Einheitenklasse des Typs FILE oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet, in einen Verzeichniscontainerspeicherpool konvertieren.

### Berechtigungsklasse

Für diesen Befehl ist die eingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-Query CONVERSion--+-+-----+----->
                        '-Poolname-'
.-Format-----Standard-----
>--+-+-----+-----<<
    '-Format-----+Standard-+-'
                        '-Detailed-'
```

### Parameter

Poolname

Gibt den Quellenspeicherpool an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Wird kein Wert für diesen Parameter angegeben, werden Informationen für alle Speicherpools angezeigt.

Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Geben Sie einen der folgenden Werte an:

Standard

- Gibt an, dass Teilinformationen angezeigt werden.
- Detailed
- Gibt an, dass die gesamten Informationen angezeigt werden.

## Beispiel: Konvertierungsinformationen für alle Speicherpools anzeigen

Konvertierungsinformationen für alle Speicherpools anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query conversion
```

| Quellen-<br>speicherpool | Zielspeicher-<br>pool | Anfangs-<br>volumen | Summe<br>konvertiert | Zuletzt<br>konvertiert |
|--------------------------|-----------------------|---------------------|----------------------|------------------------|
| FILEPOOL                 | CTR                   | 3 GB                | 3 GB                 | 3 GB                   |
| FPOOL                    | CTR                   | 333 MB              | 333 MB               | 267 MB                 |

## Beispiel: Ausführliche Informationen zur Speicherpoolkonvertierung anzeigen

Ausführliche Informationen zur Speicherpoolkonvertierung anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query conversion format=detailed
```

```

Quellenspeicherpool: FILEPOOL
  Zielspeicherpool: CTR
  Maximale Anzahl Prozesse: 4
    Dauer: 60 Minuten
  Anfangsvolumen: 333 MB
  Summe konvertiert: 333 MB
  Zuletzt konvertiert: 333 MB
  Startdatum/-zeit: 03/24/2016 13:22:32

```

## Feldbeschreibungen

### Quellenspeicherpool

Der Name des Speicherpools, der konvertiert wird.

### Zielspeicherpool

Der Name des Zielspeicherpools, in dem die konvertierten Daten gespeichert werden.

### Maximale Anzahl Prozesse

Gibt die maximale Anzahl Konvertierungsprozesse an.

### Dauer

Gibt die Zeit in Minuten für die Konvertierung an.

### Anfangsvolumen

Das Anfangsdatenvolumen in Megabyte (MB), Gigabyte (GB) oder Terabyte (TB), das konvertiert werden soll.

### Summe konvertiert

Das Gesamtdatenvolumen in Megabyte (MB), Gigabyte (GB) oder Terabyte (TB), das konvertiert wurde.

### Zuletzt konvertiert

Das Datenvolumen in Megabyte (MB), Gigabyte (GB) oder Terabyte (TB), das während dieses Konvertierungsprozesses konvertiert wurde.

### Startdatum/-zeit

Die Uhrzeit und das Datum, zu der bzw. an dem der Befehl CONVERT STGPOOL zum ersten Mal für den Speicherpool ausgegeben wurde.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY CONVERSION

| Befehl          | Beschreibung  |
|-----------------|---|
| CONVERT STGPOOL | Konvertiert einen Speicherpool in einen Verzeichniscontainerspeicherpool. |
| QUERY CLEANUP   | Frägt den Bereinigungsstatus eines Quellenspeicherpools ab.               |

## QUERY COPYGROUP (Kopiengruppen abfragen)

Mit diesem Befehl können Informationen über eine oder mehrere Kopiengruppen angezeigt werden.

## Berechtigungsklasse



| Name d. Maßnahmen-<br>domäne | Name d. Maßnahmen-<br>gruppe | Name d. Verw.-<br>Klasse | Name d. Kopien-<br>gruppe | Versionen<br>bestehender<br>Daten | Versionen<br>gelöschter<br>Daten | Extra-<br>versionen<br>aufbew. | Einzig<br>e Version<br>aufbew. |
|------------------------------|------------------------------|--------------------------|---------------------------|-----------------------------------|----------------------------------|--------------------------------|--------------------------------|
| ENGPOLDOM                    | ACTIVE                       | MCENG                    | STANDARD                  | 5                                 | 4                                | 90                             | 600                            |
| ENGPOLDOM                    | ACTIVE                       | STANDARD                 | STANDARD                  | 2                                 | 1                                | 30                             | 60                             |
| ENGPOLDOM                    | STANDARD                     | MCENG                    | STANDARD                  | 5                                 | 4                                | 90                             | 600                            |
| ENGPOLDOM                    | STANDARD                     | STANDARD                 | STANDARD                  | 2                                 | 1                                | 30                             | 60                             |
| ENGPOLDOM                    | TEST                         | STANDARD                 | STANDARD                  | 2                                 | 1                                | 30                             | 60                             |

## Beispiel: Ausführliche Informationen zu einer Sicherungskopiengruppe anzeigen

Die gesamten Informationen für die Sicherungskopiengruppe anzeigen, die zur Verwaltungsklasse ACTIVEFILES in der Maßnahmengruppe VACATION der Maßnahmendomäne EMPLOYEE\_RECORDS gehört. Den folgenden Befehl ausgeben:

```
query copygroup employee_records vacation
activefiles format=detailed
```

## Beispiel: Informationen zu der Sicherungskopiengruppe in der Verwaltungsklasse und Maßnahmengruppe STANDARD anzeigen

Von einem verwalteten Server die vollständigen Informationen für die Sicherungskopiengruppe anzeigen, die der Verwaltungsklasse STANDARD in der Maßnahmengruppe STANDARD der Maßnahmendomäne ADMIN\_RECORDS zugeordnet ist. Den folgenden Befehl ausgeben:

```
query copygroup admin_records
standard standard format=detailed
```

```

Name der Maßnahmendomäne: ADMIN_RECORDS
Name der Maßnahmengruppe: STANDARD
Verwaltungsklassenname: STANDARD
Name der Kopiengruppe: STANDARD
Typ der Kopiengruppe: Backup
Versionen bestehender Daten: 2
Versionen gelöschter Daten: 1
Extraversionen aufbewahren: 30
Einzig Version aufbewahren: 60
Kopienmodus: Modified
Kopiennumerierung: Shared Static
Kopienhäufigkeit: 0
Kopienzielort: BACKUPPOOL
Zielort für Inhaltsverzeichnis:
Letzte Aktualisierung durch
(Administrator): $$CONFIG_MANAGER$$
Datum/Zeit der letzten Aktualisierung: 2002.10.02 17.51.49
Verwaltendes Profil: ADMIN_INFO
Änderungen anstehend: Yes
```

## Beispiel: Informationen zu einer Archivierungskopiengruppe anzeigen

Von einem verwalteten Server die vollständigen Informationen über die Archivierungskopiengruppe STANDARD anzeigen, die der Verwaltungsklasse MCLASS1 in der Maßnahmengruppe SUMMER der Maßnahmendomäne PROG1 zugeordnet ist. Den folgenden Befehl ausgeben:

```
query copygroup progl summer mclass1
type=archive format=detailed
```

```

Name der Maßnahmendomäne: PROG1
Name der Maßnahmengruppe: SUMMER
Name der Verwaltungsklasse: MCLASS1
Name der Kopiengruppe: STANDARD
Typ der Kopiengruppe: Archive
Version aufbewahren: 730
Aufbewahrungsstart: Creation
Mindestaufbewahrung:
Kopiennumerierung: Shared Static
Kopienhäufigkeit: Cmd
Kopienmodus: Absolute
Kopienzielort: ARCHPOOL
Letzte Aktualisierung durch
(Administrator): $$CONFIG_MANAGER$$
Datum/Zeit der letzten Aktualisierung: 2002.10.02 17.42.49
Verwaltendes Profil: ADMIN_INFO
```

## Beispiel: Informationen zu der Kopiengruppe für eine NAS-Sicherung anzeigen

---

Die Kopiengruppe für die NAS-Sicherung abfragen. Den folgenden Befehl ausgeben:

```
query copygroup nasdomain
type=backup
```

```
Name der Maßnahmendomäne: NASDOMAIN
Name der Maßnahmengruppe: ACTIVE
Verwaltungsklassenname: STANDARD
Name der Kopiengruppe: STANDARD
Typ der Kopiengruppe: Backup
Versionen bestehender Daten: 2
Versionen gelöschter Daten: 1
Extraversionen aufbewahren: 30
Einzige Version aufbewahren: 60
Kopienmodus: Modified
Kopiennummerierung: Shared Static
Kopienhäufigkeit: 0
Kopienzielort: NASPOOL
Zielort für Inhaltsverzeichnis: BACKUPOOL
Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
Datum/Zeit der letzten Aktualisierung: 10/02/2002 12:16:52
Verwaltendes Profil:
Änderungen anstehend: Yes
```

## Feldbeschreibungen

---

Name der Maßnahmendomäne

Der Name der Maßnahmendomäne.

Name der Maßnahmengruppe

Der Name der Maßnahmengruppe.

Name der Verwaltungsklasse

Der Name der Verwaltungsklasse.

Name der Kopiengruppe

Der Name der Kopiengruppe. Dieser Name lautet immer STANDARD.

Typ der Kopiengruppe

Der Typ der Kopiengruppe.

Versionen bestehender Daten

Die maximale Anzahl Sicherungsversionen, die für Dateien aufbewahrt werden sollen, die sich momentan im Clientdateisystem befinden.

Versionen gelöschter Daten

Die maximale Anzahl Sicherungsversionen, die für Dateien aufbewahrt werden sollen, die aus dem Clientdateisystem gelöscht wurden, nachdem sie mit IBM Spectrum Protect gesichert wurden.

Extraversionen aufbewahren

Die Anzahl Tage, die eine Sicherungsversion aufbewahrt werden soll, nachdem diese Version inaktiv wurde.

Einzige Version aufbewahren

Die Anzahl Tage, die die letzte Sicherungsversion einer Datei aufbewahrt werden soll, die aus dem Clientdateisystem gelöscht wurde.

Kopiennummerierung

Angabe, ob eine Datei während einer Archivierungsoperation verwendet werden darf.

Kopienhäufigkeit

Die Kopienhäufigkeit der Kopiengruppe. Bei Archivierungskopiengruppen lautet dieser Wert immer CMD.

Kopienmodus

Gibt an, daß Dateien in der Kopiengruppe ohne Rücksicht darauf, ob sie geändert wurden, archiviert werden sollen. Bei Archivierungskopiengruppen lautet dieser Wert immer ABSOLUTE.

Kopienzielort

Der Name des Speicherpools, in dem der Server Dateien anfänglich speichert, die dieser Archivierungskopiengruppe zugeordnet sind.

Zielort für Inhaltsverzeichnis

Der Name des primären Speicherpools, in dem Inhaltsverzeichnisse für Imagesicherungsoperationen anfänglich gespeichert werden, bei denen die Generierung eines Inhaltsverzeichnisses angefordert wird.

Letzte Aktualisierung durch (Administrator)

Der Name des Administrators oder Servers, der die Kopiengruppe zuletzt aktualisiert hat. Enthält dieses Feld \$\$CONFIG\_MANAGER\$\$, ist die Kopiengruppe einer Domäne zugeordnet, die von dem Konfigurationsmanager verwaltet wird.

Datum/Zeit der letzten Aktualisierung

Das Datum und die Uhrzeit, an dem bzw. zu der die Kopiengruppe definiert oder zuletzt aktualisiert wurde.




Verwaltendes Profil

Das Profil oder die Profile, für die der verwaltete Server subskribiert hat, um die Definition dieser Maßnahmengruppe zu erhalten. Änderungen anstehend  
 Angabe, ob Änderungen vorgenommen, aber nicht aktiviert werden. Sobald die Änderungen aktiviert werden, wird das Feld auf No zurückgesetzt.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY COPYGROUP

| Befehl           | Beschreibung  |
|------------------|---|
| DEFINE COPYGROUP | Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse. |
| DELETE COPYGROUP | Löscht eine Sicherungs- oder Archivierungskopiengruppe aus einer Maßnahmendomäne und Maßnahmengruppe.                         |
| UPDATE COPYGROUP | Ändert ein oder mehrere Attribute einer Kopiengruppe.   |

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## QUERY DAMAGED (Beschädigte Daten in einem Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool abfragen)

Mit diesem Befehl können Informationen zu beschädigten Datenbereichen in einem Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool angezeigt werden. Verwenden Sie diesen Befehl zusammen mit dem Befehl AUDIT CONTAINER, um eine Wiederherstellungsmethode für die beschädigten Daten festzulegen.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

>>-Query DAMAGED--Poolname--+-Type---Status-----+---<
                               '-Type---+INVENTORY-----+'
                               +-Node--| A |-----+
                               '-CONTAINER--| A |- '

A (Zusätzlicher Filter nach Knotenname)

|-----+-----|
  '-Nodename---Knotenname-'
  
```

### Parameter

Poolname (Erforderlich)

Gibt den Namen des Verzeichniscontainer- oder Cloudspeicherpools an.

Type

Gibt den Typ der Informationen an, die angezeigt werden sollen. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

Status

Gibt an, dass Informationen zu beschädigten Datenbereichen angezeigt werden. Für Cloudspeicherpools werden auch verwaiste Bereiche angezeigt. Dies ist der Standardwert.

Knoten

Gibt an, dass Informationen zur Anzahl beschädigter Dateien pro Knoten angezeigt werden sollen.

INVENTORY

Gibt an, dass Informationen zum Bestand für jede beschädigte Datei angezeigt werden.

CONTAINER

Gibt an, dass die Container, die beschädigte Datenbereiche oder verwaiste Bereiche in Cloudspeicherpools enthalten, angezeigt werden. Für Verzeichniscontainerspeicherpools werden auch Speicherpoolverzeichnisse angezeigt.

## Nodename

Gibt an, dass Informationen zu beschädigten Dateien für einen einzelnen Knoten angezeigt werden.

Einschränkung: Sie können diesen Parameter nicht angeben, wenn der Parameter TYPE=CONTAINER oder TYPE=STATUS angegeben wird.

## Beispiel: Statusinformationen zu beschädigten oder verwaisten Datenbereichen anzeigen

Informationen zum Status beschädigter Datenbereiche anzeigen, die in einem Container gespeichert sind.

```
query damaged pool1 type=status
```

| Speicherpool-<br>name | Anzahl nicht<br>deduplizierter<br>Datenbereiche | Anzahl<br>deduplizierter<br>Datenbereiche | Anzahl verwaister<br>Bereiche in Cloud-<br>speicherpools |
|-----------------------|---|---|--|
| -----                 | -----   | -----                                     | -----  |
| POOL1                 | 58  | 145                                       |  |

Für Cloudspeicherpools wird auch die Anzahl verwaister Bereiche angezeigt.

| Speicherpool-<br>name | Anzahl nicht<br>deduplizierter<br>Datenbereiche | Anzahl<br>deduplizierter<br>Datenbereiche | Anzahl verwaister<br>Bereiche in Cloud-<br>speicherpools |
|-----------------------|---|---|--|
| -----                 | -----   | -----                                     | -----  |
| POOL1                 | 65  | 238                                       | 18   |

## Beispiel: Informationen zu einer beschädigten Datei für einen Knotentyp anzeigen

Informationen zu beschädigten Dateien anzeigen, die in einem Knoten gespeichert werden.

```
query damaged pool1 type=node
```

| Knotenname | Anzahl beschädigter<br>Dateien |
|------------|--------------------------------|
| -----      | -----                          |
| POOL1      | 37                             |

## Beispiel: Informationen zu einer beschädigten Datei für einen Bestandstyp anzeigen

Informationen zu beschädigten Dateien anzeigen, die in einem Bestand gespeichert werden.

```
query damaged pool2 type=inventory
```

```
Dateiname des Clients: /data/files/10.out
                          Typ: Bkup
                          Knotenname: NODE1
                          Dateibereichsname: /data/space
                          Status: Available
                          Einfügezeit: 01/19/2015 16:01:35
                          Objekt-ID: 2073
```

## Beispiel: Informationen zu einer beschädigten Datei für einen Containertyp anzeigen

Informationen zu beschädigten Dateien anzeigen, die in einem Container gespeichert werden.

```
query damaged pool3 type=container
```

```
Verzeichnis-ID: 1
Verzeichnis: /abc/space/container1
Container: /abc/space/container1/00/0000000000000022.dcf
Status: Unavailable
```

Für Cloud-Container wird nur der Name des Containers angezeigt.

```
Verzeichnis-ID:
Verzeichnis:
Container: ibmsp.12520ae05b4011e613320a0027000000/
          001-10006a3278bc34f0e4118a850090fa3dcb48/
          00000000000001.ncf
Status:
```

Für den lokalen Speicher werden die folgenden Informationen zu einem beschädigten Container angezeigt.

```
Verzeichnis-ID: 1
Verzeichnis: localdirectory
```



## Feldbeschreibungen

---

Dateiname des Clients (nur bei TYPE=INVENTORY)

Der Name der Datei.

Anzahl verwaister Bereiche in Cloudspeicherpools (nur bei TYPE=STATUS)

Die Anzahl verwaister Bereiche in einem Cloudspeicherpool. Bereiche werden als verwaist betrachtet, wenn sie keinen entsprechenden Datenbankeintrag haben.

Container (nur bei TYPE=CONTAINER)

Der Name des Containers.

Anzahl deduplizierter Bereiche (nur bei TYPE=STATUS)

Die Anzahl beschädigter Bereiche im Speicherpool für deduplizierte Daten.

Verzeichnis (nur bei TYPE=CONTAINER)

Der Name des Speicherpoolverzeichnisses.

Verzeichnis-ID (nur bei TYPE=CONTAINER)

Die Identifikationsnummer des Speicherpoolverzeichnisses.

Dateibereichsname (nur bei TYPE=INVENTORY)

Der Name des Dateibereichs.

Einfügezeit (nur bei TYPE=INVENTORY)

Das Datum und die Uhrzeit, an dem bzw. zu der das Objekt auf dem Server gespeichert wurde.

Knotenname (nur bei TYPE=INVENTORY oder TYPE=NODE)

Der Name des Knotens.

Anzahl nicht deduplizierter Bereiche (nur bei TYPE=STATUS)

Die Anzahl beschädigter Bereiche im Speicherpool für nicht deduplizierte Daten, wie beispielsweise Metadaten und vom Client verschlüsselte Daten.

Anzahl beschädigter Dateien (nur bei TYPE=NODE)

Die Anzahl beschädigter Dateien pro Knoten.

Objekt-ID (nur bei TYPE=INVENTORY)

Die Identifikationsnummer des Objekts.

Status (nur bei TYPE=INVENTORY oder TYPE=CONTAINER)

Der Status der Daten im Bestand oder Container, abhängig vom Typ der Daten, die abgefragt werden. Das Feld kann einen der folgenden Werte enthalten:

Active

Die Version der Datei im Bestand ist aktiv. Es kann nur eine aktive Version der Datei im Bestand vorhanden sein.

Inactive

Die Version der Datei im Bestand ist inaktiv. Es können mehrere inaktive Versionen der Datei im Bestand vorhanden sein.

Available

Der Status des Containers ist 'verfügbar'.

Unavailable

Der Status des Containers ist 'nicht verfügbar'. Beispielsweise kann ein Container nicht verfügbar sein, wenn der Header beschädigt ist oder der Container nicht geöffnet werden kann.

Read-Only

Der Container hat den Status 'Nur lesen'. Daten in dem Container können gelesen werden, aber es können keine Daten in den Container geschrieben werden.

Pending

Das Löschen des Containers ist anstehend. Der Inhalt des Containers wurde in einen anderen Container versetzt und der Container kann jetzt gelöscht werden.

Typ (nur bei TYPE=INVENTORY)

Der Typ der Daten in der Datei.

Tabelle 1. Zugehörige Befehle für QUERY DAMAGED

| Befehl          | Beschreibung  |
|-----------------|---|
| AUDIT CONTAINER | Prüft einen Verzeichniscontainerspeicherpool.               |
| QUERY CLEANUP   | Fragt den Bereinigungsstatus eines Quellenspeicherpools ab. |

| Befehl          | Beschreibung  |
|-----------------|---|
| QUERY CONTAINER | Zeigt Informationen zu einem Container an.                |
| REMOVE DAMAGED  | Entfernt beschädigte Daten aus einem Quellenspeicherpool. |

## QUERY DATAMOVER (Definitionen der Einheit zum Versetzen von Daten anzeigen)

Verwenden Sie diesen Befehl, um Definitionen der Einheit zum Versetzen von Daten anzuzeigen.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query DATAMover----->
. -*-----
>+----->
  '-Name_der_Einheit_zum_Versetzen_von_Daten-'
. -Format----Standard----.
>+----->
  '-Format----+Standard-+'
    '-Detailed-'
. -Type----*-----
>+-----><
  |                                     (1) (2) |
  '-Type----+NAS-----+'
    +-NASCLUSTER-+
    '-NASVSERVER-'
```

Anmerkungen:

1. Bei FORMAT=DETAILED müssen Sie den Parameter TYPE angeben.
2. Sie können TYPE=NASCLUSTER und TYPE=NASVSERVER nur auf einem AIX-, Linux- oder Windows-Betriebssystem angeben.

### Parameter

Name der Einheit zum Versetzen von Daten

Gibt den Namen der Einheit zum Versetzen von Daten an, die angezeigt werden soll. Sie können mehrere Namen mit einem Platzhalterzeichen angeben. Standardmäßig werden alle Einheiten zum Versetzen von Daten angezeigt.

Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD.

Standard

Gibt an, dass Informationen zum Namen und zur Adresse angezeigt werden.

Detailed


Gibt an, dass die gesamten Informationen angezeigt werden.




Type

Gibt den Typ der Einheit zum Versetzen von Daten an, die angezeigt werden soll. Wenn Sie FORMAT=DETAILED angeben, müssen Sie einen Wert für den Parameter TYPE angeben.




NAS

Gibt einen NAS-Dateiserver an.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme NASCLUSTER

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme Gibt einen NAS-Dateiserver in einem Cluster an.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme NASVSERVER

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme Gibt eine virtuelle Speichereinheit innerhalb eines Clusters an.

## Beispiel: Informationen zu allen Einheiten zum Versetzen von Daten anzeigen

---

Die Einheiten zum Versetzen von Daten auf dem Server anzeigen. Den folgenden Befehl ausgeben:

```
query datamover
```

| Name der Einheit zum Versetzen von Daten | Typ der Einheit zum Versetzen von Daten | Online |
|--|---|--------|
| NASMOVER1                                | NAS                                     | Yes    |
| NASMOVER2                                | NAS                                     | No     |

Für Felddesreibungen siehe Felddesreibungen.

## Beispiel: Informationen zu einer Einheit zum Versetzen von Daten anzeigen

---

Teilinformationen zu der Einheit zum Versetzen von Daten DATAMOVER6 anzeigen. Den folgenden Befehl ausgeben:

```
query datamover datamover6 type=nas
```

| Quellename | Typ | Online |
|------------|-----|--------|
| DATAMOVER6 | NAS | Yes    |

Für Felddesreibungen siehe Felddesreibungen.

## Beispiel: Ausführliche Informationen zu einer Einheit zum Versetzen von Daten anzeigen


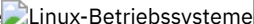

---

Ausführliche Informationen zur Einheit zum Versetzen von Daten DATAMOVER6 anzeigen. Der Parameter TYPE ist bei FORMAT = DETAILED erforderlich. Den folgenden Befehl ausgeben:

```
query datamover datamover6 format=detailed type=nas
```

```
Name der Einheit zum Versetzen von Daten: DataMover6
Typ der Einheit zum Versetzen von Daten: NAS
IP-Adresse: 198.51.100.0
TCP/IP-Anschlussnummer: 10000
Benutzername: NDMPadmin
Speicherpooldatenformat: NDMPDUMP
Online: Yes
Letzte Aktualisierung durch (Administrator): ADMIN
Datum/Zeit der letzten Aktualisierung: 05/23/2015 09:26:33
```

Für Felddesreibungen siehe Felddesreibungen.

## Beispiel: Ausführliche Informationen zu einer NAS-Einheit zum Versetzen von Daten in einem Cluster anzeigen

---

Beispiel: Ausführliche Informationen zu einer NAS-Einheit zum Versetzen von Daten (mit dem Namen CLUSTERA) in einem Cluster anzeigen. Geben Sie den folgenden Befehl aus:

```
query datamover clustera format=detailed type=nascluster
```

```
Name der Einheit zum Versetzen von Daten: CLUSTERA
Typ der Einheit zum Versetzen von Daten: NASCLUSTER
IP-Adresse: 192.0.2.255
TCP/IP-Anschlussnummer: 10000
Benutzername: ndmp
Speicherpooldatenformat: NETAPPDUMP
Online: Yes
Letzte Aktualisierung durch (Administrator): ADMIN
Datum/Zeit der letzten Aktualisierung: 04/28/2015 09:26:33
```

Für Felddesreibungen siehe Felddesreibungen.

## Felddesreibungen

---

Name der Einheit zum Versetzen von Daten

Gibt den Namen der Einheit zum Versetzen von Daten an.

Typ der Einheit zum Versetzen von Daten

- Gibt den Typ der Einheit zum Versetzen von Daten an.
- IP-Adresse
  - Gibt die IP-Adresse der Einheit zum Versetzen von Daten an.
- TCP/IP-Anschlussnummer
  - Gibt die TCP-Anschlussnummer für die Einheit zum Versetzen von Daten an.
- Benutzername
  - Gibt die Benutzer-ID an, die der Server verwendet, um auf die Einheit zum Versetzen von Daten zuzugreifen.
- Speicherpooldatenformat
  - Gibt das Datenformat an, das von der Einheit zum Versetzen von Daten verwendet wird.
- Online
  - Gibt an, ob die Einheit zum Versetzen von Daten online und für die Verwendung verfügbar ist.
- Letzte Aktualisierung durch (Administrator)
  - Gibt die ID des Administrators an, der die letzte Aktualisierung ausgeführt hat.
- Datum/Zeit der letzten Aktualisierung
  - Gibt das Datum und die Uhrzeit der letzten Aktualisierung an.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DATAMOVER

| Befehl           | Beschreibung  |
|------------------|---|
| DEFINE DATAMOVER | Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server. |
| DELETE DATAMOVER | Löscht eine Einheit zum Versetzen von Daten.  |
| UPDATE DATAMOVER | Ändert die Definition einer Einheit zum Versetzen von Daten.                        |

## QUERY DB (Datenbankinformationen anzeigen)

Mit diesem Befehl können Informationen über die Datenbank angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

.-Format-----Standard-----
>>-Query DB--+-----+-----><
'-Format-----+Standard-+-'
                '-Detailed-'

```

### Parameter

- Format
  - Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Die folgenden Werte sind gültig:
- Standard
  - Gibt an, dass Teilinformationen angezeigt werden.
- Detailed
  - Gibt an, dass die gesamten Informationen angezeigt werden.

### Beispiel: Übersichtsstatistik zur Datenbank anzeigen

Statistikdaten zur Datenbank anzeigen. Den folgenden Befehl ausgeben:

```
query db
```

| Datenbank-<br>name | Gesamt-<br>seitenzahl | Verwendbare<br>Seiten | Belegte<br>Seiten | Freie<br>Seiten |
|--------------------|-----------------------|-----------------------|-------------------|-----------------|
| TSMDB1             | 32.776                | 32.504                | 24.220            | 8.284           |

Für Felddesreibungen siehe Felddesreibungen.

## Beispiel: Ausführliche Datenbankinformationen anzeigen

---

Ausführliche statistische Informationen zur Datenbank anzeigen. Den folgenden Befehl ausgeben:

```
query db format=detailed
```

```
Datenbankname: TSM_DB2
GesamtSpeicherbereich des Dateisystems (MB): 1.748.800
Verwendeter Speicherbereich im Dateisystem (MB): 2.304.355
Von Datenbank verwendeter Speicherbereich (MB): 448
Freier verfügbarer Speicherbereich (MB): 235.609
Gesamtseitenzahl: 32.776
Verwendbare Seiten: 32.504
Belegte Seiten: 24.220
Freie Seiten: 8.284
Pufferpooltrefferquote: 99,3
Pufferanforderungen insgesamt: 204.121
Sortierüberlauf: 0
Paketcachetrefferquote: 89,8
Letzte Datenbankreorganisation: 05/25/2009 16:44:06
Einheitenklassenname für Gesamtsicherungen: FILE
Anzahl Datenbanksicherungsdatenströme: 4
Teilsicherungen seit letzter Gesamtsicherung: 0
Datum/Zeit der letzten Gesamtsicherung: 05/18/2009 22:55:19
Datenbanksicherungen komprimieren: Yes
Masterverschlüsselungsschlüssel schützen: No
```


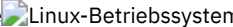
Für Felddesreibungen siehe Felddesreibungen.

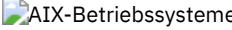
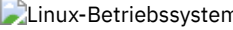
## Felddesreibungen

---

### Datenbankname

Der Name der Datenbank, die für die Verwendung durch den IBM Spectrum Protect-Server definiert und konfiguriert ist.

  GesamtSpeicherbereich des Dateisystems (MB)

  Der GesamtSpeicherbereich in Megabyte der Dateisysteme, in denen sich die Datenbank befindet.

 GesamtSpeicherbereich des Dateisystems (MB)

 Der GesamtSpeicherbereich in Megabyte der Laufwerke, auf denen sich die Datenbank befindet.

### Verwendeter Speicherbereich im Dateisystem (MB)

Der Datenbankbereich in Megabyte, der verwendet wird.

### Von der Datenbank verwendeter Speicherbereich (MB)

Die Größe der Datenbank in Megabyte. Der Wert schließt keinen Tabellenbereich für temporäre Tabellen ein. Die Größe der Datenbank wird anhand der Größe des Speicherbereichs berechnet, der auf dem Dateisystem, das die Datenbank enthält, belegt ist.

### Freier verfügbarer Speicherbereich (MB)

Der Datenbankbereich in Megabyte, der nicht verwendet wird.

### Gesamtseitenzahl

Die Gesamtzahl der Seiten im Tabellenbereich.

### Verwendbare Seiten

Die Anzahl der verwendbaren Seiten im Tabellenbereich.

### Belegte Seiten

Die Anzahl der belegten Seiten im Tabellenbereich.

### Freie Seiten

Die Gesamtzahl der freien Seiten in allen Tabellenbereichen. Die IBM Spectrum Protect-Datenbank hat bis zu 10 Tabellenbereiche.

### Pufferpooltrefferquote

Die Gesamttrefferquote in Prozent.

### Pufferanforderungen insgesamt

Die Gesamtzahl der logischen Lesevorgänge für Pufferpooldaten und der logischen Lesevorgänge für Indexeinträge seit dem letzten Start der Datenbank oder seit dem Zurücksetzen des Datenbankmonitors.

### Sortierüberlauf

Die Gesamtzahl der Sortiervorgänge, die den Sortierspeicher überschritten haben und möglicherweise Plattenspeicherplatz für temporären Speicher erfordern.

### Paketcachetrefferquote

Ein Prozentsatz, der angibt, in welchem Umfang der Paketcache hilft, das erneute Laden von Paketen und Abschnitten für statisches SQL aus den Systemkatalogen zu vermeiden. Außerdem gibt der Prozentsatz an, inwieweit der Paketcache dabei hilft,

das erneute Kompilieren von Anweisungen für dynamisches SQL zu vermeiden. Eine hohe Trefferquote gibt eine erfolgreiche Unterstützung bei der Vermeidung dieser Aktivitäten an.

Letzte Datenbankreorganisation

Der Zeitpunkt, zu dem der Datenbankmanager zuletzt eine automatische Reorganisationsaktivität ausgeführt hat.

Einheitenklassenname für Gesamtsicherungen

Der Name der Einheitenklasse, die für Datenbankgesamtsicherungen verwendet wird.

Anzahl Datenbanksicherungsdatenströme

Die Anzahl der parallelen Datenversetzungsdatenströme, die während der Datenbanksicherung verwendet wurden.

Teilsicherungen seit letzter Gesamtsicherung

Die Anzahl der Teilsicherungen, die seit der letzten Gesamtsicherung ausgeführt wurden.

Datum/Zeit der letzten Gesamtsicherung

Das Datum und die Uhrzeit der letzten Gesamtsicherung.

Datenbanksicherungen komprimieren

Gibt an, ob Datenbanksicherungen komprimiert werden.

Masterverschlüsselungsschlüssel schützen

Gibt an, ob Datenbanksicherungen eine Kopie des Masterverschlüsselungsschlüssels des Servers einschließen.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DB

| Befehl         | Beschreibung   |
|----------------|--|
| BACKUP DB      | Sichert die IBM Spectrum Protect-Datenbank auf Datenträgern mit sequenziellem Zugriff.                 |
| EXTEND DBSPACE | Fügt Verzeichnisse hinzu, um den Speicherbereich für die Verwendung durch die Datenbank zu vergrößern. |
| QUERY DBSPACE  | Zeigt Informationen zum Speicherplatz an, der für die Datenbank definiert ist.                         |

## QUERY DBSPACE (Datenbankspeicherbereich anzeigen)

Verwenden Sie diesen Befehl, um Informationen zu den Verzeichnissen anzuzeigen, die von der Datenbank zum Speichern von Daten verwendet werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-QUERY DBSpace-----<<
```

### Parameter

Keine.


### Beispiel: Informationen zum Datenbankspeicherbereich anzeigen

Informationen zum Datenbankspeicherbereich anzeigen. Den folgenden Befehl ausgeben:

```
query dbspace
```

 Linux-Betriebssysteme

| Position  | Gesamtspeicherber.<br>des Dateisystems<br>(MB) | Verw. Sp.-Ber.<br>im Dateisystem<br>(MB) | Freier verfügbarer<br>Speicherbereich<br>(MB) |
|-----------|--|--|---|
| /tsmdb001 | 1,748,800                                      | 1,513,191.125                            | 117,804.422                                   |
| /tsmdb002 | 1.748.800                                      | 1.513.191,125                            | 117.804,422                                   |

 Windows-Betriebssysteme

| Position     | Gesamtspeicherber.<br>des Dateisystems<br>(MB) | Verw. Sp.-Ber.<br>im Dateisystem<br>(MB) | Freier verfügbarer<br>Speicherbereich<br>(MB) |
|--------------|--|--|---|
| d:\tsm\db001 | 1.748.800                                      | 1.513.191,125                            | 117.804,422                                   |
| e:\tsm\db002 | 1.748.800                                      | 1.513.191,125                            | 117.804,422                                   |

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Feldbeschreibungen

### Position

Gibt die Positionen der Datenbankverzeichnisse an.

Gesamtspeicherbereich des Dateisystems (MB)

Der Gesamtspeicherbereich in Megabyte des Dateisystems, in dem sich die Datenbank befindet.

Gesamtspeicherbereich des Dateisystems (MB)

Der Gesamtspeicherbereich in Megabyte der Laufwerke, auf denen sich die Datenbank befindet.

### Verwendeter Speicherbereich im Dateisystem (MB)

Der Speicherbereich in Megabyte, der verwendet wird.

Wenn Sie den Befehl QUERY DBSPACE ausführen, kann der Wert in der Ausgabe größer als der Wert sein, den Sie bei der Ausführung des Systembefehls df erhalten. Die Ausgabe des Systembefehls df enthält nicht den Speicherbereich, der für den Rootbenutzer reserviert ist.

Wenn Sie den Systembefehl df ausführen, beträgt der Standardprozentsatz des Speicherbereichs, der für den Rootbenutzer reserviert ist, 5 %. Sie können diesen Standardwert ändern.

### Freier verfügbarer Speicherbereich (MB)

Der Speicherbereich in Megabyte, der nicht verwendet wird.

Freier verfügbarer Speicherbereich (MB)

Der Speicherbereich, der auf dem Laufwerk verbleibt, auf dem sich das Verzeichnis befindet.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DBSPACE

| Befehl         | Beschreibung   |
|----------------|--|
| BACKUP DB      | Sichert die IBM Spectrum Protect-Datenbank auf Datenträgern mit sequenziellem Zugriff.                 |
| EXTEND DBSPACE | Fügt Verzeichnisse hinzu, um den Speicherbereich für die Verwendung durch die Datenbank zu vergrößern. |
| QUERY DB       | Zeigt Zuordnungsinformationen zu der Datenbank an.   |

## QUERY DEDUPSTATS (Dateneduplizierungsstatistikdaten abfragen)

Verwenden Sie diesen Befehl, um Informationen zu Dateneduplizierungsstatistikdaten für einen Verzeichniscontainerspeicherpool oder einen Cloudspeicherpool anzuzeigen.

Sie müssen den Befehl GENERATE DEDUPSTATS ausgeben, bevor Sie den Befehl QUERY DEDUPSTATS ausgeben können.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-Query DEDUPSTATs----->
      '-Poolname-' '-Knotenname-'

  .-*----- .-Format---Standard-----
>>----->
  | .-,----- | '-Format---Standard-+-'
  | v           | | '-Detailed-'
+---Dateibereichsname---+
```

```

| .-,------ . |
| V | |
|-----FSID-----|
. -CODEType----BOTH----- .
>-----+----->
'-CODEType----+-UNICODE----+'
          +-NONUNICODE-+
          '-BOTH-----'

. -NAMEType----SERVER----- .
>-----+-----+-----+----->
'-NAMEType----+-SERVER--+-' '-BEGINDate----Datum-'
          +-UNICODE-+
          '-FSID----'

>-----+-----+-----+----->
'-BEGINTime----Zeit-' '-ENDDate----Datum-'

. -ALLStats----No----- .
>-----+-----+-----+-----<
'-ENDTime----Zeit-' '-ALLStats----+-Yes-+-'
                                     '-No--'

```

## Parameter

### Poolname

Gibt den Namen des Verzeichniscontainerspeicherpools an, dessen Daten in den Datendeduplizierungsstatistikdaten enthalten sind. Dieser Parameter ist wahlfrei. Wird kein Wert für diesen Parameter angegeben, werden alle Speicherpools angezeigt. Für den Speicherpoolnamen können bis zu 30 Zeichen angegeben werden. Wenn Sie mehr als 30 Zeichen angeben, schlägt der Befehl fehl.

Einschränkung: Sie können nur Verzeichniscontainerspeicherpools oder Cloudspeicherpools angeben.

### Knotenname

Gibt den Namen des Clientknotens an, dessen Daten in den Datendeduplizierungsstatistikdaten enthalten sind. Dieser Parameter ist wahlfrei. Wird für diesen Parameter kein Wert angegeben, werden alle Knoten angezeigt. Für den Knotennamen können bis zu 64 Zeichen angegeben werden. Wenn Sie mehr als 64 Zeichen angeben, schlägt der Befehl fehl.

### Dateibereichsname oder FSID

Gibt die Namen der Dateibereiche an, die die Daten enthalten, die in den Datendeduplizierungsstatistikdaten berücksichtigt werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Dateibereiche angezeigt. Es können mehrere Dateibereiche angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden.

Für einen Server, der über Clients mit Unterstützung für Dateibereiche im Unicode-Format verfügt, können Sie entweder einen Dateibereichsnamen oder eine Dateibereichs-ID (FSID) angeben. Wird ein Dateibereichsname eingegeben, muss der Server möglicherweise den eingegebenen Dateibereichsnamen konvertieren. Beispielsweise muss der Server gegebenenfalls den Namen, den Sie eingeben, aus der Zeichenumsetztabelle des Servers in Unicode konvertieren.

Einschränkungen: Die folgenden Einschränkungen gelten für Dateibereichsnamen und FSIDs:

- Ein Knotenname muss angegeben werden, wenn ein Dateibereichsname angegeben wird.
- Mischen Sie nicht Dateibereichsnamen und FSIDs in demselben Befehl.

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

#### Standard

Gibt an, dass Teilinformationen für die angegebenen Datendeduplizierungsgruppen angezeigt werden. Dies ist der Standardwert.

#### Detailed

Gibt an, dass vollständige Information für die angegebenen Datendeduplizierungsgruppen angezeigt werden.

### CODEType

Geben Sie an, welcher Typ von Dateibereichen in der Operation berücksichtigt werden soll. Der Standardwert lautet BOTH. Dieser Standardwert gibt an, dass Dateibereiche unabhängig vom Typ der Codepage eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben. Geben Sie einen der folgenden Werte an:

#### UNICODE

Dateibereiche einschließen, die ein Unicode-Format haben.

#### NONUNICODE

Dateibereiche einschließen, die kein Unicode-Format haben.



BOTH

Dateibereiche unabhängig von der Art der Zeichenumsetzungstabelle einschließen. Dies ist der Standardwert.

#### NAMETYPE

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unterstützung für Dateibereiche im Unicode-Format verfügt. Sie können diesen Parameter für IBM Spectrum Protect-Clients angeben, die die Betriebssysteme Windows, NetWare oder Macintosh OS X verwenden. Verwenden Sie diesen Parameter nur, wenn Sie einen Knotennamen und einen Dateibereichsnamen oder eine FSID eingeben. Einschränkung: Wenn Sie diesen Parameter angeben, darf der Dateibereichsname kein Platzhalterzeichen enthalten.

Geben Sie einen der folgenden Werte an:

#### SERVER

Der Server verwendet die Zeichenumsetzungstabelle des Servers, um die Dateibereichsnamen zu interpretieren. Dies ist der Standardwert.

#### UNICODE

Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetzungstabelle in die Zeichenumsetzungstabelle UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetzungstabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetzungstabelle nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

#### FSID

Der Server interpretiert die Dateibereichsnamen als ihre FSIDs.

#### BEGINDATE

Gibt das Startdatum zum Abfragen von Dateneduplizierungsstatistikdaten an. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter BEGINTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird ein Anfangsdatum ohne eine Anfangszeit angegeben, lautet die Zeit 24:00 (Mitternacht) an dem angegebenen Datum. Einschränkung: Sie können diesen Parameter nur angeben, wenn Sie den Parameter ALLSTATS=YES angeben.

Geben Sie einen der folgenden Werte an:

| Wert                           | Beschreibung  | Beispiel   |
|--------------------------------|---|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum.                                     | 09/15/2015   |
| TODAY                          | Das aktuelle Datum.                                       | TODAY  |
| TODAY-Tage oder -Tage          | Das aktuelle Datum minus der Anzahl der angegebenen Tage. | TODAY -3 oder -3.  |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.                             | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.       | EOLM-1<br>Um Sätze einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.                       | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.  | BOTM+9<br>Um Sätze einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

#### BEGINTIME

Gibt die Startzeit zum Abfragen der Dateneduplizierungsstatistikdaten an. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter BEGINDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird eine Anfangszeit ohne ein Anfangsdatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Uhrzeit. Einschränkung: Sie können diesen Parameter nur angeben, wenn Sie den Parameter ALLSTATS=YES angeben.

Geben Sie einen der folgenden Werte an:

| Wert                  | Beschreibung  | Beispiel               |
|-----------------------|---|------------------------|
| HH:MM:SS              | Eine bestimmte Uhrzeit.   | 10:30:08               |
| NOW                   | Die aktuelle Uhrzeit.   | NOW                    |
| NOW+HH:MM oder +HH:MM | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.  | NOW+02:00 oder +02:00. |
| NOW-HH:MM oder -HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten. | NOW-02:00 oder -02:00. |

## ENDDate

Gibt das Enddatum zum Abfragen von Dateneduplizierungsstatistikdaten an. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter ENDTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird ein Enddatum ohne eine Endzeit angegeben, lautet die Zeit 23:59:59 am angegebenen Enddatum.

Einschränkung: Sie können diesen Parameter nur angeben, wenn Sie den Parameter ALLSTATS=YES angeben.

Geben Sie einen der folgenden Werte an:

| Wert                           | Beschreibung  | Beispiel   |
|--------------------------------|---|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum                                      | 09/15/1999   |
| TODAY                          | Das aktuelle Datum  | TODAY  |
| TODAY-Tage oder -Tage          | Das aktuelle Datum minus der Anzahl der angegebenen Tage. | TODAY -3 oder -3.  |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.                             | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.       | EOLM-1<br>Um Sätze einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.                       | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.  | BOTM+9<br>Um Sätze einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

## ENDTime

Gibt die Endzeit des Bereichs an, für den die Dateneduplizierungsstatistikdaten abgefragt werden sollen. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter ENDDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird eine Endzeit ohne ein Enddatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Zeit.

Einschränkung: Sie können diesen Parameter nur angeben, wenn Sie den Parameter ALLSTATS=YES angeben.

Geben Sie einen der folgenden Werte an:

| Wert                  | Beschreibung   | Beispiel               |
|-----------------------|--|------------------------|
| HH:MM:SS              | Eine bestimmte Uhrzeit.  | 10:30:08               |
| NOW                   | Die aktuelle Uhrzeit.  | NOW                    |
| NOW+HH:MM oder +HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum  | NOW+02:00 oder +02:00. |
| NOW-HH:MM oder -HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum | NOW-02:00 oder -02:00. |

## ALLStats

Gibt an, ob alle Dateneduplizierungsstatistikdaten oder nur die zuletzt generierten Dateneduplizierungsstatistikdaten angezeigt werden sollen. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

No

Zeigt nur die zuletzt generierten Dateneduplizierungsstatistikdaten für jeden Knoten und Dateibereich an.

Yes

Zeigt alle Dateneduplizierungsstatistikdaten an.

## Beispiel: Dateneduplizierungsstatistikdaten im Standardformat anzeigen

Dateneduplizierungsstatistikdaten für einen Speicherpool mit dem Namen POOL1 anzeigen. Die Dateneduplizierungsstatistikdaten gelten für den Knoten NODE1; es werden die Statistikdaten vom 8. Mai 2015 angezeigt. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query dedupstats pool1 node1 begindate=05/08/2015
```

```
Datum/Zeit: 05/05/2015 15:15:23
Speicherpoolname: POOL1
Knotenname: NODE1
Dateibereichsname: \\fs1\al
FSID: 41
Typ: Bkup
Gesamteinsparung in Prozent: 86,62
Geschützte Daten insgesamt (MB): 311
```

## Beispiel: Ausführliche Dateneduplizierungsstatistikdaten anzeigen

---

Ausführliche Informationen zur Dateneduplizierung für einen Speicherpool mit dem Namen POOL1 anzeigen.

```
query dedupstats pool1 format=detailed
```

```

Datum/Zeit: 05/05/2015 15:15:23
Speicherpoolname: POOL1
Knotenname: NODE1
Dateibereichsname: \\fs1\al
FSID: 41
Typ: Bkup
Geschützte Daten insgesamt (MB): 47.646
Gesamtspeicherbereichsbelegung (MB): 10.139
Eingesparter Gesamtspeicherbereich (MB): 37.507
Gesamteinsparung in Prozent: 78,72
Deduplizierungseinsparungen: 16.228.107.499
Deduplizierung in Prozent: 42,59
Anzahl nicht deduplizierter Bereiche: 1.658
Von nicht deduplizierten Bereichen belegter Speicherbereich: 732.626
Anzahl eindeutiger Bereiche: 189.791
Vom eindeutigen Bereich belegter Speicherbereich: 23.385.014.635
Anzahl gemeinsam genutzter Bereiche: 178.712
Geschützte gemeinsam genutzte Datenbereiche: 26.575.010.669
Von gemeinsam genutzten Bereichen belegter Speicherbereich: 5.267.815.421
Komprimierungseinsparungen: 5.267.815.421
Komprimierung in Prozent: 62,93
Anzahl komprimierter Bereiche: 352.498
Anzahl nicht komprimierter Bereiche: 17.663
Von verschlüsselten Bereichen belegter Speicherbereich: 52.901.672
Verschlüsselung in Prozent: 100,00
Anzahl verschlüsselter Bereiche: 188
Anzahl nicht verschlüsselter Bereiche: 0
```

## Feldbeschreibungen

---

Datum/Zeit

Zeigt das Datum und die Uhrzeit an, am dem bzw. zu der die Dateneduplizierungsstatistikdaten generiert werden.

Speicherpoolname

Der Name des Speicherpools.

Knotenname

Der Name des Clientknotens, dessen Daten in den Dateneduplizierungsstatistikdaten enthalten sind.

Dateibereichsname

Der Name des Dateibereichs.

FSID

Der Name der Dateibereichs-ID.

Typ

Der Datentyp. Die folgenden Werte sind gültig:

Arch

Daten, die archiviert wurden.

Bkup

Daten, die gesichert wurden.

SpMg

Daten, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

Geschützte Daten insgesamt (MB)

Das logische Datenvolumen (in Megabyte), das im Speicherpool geschützt wird, vor der Dateneduplizierung und -komprimierung. Dieser Wert stellt die Summe der Werte für Gesamtspeicherbereichsbelegung (MB) und Eingesparter Gesamtspeicherbereich (MB) dar.

Gesamtspeicherbereichsbelegung (MB)

Der im Speicherpool belegte Gesamtspeicherbereich in Megabyte. Dieser Wert ist das physische Datenvolumen, das nach der Dateneduplizierung und -komprimierung gesichert wird.

Eingesparter Gesamtspeicherbereich (MB)

Der Gesamtspeicherbereich in Megabyte der Daten, die aufgrund der Dateneduplizierung und Komprimierung aus dem Speicherpool entfernt werden. Dieser Wert stellt die Summe der Werte für Deduplizierungseinsparungen und Komprimierungseinsparungen dar.

Gesamteinsparung in Prozent

Der Prozentsatz der Daten, die aufgrund der Komprimierung und Datendeduplizierung aus dem Speicherpool entfernt werden.  
 Deduplizierungseinsparungen  
 Der Umfang des belegten Speicherbereichs, der im Speicherpool aufgrund der Datendeduplizierung eingespart wird.  
 Deduplizierung in Prozent  
 Der Prozentsatz der Daten, die aufgrund der Datendeduplizierung aus dem Speicherpool entfernt werden.  
 Anzahl nicht deduplizierter Bereiche  
 Die Anzahl nicht deduplizierter Datenbereiche im Speicherpool.  
 Von nicht deduplizierten Bereichen belegter Speicherbereich  
 Der Umfang des Speicherbereichs, der von Datenbereichen belegt wird, die im Speicherpool nicht dedupliziert werden. Dieser Wert gilt Container mit dem Dateityp .ncf, die keine deduplizierten Daten enthalten.  
 Tipp: Datenbereiche, die nicht dedupliziert sind, bestehen aus den folgenden Daten- oder Dateitypen:

- Dateimetadaten
- Dateien mit einer Größe von weniger als 2 KB
- Dateien, die die Clientverschlüsselung verwenden

Anzahl eindeutiger Bereiche  
 Die Anzahl Datenbereiche, die nicht von einem Knoten gemeinsam genutzt werden.  
 Vom eindeutigen Bereich belegter Speicherbereich  
 Der Umfang des Speicherbereichs im Speicherpool, der von einem Knoten nicht gemeinsam genutzt wird. Dieser Wert gilt Container mit dem Dateityp .dcf, die keine deduplizierten Daten enthalten.  
 Anzahl gemeinsam genutzter Bereiche  
 Die Anzahl Datenbereiche, die aufgrund der Datendeduplizierung mehrmals von demselben Knoten oder von unterschiedlichen Knoten verwendet werden.  
 Geschützte gemeinsam genutzte Datenbereiche  
 Der Umfang des Speicherbereichs im Speicherpool, der von gemeinsam genutzten Datenbereichen schützt wird, vor der Datendeduplizierung.  
 Von gemeinsam genutzten Bereichen belegter Speicherbereich  
 Der Umfang des Speicherbereichs im Speicherpool, der von gemeinsam genutzten Datenbereichen belegt ist, nach der Datendeduplizierung.  
 Komprimierungseinsparungen  
 Der Umfang des belegten Speicherbereichs, der im Speicherpool aufgrund einer Komprimierung nach der Datendeduplizierung eingespart wird.  
 Komprimierung in Prozent  
 Der Prozentsatz der Daten, die aufgrund der Komprimierung aus dem Speicherpool entfernt werden.  
 Anzahl komprimierter Bereiche  
 Die Anzahl der komprimierten Datenbereiche.  
 Anzahl nicht komprimierter Bereiche  
 Die Anzahl der nicht komprimierten Datenbereiche.  
 Von verschlüsselten Bereichen belegter Speicherbereich  
 Der Umfang des Speicherbereichs im Speicherpool, der von verschlüsselten Datenbereichen belegt ist.  
 Verschlüsselung in Prozent  
 Der Prozentsatz der verschlüsselten Daten im Speicherpool.  
 Anzahl verschlüsselter Bereiche  
 Die Anzahl der verschlüsselten Datenbereiche.  
 Anzahl nicht verschlüsselter Bereiche  
 Die Anzahl der nicht verschlüsselten Datenbereiche.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DEDUPSTATS

| Befehl              | Beschreibung                                  |
|---------------------|---|
| DELETE DEDUPSTATS   | Löscht Datendeduplizierungsstatistikdaten.    |
| GENERATE DEDUPSTATS | Generiert Datendeduplizierungsstatistikdaten. |

## QUERY DEVCLASS (Informationen über Einheitenklassen anzeigen)

Mit diesem Befehl können Informationen über eine oder mehrere Einheitenklassen angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
.-*-----  
>>-Query DEVclass----->  
      '-Einheitenklassenname-'  
  
.-Format----Standard----  
>-----<  
      '-Format----+Standard-+-'  
      '-Detailed-'
```

## Parameter

### Einheitenklassenname

Gibt den Namen der abzufragenden Einheitenklasse an. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Alle übereinstimmenden Einheitenklassen werden angezeigt. Wird für diesen Parameter kein Wert angegeben, werden alle Einheitenklassen angezeigt.

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

#### Standard

Gibt an, dass Teilinformationen für die angegebene Einheitenklasse angezeigt werden.

#### Detailed

Gibt an, dass die gesamten Informationen für die angegebene Einheitenklasse angezeigt werden.

## Beispiel: Alle Einheitenklassen auflisten

Informationen über alle Einheitenklassen anzeigen.

```
query devclass
```

| Einheiten-<br>klassen-<br>name | Einheiten-<br>zugriffs-<br>strategie | Anzahl<br>Speicher-<br>pools | Ein-<br>hei-<br>tentyp | Format | Gesch./<br>Max. Ka-<br>pazität<br>(MB) | Grenzwert<br>für Ladean-<br>forderung |
|--------------------------------|--------------------------------------|------------------------------|------------------------|--------|--|---------------------------------------|
| 8MMTAPE                        | Sequenziell                          | 1                            | 8MM                    | DRIVE  | 6.144,0                                | 2                                     |
| DISK                           | Wahlfrei                             | 4                            |                        |        |  |                                       |
| PLAINFILES                     | Sequenziell                          | 1                            | FILE                   |        | 50,0                                   | 1                                     |
| 8MMSP2                         | Sequenziell                          | 2                            | 8MM                    | DRIVE  | 44,4                                   | DRIVES                                |

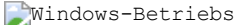
Für Feldbeschreibungen siehe Feldbeschreibungen.

## Beispiel: Ausführliche Informationen zu einer bestimmten Einheitenklasse FILE anzeigen

Ausführliche Informationen über die Einheitenklasse PLAINFILES anzeigen.

```
query devclass plainfiles format=detailed
```

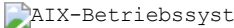
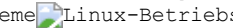

```
Einheitenklassenname: PLAINFILES  
Einheitenzugriffsstrategie: Sequenziell  
Anzahl Speicherpools: 1  
Einheitentyp: FILE  
Format:  
Gesch./Max. Kapazität (MB): 50,0  
Grenzwert für Ladeanforderung: 1  
Ladewartezeit (Min):  
Ladedauer (Min):  
Kennsatzpräfix:
```



Laufwerksbuchstabe:

```
Kassettenarchiv:  
Verzeichnis:  
Servername:
```

```
Wiederholungszeitlimit:  
Wiederholungsintervall:
```

   Gemeinsam

benutzt:

   
Sekundäre Bereichszuordnung (MB):

Primäre Bereichszuordnung (MB):

```

        Komprimierung:
    Aufbewahrungszeitraum:
        Schutz:
        Verfallsdatum:
        Einheit:
        Schutz logischer Blöcke:
    Letzte Aktualisierung durch (Administrator): ADMIN
        Datum/Zeit der letzten Aktualisierung: 05/31/2000 13:15:36

```

Für Felddesreibungen siehe Felddesreibungen.

## Beispiel: Ausführliche Informationen zu einer bestimmten Einheitenklasse 3592 anzeigen

Ausführliche Informationen zur Einheitenklasse 3592 anzeigen.

```
query devclass 3592 format=detailed
```

```

        Einheitenklassenname: 3592
    Einheitenzugriffsstrategie: Sequenziell
        Anzahl Speicherpools: 1
        Einheitentyp: 3592
        Format: 3592
    Gesch./Max. Kapazität (MB):
        Grenzwert für Ladeanforderung: DRIVES
        Ladewartezeit (Min): 60
        Ladedauer (Min): 60
        Kennsatzpräfix: ADSM
    Windows-Betriebssysteme
        Laufwerksbuchstabe:
        Kassettenarchiv: MANLIB
        Verzeichnis:
        Servername:
        Wiederholungszeitlimit:
        Wiederholungsintervall:
    AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme
    benutzt:
        Adresse der oberen Ebene:
        WORM: No
        Skalierte Kapazität: 90
        Laufwerkverschlüsselung: On
    AIX-Betriebssysteme Linux-Betriebssysteme
        Primäre Bereichszuordnung (MB):
        Sekundäre Bereichszuordnung (MB):
        Komprimierung:
        Aufbewahrungszeitraum:
        Schutz:
        Verfallsdatum:
        Einheit:
        Schutz logischer Blöcke: Read/Write
    Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
        Datum/Zeit der letzten Aktualisierung: 08/04/03 14:28:31

```

Für Felddesreibungen siehe Felddesreibungen.

## Felddesreibungen

Einheitenklassenname

Der Name der Einheitenklasse.

Einheitenzugriffsstrategie

Gibt an, wie Daten in die Einheitenklasse geschrieben werden.

Anzahl Speicherpools

Die Anzahl der Speicherpools, die der Einheitenklasse zugeordnet sind.

Einheitentyp

Der Einheitentyp der Einheitenklasse.

Format

Das Aufzeichnungsformat.

Gesch./Max. Kapazität (MB)

Die geschätzte oder die maximale Kapazität eines Datenträgers, der der Einheitenklasse zugeordnet ist.

Grenzwert für Ladeanforderung

Die maximale Anzahl Datenträger mit sequenziellem Zugriff, die gleichzeitig geladen sein kann, oder gibt an, dass DRIVES der Grenzwert für Ladeanforderungen ist.

Ladewartezeit (Min)


Die maximale Wartezeit in Minuten für das Laden eines Datenträgers mit sequenziellem Zugriff.


Ladedauer (Min)

Die Anzahl Minuten, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten werden soll, bevor er entladen wird.

#### Kennsatzpräfix

Die Kennung der oberen Ebene des Dateinamens, die der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt.

 Windows-Betriebssysteme Laufwerkbuchstabe

 Windows-Betriebssysteme Der Laufwerkbuchstabe für einen austauschbaren Datenträger.

#### Kassettenarchiv

Der Name des definierten Kassettenarchivobjekts, das die von der Einheitenklasse verwendeten Laufwerke enthält.

#### Verzeichnis

Das Verzeichnis bzw. die Verzeichnisse für eine gemeinsam benutzte Einheitenklasse FILE.

#### Servername

Der Name eines definierten Servers.

#### Wiederholungszeitlimit

Das Intervall, in dem der Server versucht, eine Verbindung zu einem Zielservers herzustellen, falls ein Übertragungsfehler vermutet wird.

#### Wiederholungsintervall

Gibt an, wie oft die Wiederholungen in einem Wiederholungszeitraum erfolgen.

#### Gemeinsam benutzt

Gibt an, ob diese Einheitenklasse FILE von dem Server und von einem oder mehreren Speicheragenten gemeinsam benutzt wird.

#### Adresse der höheren Ebene

Die IP-Adresse der Einheit in Schreibweise mit Trennzeichen.

#### Mindestkapazität

Die Mindestkapazität eines Datenträgers, der der Einheitenklasse zugeordnet ist.

#### WORM



Die Angabe, ob dieses Laufwerk eine WORM-Einheit ist (WORM = Write Once, Read Many).



#### Laufwerkverschlüsselung



Die Angabe, ob die Laufwerkverschlüsselung zulässig ist. Dieses Feld gilt nur für Datenträger in einem Speicherpool, dem der Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet ist.



#### Skalierte Kapazität



Der Prozentsatz der Datenträgerkapazität, der zum Speichern von Daten verwendet werden kann.



 AIX-Betriebssysteme  Linux-Betriebssysteme Primäre Bereichszuordnung (MB)



 AIX-Betriebssysteme  Linux-Betriebssysteme Für Einheitenklassen FILE, die Speicher darstellen, der von einem z/OS Media-Server verwaltet wird. Gibt den anfänglichen Speicherbereich an, der dynamisch zugeordnet wird, wenn ein neuer Datenträger geöffnet wird.



 AIX-Betriebssysteme  Linux-Betriebssysteme Sekundäre Bereichszuordnung (MB)

 AIX-Betriebssysteme  Linux-Betriebssysteme Für Einheitenklassen FILE, die Speicher darstellen, der von einem z/OS Media-Server verwaltet wird. Gibt den Speicherbereich an, um den ein Dateidatenträger erweitert wird, wenn der Speicherbereich, der dem Dateidatenträger bereits zugeordnet ist, verbraucht ist.



 AIX-Betriebssysteme  Linux-Betriebssysteme Komprimierung



 AIX-Betriebssysteme  Linux-Betriebssysteme Für Bändeinheitenklassen, die Speicher darstellen, der von einem z/OS Media-Server verwaltet wird. Gibt an, ob die Daten komprimiert werden.



 AIX-Betriebssysteme  Linux-Betriebssysteme Aufbewahrungszeitraum

 AIX-Betriebssysteme  Linux-Betriebssysteme Für Bändeinheitenklassen, die Speicher darstellen, der von einem z/OS Media-Server verwaltet wird. Gibt die Anzahl Tage an, die das Band aufbewahrt werden soll, wenn die Aufbewahrung verwendet wird.



 AIX-Betriebssysteme  Linux-Betriebssysteme Schutz

 AIX-Betriebssysteme  Linux-Betriebssysteme Für Bändeinheitenklassen, die Speicher darstellen, der von einem z/OS Media-Server verwaltet wird. Gibt an, ob die Datenträger durch das RACF-Programm geschützt werden.

 AIX-Betriebssysteme  Linux-Betriebssysteme Verfallsdatum

 AIX-Betriebssysteme  Linux-Betriebssysteme Für Bändeinheitenklassen, die Speicher darstellen, der von einem z/OS Media-Server verwaltet wird. Gibt das Verfallsdatum an, das auf Bandkennsätzen für diese Einheitenklasse erscheint, wenn die Verfallsverarbeitung verwendet wird.

 AIX-Betriebssysteme  Linux-Betriebssysteme Einheit

 AIX-Betriebssysteme  Linux-Betriebssysteme Für Bändeinheitenklassen, die Speicher darstellen, der von einem z/OS Media-Server verwaltet wird. Gibt den privaten Einheitennamen für die Gruppe der Bändeinheiten an.

#### Schutz logischer Blöcke

Gibt an, ob der Schutz logischer Blöcke aktiviert ist, und gibt den Modus an, wenn dies der Fall ist. Gültige Werte sind 'Read/Write', 'Write-only' und 'No'. Sie können den Schutz logischer Blöcke nur mit den folgenden Typen von Laufwerken und Datenträgern verwenden:

- IBM® LTO5 und höher
- IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
- Oracle StorageTek T10000C- und T10000D-Laufwerke


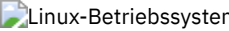



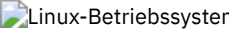


#### Letzte Aktualisierung durch (Administrator)

Der Administrator, der die letzte Aktualisierung der Einheitenklasse vorgenommen hat.

Datum/Zeit der letzten Aktualisierung  
Das Datum und die Uhrzeit der letzten Aktualisierung.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DEVCLASS

| Befehl  | Beschreibung   |
|---|--|
| DEFINE DEVCLASS   | Definiert eine Einheitenklasse.  |
|   DEFINE DEVCLASS (z/OS Media-Server) |   Definiert eine Einheitenklasse für die Verwendung von Speicher, der von einem z/OS Media-Server verwaltet wird. |
| DEFINE SERVER   | Definiert einen Server für die Übertragung zwischen Servern.   |
| DELETE DEVCLASS   | Löscht eine Einheitenklasse.   |
| QUERY DIRSPACE  | Zeigt Informationen zu Verzeichnissen FILE an.   |
| QUERY SERVER  | Zeigt Informationen über Server an.  |
| UPDATE DEVCLASS   | Ändert die Attribute einer Einheitenklasse.  |
|   UPDATE DEVCLASS (z/OS Media-Server) |   Ändert die Attribute einer Einheitenklasse für Speicher, der von einem z/OS Media-Server verwaltet wird.        |

## QUERY DIRSPACE (Speichernutzung von FILE-Verzeichnissen abfragen)

Verwenden Sie diesen Befehl, um Informationen zum freien Speicherbereich in den Verzeichnissen anzuzeigen, die einer Einheitenklasse mit dem Einheitentyp FILE zugeordnet sind.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query DIRSPace-+-----+-----<<  
                    '-Einheitenklassenname-'
```

### Parameter


#### Einheitenklassenname

Gibt den Namen der abzufragenden Einheitenklasse an. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Alle übereinstimmenden Einheitenklassen mit dem Einheitentyp FILE werden angezeigt. Wird für diesen Parameter kein Wert angegeben, werden alle Einheitenklassen mit dem Einheitentyp FILE angezeigt.


### Beispiel: Einheitenklassen des Typs FILE auflisten

Informationen für alle Einheitenklassen mit dem Einheitentyp FILE anzeigen. Im folgenden Beispiel steht M für Megabyte und G für Gigabyte.

```
query dirspace
```

 Windows-Betriebssysteme

| Einheiten-<br>klasse | Verzeichnis                | Geschätzte<br>Kapazität | Geschätzt<br>verfügbar |
|----------------------|----------------------------|-------------------------|------------------------|
| DBBKUP               | /This/is/a/large/directory | 13.000 M                | 5.543 M                |
| DBBKUP               | /This/is/directory2        | 13.000 M                | 7.123 M                |
| DBBKUP2              | /This/is/a/huge/directory  | 2.256 G                 | 2.200 G                |

 Windows-Betriebssysteme



| Einheiten-<br>klasse | Verzeichnis                  | Geschätzte<br>Kapazität | Geschätzt<br>verfügbar |
|----------------------|------------------------------|-------------------------|------------------------|
| DBBKUP               | G:\This\is\a\large\directory | 13.000 M                | 5.543 M                |
| DBBKUP               | G:\This\is\directory2        | 13.000 M                | 7.123 M                |
| DBBKUP2              | G:\This\is\a\huge\directory  | 2.256 G                 | 2.200 G                |

## Feldbeschreibungen

### Einheitenklassenname

Der Name der Einheitenklasse.

### Verzeichnis

Der Pfad des Verzeichnisses auf dem Server.

### Geschätzte Kapazität

Die geschätzte Gesamtkapazität für das Verzeichnis.

### Geschätzt verfügbar

Der geschätzte verbleibende verfügbare Speicherplatz für das Verzeichnis.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DIRSPACE

| Befehl          | Beschreibung                                |
|-----------------|---|
| DEFINE DEVCLASS | Definiert eine Einheitenklasse.             |
| DELETE DEVCLASS | Löscht eine Einheitenklasse.                |
| QUERY DEVCLASS  | Zeigt Informationen zu Einheitenklassen an. |
| UPDATE DEVCLASS | Ändert die Attribute einer Einheitenklasse. |

## QUERY DOMAIN (Maßnahmendomäne abfragen)

Mit diesem Befehl können Informationen über eine oder mehrere Maßnahmendomänen angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

.*----- .-Format----Standard----.
>>-Query Domain--+-----+-----+-----+-----<
'-Domänenname-' '-Format----+Standard--'
'-Detailed-'

```

### Parameter

#### Domänenname

Gibt die Maßnahmendomäne an, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Maßnahmendomänen angezeigt.

#### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

#### Standard

Gibt an, dass Teilinformationen angezeigt werden.

#### Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

## Beispiel: Eine Zusammenfassung der Maßnahmendomänen anzeigen

Teilinformationen für alle Maßnahmendomänen auf dem Server anzeigen. Den folgenden Befehl ausgeben:

```
query domain
```

| Name der Maßnahmen-domäne      | Aktivierte Maßnahmen-gruppe | Aktivierte Standard-verwaltungs-klasse | Anzahl registrierter Knoten | Beschreibung                         |
|--------------------------------|-----------------------------|--|-----------------------------|--------------------------------------|
| EMPLOYEE-<br>_RECORDS<br>PROG1 | VACATION                    | ACTIVEFI-<br>LES                       | 6                           | Employee Records<br>Domain           |
| PROG2                          |                             |  | 0                           | Programming Group<br>Test Domain     |
| STANDARD                       | STANDARD                    | STANDARD                               | 1                           | Installed default<br>Maßnahmendomäne |

Für Felddesreibungen siehe Felddesreibungen.

## Beispiel: Die Liste der Pools für aktive Daten anzeigen

Die Liste der Pools für aktive Daten anzeigen. Den folgenden Befehl ausgeben:

```
query domain format=detailed

                Name der Maßnahmendomäne: STANDARD
                Aktivierte Maßnahmengruppe: STANDARD
                Aktivierungsdatum/-zeit: 05/16/2006 16:18:05
                Tage seit Aktivierung: 15
                Aktivierte Standardverwaltungs-kategorie: STANDARD
                Anzahl registrierter Knoten: 1
                Beschreibung: Inst. default policy domain.
                Aufbewahrungszeitraum für Sicherung: 30
                Aufbewahrungszeitraum für Archivierung: 365
                Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
                Datum/Zeit der letzten Aktualisierung: 05/31/2006 15:17:48
                Verwaltendes Profil:

                Änderungen anstehend: Yes
                Liste der Pools für aktive Daten: ADPPPOOL
```

Für Felddesreibungen siehe Felddesreibungen.

## Felddesreibungen

Name der Maßnahmendomäne

Der Name der Maßnahmendomäne.

Aktivierte Maßnahmengruppe

Der Name der Maßnahmengruppe, die zuletzt in der Domäne aktiviert wurde.

Die Definitionen in der letzten aktivierten Maßnahmengruppe und in der AKTIVEN Maßnahmengruppe sind nicht notwendigerweise identisch. Wird eine Maßnahmengruppe aktiviert, kopiert der Server den Inhalt der Maßnahmengruppe in die Maßnahmengruppe mit dem speziellen Namen ACTIVE. Die kopierten Definitionen in der Maßnahmengruppe ACTIVE können nur durch Aktivieren einer anderen Maßnahmengruppe geändert werden. Die ursprüngliche Maßnahmengruppe kann ohne Auswirkungen auf die Maßnahmengruppe ACTIVE geändert werden. Aus diesem Grund sind Definitionen in der Maßnahmengruppe, die zuletzt aktiviert wurde, möglicherweise nicht mit den Definitionen in der Maßnahmengruppe ACTIVE identisch.

Aktivierungsdatum/-zeit

Das Datum und die Uhrzeit, an dem bzw. zu der die Maßnahmengruppe aktiviert wurde.

Tage seit Aktivierung

Die Anzahl Tage seit der Aktivierung der Maßnahmengruppe.

Aktivierte Standardverwaltungs-kategorie

Die zugeordnete Standardverwaltungs-kategorie für die Maßnahmengruppe.

Anzahl registrierter Knoten

Die Anzahl Client-Knoten, die in der Maßnahmendomäne registriert sind.

Beschreibung

Die Beschreibung der Maßnahmendomäne.

Aufbewahrungszeitraum für Sicherung

Die Anzahl der Tage, die inaktive Sicherungs-versionen von Dateien aufbewahrt werden sollen, wenn eine der folgenden Bedingungen zutrifft:



---

#### Kassettenarchivname

Gibt den Namen des Kassettenarchivs an, in dem sich das abgefragte Laufwerk befindet. Dieser Parameter ist wahlfrei. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.

Sie müssen für diesen Parameter einen Wert angeben, wenn Sie einen Laufwerknamen angeben.

#### Laufwerkname

Gibt den Namen an, der dem Laufwerk zugeordnet ist. Dieser Parameter ist wahlfrei. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben. Wird ein Laufwerkname angegeben, muss auch ein *Kassettenarchivname* angegeben werden.

#### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

##### Standard

Gibt an, daß Teilinformationen für das Laufwerk angezeigt werden.

##### Detailed

Gibt an, daß die gesamten Informationen für das Laufwerk angezeigt werden.

---

### Beispiel: Laufwerke auflisten, die dem Server zugeordnet sind

---

Informationen über alle Laufwerke anzeigen, die dem Server zugeordnet sind. Den folgenden Befehl ausgeben:

```
query drive
```

| Kassetten-<br>archivname | Laufwerk-<br>name | Einheiten-<br>typ | Angehängt |
|--------------------------|-------------------|-------------------|-----------|
| LIB1                     | DRIVE01           | 3590              | Yes       |
| LIB2                     | DRIVE02           | 3590              | Yes       |

Für Felddesreibungen siehe Felddesreibungen.

---

### Beispiel: Ausführliche Informationen zu einem bestimmten Laufwerk und Kassettenarchiv anzeigen

---

Ausführliche Informationen über das Laufwerk DRIVE02 anzeigen, das Kassettenarchiv LIB2 zugeordnet ist. Den folgenden Befehl ausgeben:

```
query drive lib2 drive02 format=detailed
```

```
                Kassettenarchivname: LIB2
                Laufwerkname: DRIVE02
                Einheitentyp: 3590
                        Online: Yes
                Laufwerkstatus: Leer
                Zugeordnet zu:
                Letzte Aktualisierung durch (Administrator): ADMIN
                Datum/Zeit der letzten Aktualisierung: 02/29/2002 09:26:23
                Reinigungshäufigk. (Gigabyte/ASNEEDED/NONE): NONE
```

Für Felddesreibungen siehe Felddesreibungen.

---

### Felddesreibungen

---

#### Kassettenarchivname

Der Name des Kassettenarchivs, dem das Laufwerk zugeordnet ist.

#### Laufwerkname

Der Name, der dem Laufwerk zugeordnet ist.

#### Einheitentyp

Der Einheitentyp, der in der zugehörigen Einheitenklasse angegeben ist. Für den Server muss ein Pfad von dem Server zu dem Laufwerk definiert sein, damit der Server den wahren Einheitentyp bestimmen kann. Solange ein Pfad von dem Server zu dem Laufwerk definiert ist, zeigt der Server den wahren Einheitentyp des Laufwerks an, auch wenn andere Pfade zu diesem Laufwerk definiert sind. Ausnahmen treten auf, wenn der Einheitentyp "remote" oder "unknown" lautet.

#### REMOTE

Der Server hat keinen Pfad zu der Einheit. Es sind nur Pfade von den Einheiten zum Versetzen von Daten zu der Einheit definiert.

#### UNKNOWN

Es ist kein Pfad vorhanden.

Tipp: Überprüfen Sie die Ausgabe des Befehls QUERY PATH, um zu bestimmen, ob die gewünschten Pfade definiert sind. Sind sie nicht definiert, definieren Sie die gewünschten Pfade mit dem Befehl DEFINE PATH. Wird eine Einheit zum Versetzen von Daten verwendet, überprüfen Sie auch die Ausgabe des Befehls QUERY DATAMOVER, um den Typ der Einheit zum Versetzen von Daten zu bestimmen. Wird ein Pfad von dem Server zu einem Laufwerk verwendet, müssen die Einheitenklassen der Einheitenklasse und des Laufwerks übereinstimmen. Wird ein Pfad von einer Einheit zum Versetzen von Daten zu einem Laufwerk verwendet, lesen Sie die Informationen in der Dokumentation zu Ihrer Einheit zum Versetzen von Daten, um sicherzustellen, dass der Einheitstyp der Einheitenklasse mit dem Typ der Einheit zum Versetzen von Daten kompatibel ist.

#### Online

Gibt den Status des Laufwerks an:

Yes

Das Laufwerk ist angehängt und für Serveroperationen verfügbar.

No

Das Laufwerk ist abgehängt. Das Laufwerk wurde von einem Administrator, der den Status aktualisiert, in diesen Status gesetzt.

Nicht verfügbar seit

Gibt an, dass das Laufwerk seit *mm/tt/jj hh:mm:ss* nicht verfügbar ist. Die Ausgabe zeigt die Zeit, zu der der Server das Laufwerk als nicht verfügbar markiert hat.

Sendeaufruf seit

Gibt an, daß der Server das Laufwerk aufruft, da das Laufwerk nicht mehr antwortet. Die Ausgabe zeigt die Zeit, zu der der Server einen Fehler erkannt und mit dem Aufrufen des Laufwerks begonnen hat. Der Server ruft ein Laufwerk auf, bevor es als nicht verfügbar markiert wird. Die Zeitausgabe hat das Format: *mm/dd/yy hh:mm:ss*.

#### Leseformate

Die Leseformate für das Laufwerk.

#### Schreibformate

Die Schreibformate für das Laufwerk.

#### Element

Die Elementnummer für das Laufwerk.

#### Laufwerkstatus

Gibt den aktuellen Status dieses spezifischen Laufwerks auf der Basis des Ergebnisses des letzten SCSI-Befehls für das Laufwerk oder Kassettenarchiv an. Der Server verfolgt den Status des Laufwerks, um die Auswahl eines Laufwerks für eine Operation und die Fehlerbehebungsoperationen zu erleichtern. Gültige Werte:

Unavailable

Das Laufwerk steht dem Kassettenarchiv für Operationen nicht zur Verfügung.

Empty

Das Laufwerk ist leer und steht für Operationen zur Verfügung.

Loaded

Das Laufwerk ist gegenwärtig geladen, und der Server führt gerade Operationen mit dem Laufwerk aus.

Unloaded

Der Datenträger wurde vom Laufwerk ausgegeben.

Reserved

Das Laufwerk ist für eine Ladeanforderung reserviert.

Unknown

Das Laufwerk beginnt mit dem Anfangsstatus 'Unbekannt', da es gerade definiert wird, da der Server initialisiert wird oder da sein Status in 'Angehängt' aktualisiert wird.

#### Datenträgername

Der Datenträgername für das Laufwerk.

#### Zugeordnet zu

Der Name des Kassettenarchiv-Clients, der gegenwärtig das Laufwerk verwendet. Dieses Feld gilt nur für gemeinsam benutzte SCSI-Kassettenarchive; für alle anderen Kassettenarchive bleibt das Feld leer.

#### WWN

Der weltweite Name für das Laufwerk.

#### Letzte Aktualisierung durch (Administrator)

Gibt an, wer die letzte Aktualisierung des Laufwerks ausgeführt hat.

#### Datum/Zeit der letzten Aktualisierung

Das Datum und die Uhrzeit der letzten Aktualisierung.

#### Reinigungshäufigk. (Gigabyte/ASNEEDED/NONE)

Gibt an, wie oft der Server die Laufwerkreinigung aktiviert. Dieser Wert kann die Anzahl der Gigabyte, ASNEEDED oder NONE sein.

## Zugehörige Befehle

---



```

>----->
  '-WHEREState---+-----+'
      +-All-----+
      +-MOUNTable-----+
      +-NOTMOUNTable-----+
      +-COUrier-----+
      +-VAult-----+
      +-VAULTRetrieve---+
      +-COURIERRetrieve+
      '-REmote-----'

>----->
  '-BEGINDate---Datum-' '-ENDDate---Datum-'

>----->
  '-BEGINTime---Zeit-' '-ENDTime---Zeit-'

>----->
  '-COPYstgpool----Poolname-'

>----->
  '-ACTIVEDatastgpool----Poolname-'

>----->
  '-COPYCONTainerstgpool----Poolname-'

.-Source----DBBackup-----.-Format----Standard-----.
>----->
  '-Source-----+DBBackup---+' '-Format-----+Standard+++'
      +-DBSnapshot+          +-Detailed++
      '-DBNone-----'          '-Cmd-----'

>----->
  '-WHERELOCation----Standort-' | .-----|
                                | V         | |
                                '-Cmd-----"Befehl"---+'

.-APPend----No-----.
>-----<
  '-CMDFilename----Dateiname-' '-APPend-----+No---+'
                                '-Yes-'

```

## Parameter

### Datenträgername

Gibt die Namen der Datenträger an, die abgefragt werden sollen. Es können Platzhalterzeichen verwendet werden, um mehrere Namen anzugeben. Dieser Parameter ist wahlfrei. Der Server sucht nach übereinstimmenden Namen unter den folgenden auswählbaren Datenträgern:

- Datenbanksicherungsdatenträger, die mit dem Parameter SOURCE dieses Befehls ausgewählt wurden.
- Kopierspeicherpooldatenträger aus Kopierspeicherpools, die mit dem Parameter COPYSTGPOOL angegeben wurden. Wird der Parameter COPYSTGPOOL nicht verwendet, fragt der Server Datenträger aus Kopierspeicherpools ab, die zuvor mit dem Befehl SET DRMCOPYSTGPOOL angegeben wurden.
- Datenträger im Speicherpool für aktive Daten aus Speicherpools für aktive Daten, die mit dem Parameter ACTIVEDATASTGPOOL angegeben wurden. Wird der Parameter ACTIVEDATASTGPOOL nicht verwendet, fragt der Server Datenträger aus Speicherpools für aktive Daten ab, die zuvor mit dem Befehl SET DRMACTIVEDATASTGPOOL angegeben wurden.
- Containerkopierspeicherpooldatenträger aus Containerkopierspeicherpools, die mit dem Parameter COPYCONTAINERSTGPOOL angegeben wurden. Wenn der Parameter COPYCONTAINERSTGPOOL nicht verwendet wird, fragt der Server Datenträger aus Containerkopierspeicherpools ab, die zuvor im Befehl SET DRMCOPYCONTAINERSTGPOOL angegeben wurden.

Andere Parameter können ebenfalls die Ergebnisse der Abfrage begrenzen.

### WHEREState

Gibt den Status der zu verarbeitenden Datenträger an. Dieser Parameter ist wahlfrei. Standardwert ist ALL. Gültige Werte:

All

Gibt alle Datenträger in allen Status an.

MOUNTable

Datenträger in diesem Status enthalten gültige Daten und stehen für die Verarbeitung vor Ort zur Verfügung.

NOTMOUNTable

Datenträger in diesem Status befinden sich vor Ort, enthalten gültige Daten und stehen nicht für die Verarbeitung vor Ort zur Verfügung.

**COUrier**

Datenträger in diesem Status werden gerade an einen ausgelagerten Standort versetzt.

**VAult**

Datenträger in diesem Status sind ausgelagert, enthalten gültige Daten und stehen nicht für die Verarbeitung vor Ort zur Verfügung.

**VAULTRetrieve**

Datenträger in diesem Status befinden sich an dem ausgelagerten Aufbewahrungsort, enthalten keine gültigen Daten und können zur Wiederverwendung oder Entsorgung wieder vor Ort versetzt werden:

- Für einen Kopierspeicherpooldatenträger wird der Status VAULTRETRIEVE angenommen, wenn er für mindestens die Anzahl Tage leer war, die mit dem Parameter REUSEDELAY im Befehl DEFINE STGPOOL angegeben wurde.
- Für einen Datenbanksicherungsdatenträger wird der Status VAULTRETRIEVE angenommen, wenn er einer Datenbanksicherungsserie zugeordnet ist, die auf der Basis des mit dem Befehl SET DRMDBBACKUPEXPIREDDAYS angegebenen Werts als verfallen gekennzeichnet wurde.

Wichtig: Wenn Sie QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE ausgeben, bestimmt der Server dynamisch, welche Datenträger zur Wiederverwendung oder Aussonderung wieder vor Ort transportiert werden können. Um sicherzustellen, dass alle Datenträger im Status VAULTRETRIEVE identifiziert werden, müssen Sie daher den Befehl QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE ohne die Parameter BEGINDATE, ENDDATE, BEGINTIME und ENDTIME ausgeben. Das Feld Datum/Zeit der letzten Aktualisierung in der Ausgabe für QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE zeigt das Datum und die Uhrzeit an, an dem bzw. zu der ein Datenträger in den Status VAULT, nicht VAULTRETRIEVE, versetzt wurde.

**COURIERRetrieve**

Datenträger in diesem Status werden wieder an den Standort vor Ort versetzt.

**REmote**

Datenträger in diesem Status enthalten gültige Daten und befinden sich auf dem ausgelagerten fernen Server.

**BEGINDate**

Gibt das Anfangsdatum an, das zum Auswählen der Datenträger verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder nach dem angegebenen Datum in seinen aktuellen Status geändert hat. Standardwert ist das früheste Datum, ab dem Datenträgerdaten vorliegen.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 09/15/1998   |
| TODAY                          | Das aktuelle Datum   | TODAY  |
| TODAY-Tage oder -Tage          | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage beträgt 9999. | TODAY-7 oder -7.<br><br>Sollen Datenträger abgefragt werden, deren Sätze vor einer Woche in den aktuellen Status geändert wurden, kann BEGINDATE=TODAY-7 oder BEGINDATE=-7 angegeben werden. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.   |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.  |

**ENDDate**

Gibt das Enddatum an, das zum Auswählen der Datenträger verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder vor dem angegebenen Datum in seinen aktuellen Status geändert hat. Standardwert ist das aktuelle Datum.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert | Beschreibung | Beispiel |
|------|--------------|----------|
|------|--------------|----------|



| Wert                           | Beschreibung   | Beispiel  |
|--------------------------------|--|---|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 09/15/1998  |
| TODAY                          | Das aktuelle Datum   | TODAY   |
| TODAY-Tage <i>oder</i> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage beträgt 9999. | TODAY-7 <i>oder</i> -7.<br><br>Sollen Datenträger abgefragt werden, deren Sätze vor einer Woche in den aktuellen Status geändert wurden, kann BEGINDATE=TODAY-7 oder BEGINDATE=-7 angegeben werden. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM  |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.  |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM  |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.   |

#### BEGINTime

Gibt die Anfangszeit an, die zum Auswählen der Datenträger verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder nach der angegebenen Uhrzeit und dem angegebenen Datum in seinen aktuellen Status geändert hat. Der Standardwert ist Mitternacht (00:00:00) an dem mit dem Parameter BEGINDATE angegebenen Datum.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert                         | Beschreibung   | Beispiel   |
|------------------------------|--|--|
| HH:MM:SS                     | Eine bestimmte Uhrzeit am angegebenen Anfangsdatum                             | 12:33:28   |
| NOW                          | Die aktuelle Uhrzeit am angegebenen Anfangsdatum                               | NOW  |
| NOW+HH:MM <i>oder</i> +HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Anfangsdatum  | NOW+03:00 <i>oder</i> +03:00.<br><br>Wird der Befehl QUERY DRMEDIA um 9:00 Uhr mit der Angabe BEGINTIME=NOW+03:00 oder BEGINTIME=+03:00 ausgegeben, zeigt der Server Datenträger an, die um 12:00 Uhr am angegebenen Anfangsdatum in ihren aktuellen Status geändert wurden. |
| NOW-HH:MM <i>oder</i> -HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Anfangsdatum | NOW-03:30 <i>oder</i> -03:30.<br><br>Wird der Befehl QUERY DRMEDIA um 9:00 Uhr mit der Angabe BEGINTIME=NOW-03:30 oder BEGINTIME=-03:30 ausgegeben, zeigt der Server Datenträger an, die um 5:30 Uhr am angegebenen Anfangsdatum in ihren aktuellen Status geändert wurden.  |

#### ENDTime

Gibt die Endzeit an, die zum Auswählen der Datenträger verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder vor der angegebenen Uhrzeit und dem angegebenen Datum in seinen aktuellen Status geändert hat. Der Standardwert ist 23:59:59.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert     | Beschreibung                                   | Beispiel |
|----------|--|----------|
| HH:MM:SS | Eine bestimmte Uhrzeit am angegebenen Enddatum | 10:30:08 |
| NOW      | Die aktuelle Uhrzeit am angegebenen Enddatum   | NOW      |

| Wert                         | Beschreibung   | Beispiel  |
|------------------------------|--|---|
| NOW+HH:MM <i>oder</i> +HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum  | NOW+03:00 <i>oder</i> +03:00.<br><br>Wird der Befehl QUERY DRMEDIA um 9:00 Uhr mit der Angabe ENDTIME=NOW+03:00 oder ENDTIME=+03:00 ausgegeben, verarbeitet IBM Spectrum Protect Datenträger, die um 12:00 Uhr am angegebenen Enddatum in ihren aktuellen Status geändert wurden. |
| NOW-HH:MM <i>oder</i> -HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum | NOW-03:30 <i>oder</i> -03:30<br><br>Wird der Befehl QUERY DRMEDIA um 9:00 Uhr mit der Angabe ENDTIME=NOW-03:00 oder ENDTIME=-03:00 ausgegeben, verarbeitet IBM Spectrum Protect Datenträger, die um 6:00 Uhr am angegebenen Enddatum in ihren aktuellen Status geändert wurden.   |

#### COPYstgpool

Gibt den Namen des Kopierspeicherpools an, dessen Datenträger verarbeitet werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Die mit diesem Parameter angegebenen Kopierspeicherpools überschreiben die mit dem Befehl SET DRMCOPYSTGPOOL angegebenen Kopierspeicherpools.

Wird dieser Parameter nicht angegeben, wählt der Server die Speicherpools wie folgt aus:

- Wurde der Befehl SET DRMCOPYSTGPOOL zuvor mit gültigen Kopierspeicherpoolnamen ausgegeben, verarbeitet der Server nur diese Speicherpools.
- Wurde der Befehl SET DRMCOPYSTGPOOL nicht ausgegeben, oder wurden alle Kopierspeicherpools mit dem Befehl SET DRMCOPYSTGPOOL entfernt, verarbeitet der Server alle Kopierspeicherpooldatenträger in dem angegebenen Status (ALL, MOUNTABLE, NOTMOUNTABLE, COURIER, VAULT, VAULTRETRIEVE, COURIERRETRIEVE oder REMOTE).

#### Source

Gibt an, ob Datenbanksicherungsdatenträger ausgewählt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist DBBACKUP. Gültige Werte:

##### DBBackup

Datenbanksicherungsdatenträger mit Gesamt- und Teilsicherungen werden ausgewählt.

##### DBSnapshot

Datenbanksicherungsdatenträger mit Momentaufnahmen werden ausgewählt.

##### DBNone

Es werden keine Datenbanksicherungsdatenträger ausgewählt.

#### ACTIVEDatastgpool

Gibt den Namen des Speicherpools für aktive Daten an, dessen Datenträger verarbeitet werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Die mit diesem Parameter angegebenen Speicherpools für aktive Daten überschreiben die mit dem Befehl SET DRMACTIVEDATASTGPOOL angegebenen Speicherpools für aktive Daten.

Wird dieser Parameter nicht angegeben, wählt der Server die Speicherpools wie folgt aus:

- Wurde der Befehl SET DRMACTIVEDATASTGPOOL zuvor mit gültigen Namen von Speicherpools für aktive Daten ausgegeben, verarbeitet der Server nur diese Speicherpools.
- Wurde der Befehl SET DRMACTIVEDATASTGPOOL nicht ausgegeben, oder wurden alle Speicherpools für aktive Daten mit dem Befehl SET DRMACTIVEDATASTGPOOL entfernt, verarbeitet der Server alle Datenträger im Speicherpool für aktive Daten in dem angegebenen Status (ALL, NOTMOUNTABLE, COURIER, VAULT, VAULTRETRIEVE, COURIERRETRIEVE oder REMOTE). Datenträger im Status MOUNTABLE werden nicht verarbeitet.

#### COPYContainerstgpool

Gibt den Namen des Containerkopierspeicherpools an, dessen Datenträger verarbeitet werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Die in diesem Parameter angegebenen Containerkopierspeicherpools überschreiben die im Befehl SET DRMCOPYCONTAINERSTGPOOL angegebenen Speicherpools.

Wird dieser Parameter nicht angegeben, wählt der Server die Speicherpools wie folgt aus:

- Wenn der Befehl SET DRMCOPYCONTAINERSTGPOOL zuvor mit Namen gültiger Containerkopierspeicherpools ausgegeben wurde, verarbeitet der Server nur diese Speicherpools.

- Wenn der Befehl SET DRMCOPYCONTAINERSTGPOOL nicht ausgegeben wurde oder alle Containerkopierspeicherpools mit dem Befehl SET DRMCOPYCONTAINERSTGPOOL entfernt wurden, verarbeitet der Server alle Containerkopierspeicherpooldatenträger auf der Basis des Werts im Parameter WHERESTATE. Ist der Parameter auf den Wert ALL, NOTMOUNTABLE, COURIER, VAULT, VAULTRETRIEVE, COURIERRETRIEVE oder REMOTE gesetzt, werden die Datenträger verarbeitet. Lautet der Wert MOUNTABLE, werden die Datenträger nicht verarbeitet.

#### Format

Gibt die Informationen an, die angezeigt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

##### Standard

Gibt an, dass Teilinformationen angezeigt werden.

##### Detailed

Gibt an, dass ausführliche Informationen angezeigt werden.

##### Cmd

Gibt an, dass ausführbare Befehle für die ausgewählten Datenträger erstellt werden. Wenn Sie FORMAT=CMD angeben, müssen Sie auch den Parameter CMD angeben.

#### WHERELOCATION

Gibt den Standort der Datenträger an, die abgefragt werden sollen. Dieser Parameter ist wahlfrei. Die maximale Länge des Standorts beträgt 255 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält. Wird der Name eines Zielservers angegeben, zeigt Disaster Recovery Manager alle Datenbanksicherungsdatenträger und Kopierspeicherpooldatenträger an, die sich auf dem Zielserver befinden.

#### CMD

Gibt die Erstellung von ausführbaren Befehlen an, um den mit diesem Befehl erhaltenen Datenträgernamen und Standort zu verarbeiten. Dieser Parameter ist wahlfrei. Die Befehlsangabe muss in Anführungszeichen eingeschlossen werden. Die maximale Länge dieses Parameters beträgt 255 Zeichen. Disaster Recovery Manager schreibt die Befehle in eine Datei, die mit dem Parameter CMDFILENAME oder dem Befehl SET DRMCMDFILENAME angegeben oder mit dem Befehl QUERY DRMEDIA generiert wurde. Ist der Befehl länger als 240 Zeichen, wird er in mehrere Zeilen geteilt und es werden Fortsetzungszeichen (+) hinzugefügt. Das Fortsetzungszeichen muss möglicherweise entsprechend dem Produkt, das die Befehle ausführt, geändert werden.

Wenn der Parameter FORMAT=CMD nicht angegeben wird, werden von diesem Befehl keine Befehlszeilen erstellt.

#### Zeichenfolge

Die Befehlszeichenfolge. Die Zeichenfolge darf keine eingebetteten Anführungszeichen enthalten. Dies ist beispielsweise ein gültiger CMD-Parameter:

```
cmd="checkin libvol lib8mm &vol status=scratch"
```

Dies ist ein Beispiel eines CMD-Parameters, der *nicht* gültig ist:

```
cmd=""checkin libvolume lib8mm" &vol status=scratch""
```

#### Substitution

Gibt eine Substitutionsvariable an, mit der QUERY DRMEDIA angewiesen wird, einen Wert für die Variable einzusetzen. Bei den Variablen muss die Groß-/Kleinschreibung nicht berücksichtigt werden. Die Variablen dürfen keine Leerstellen hinter dem Et-Zeichen (&) enthalten. Gültige Variablen sind:

##### &VOL

Eine Variable für den Datenträgernamen.

##### &LOC



Ein Datenträgerstandort.

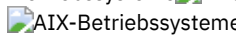
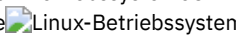
##### &VOLDSN

Der Name der Datei, in die der Server die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Ein Beispiel für einen Dateinamen eines Banddatenträgers aus dem Kopierspeicherpool unter Verwendung des Standardpräfix TSM lautet TSM.BFS. Ein Beispiel für einen Dateinamen eines Banddatenträgers für die Datenbanksicherung unter Verwendung des Präfix TSM310 lautet TSM310.DBB.

##### &NL

Das Zeilenvorschubzeichen. Wird &NL angegeben, teilt der Befehl QUERY DRMEDIA den Befehl bei der Variablen &NL und fügt kein Fortsetzungszeichen hinzu. Es muss das korrekte Fortsetzungszeichen vor &NL angegeben werden, sofern ein Fortsetzungszeichen erforderlich ist. Wird &NL nicht angegeben und hat die Befehlszeile mehr als 240 Zeichen, wird die Zeile in mehrere Zeilen geteilt und es werden Fortsetzungszeichen (+) hinzugefügt.


  CMDFilename

  Gibt den vollständig qualifizierten Namen der Datei an, die die mit dem Parameter CMD angegebenen Befehle enthalten soll. Dieser Parameter ist wahlfrei.

Wenn kein Name mit dem Befehl SET DRMCMDFILENAME angegeben wird, erstellt der Server einen Dateinamen, indem `exec.cmds` an den absoluten Verzeichnispfadnamen des IBM Spectrum Protect-Instanzverzeichnisses angehängt wird. Wird eine Nullzeichenfolge ("" ) angegeben, werden die Befehle nur an der Konsole angezeigt. Die Befehle können an eine Datei umgeleitet werden, indem das Umleitungszeichen für das Betriebssystem verwendet wird.

Schlägt die Operation fehl, nachdem die Befehlsdatei erstellt wurde, wird die Datei nicht gelöscht.

#### Windows-BetriebssystemeCMDFilename

 Windows-BetriebssystemeGibt den vollständig qualifizierten Namen der Datei an, die die mit dem Parameter CMD angegebenen Befehle enthalten soll. Dieser Parameter ist wahlfrei.

Wenn kein Dateiname mit dem Befehl SET DRMCMDFILENAME angegeben wird, erstellt der Server einen Dateinamen, indem `exec.cmd` an das Verzeichnis angehängt wird, das diese Instanz des Servers darstellt (normalerweise das Verzeichnis, in dem der IBM Spectrum Protect-Server ursprünglich installiert wurde). Wird eine Nullzeichenfolge ("" ) angegeben, werden die Befehle nur an der Konsole angezeigt. Die Befehle können an eine Datei umgeleitet werden, indem die Zeichen > und >> verwendet werden, die vom System zur Verfügung gestellt werden. Disaster Recovery Manager ordnet den angegebenen oder generierten Dateinamen zu. Ist die Datei vorhanden, versucht Disaster Recovery Manager, die Datei zu verwenden, und es werden alle vorhandenen Daten überschrieben.

Schlägt die Operation fehl, nachdem die Befehlsdatei erstellt wurde, wird die Datei nicht gelöscht.

#### APPend

Gibt an, ob der vorhandene Inhalt der Befehlsdatei überschrieben werden soll oder ob die Befehle an die Datei angehängt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No

Disaster Recovery Manager überschreibt den Inhalt der Datei.

Yes

Disaster Recovery Manager hängt die Befehle an die Datei an.

## Beispiel: Datenträger auflisten, die zur Speicherung ausgelagert werden sollen

Es sollen alle Datenträger angezeigt werden, die einem Kurier für die ausgelagerte Speicherung übergeben werden sollen.

```
query drmedia wherestate=notmountable
format=standard
```

| Datenträger- | Status        | Dat./Zeit<br>name   | Automat. | d.letz.Akt. | Kassettenarchiv |
|--------------|---------------|---------------------|----------|-------------|-----------------|
| TAPE01       | Not mountable | 01/20/1998 14:25:22 |          |             |                 |
| DBTP01       | Not mountable | 01/20/1998 14:25:22 |          |             |                 |
| DBTP03       | Not mountable | 01/20/1998 14:31:53 |          |             |                 |

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Beispiel: Informationen zu Datenträgern am Aufbewahrungsort anzeigen

Ausführliche Informationen über alle Datenträger an dem Aufbewahrungsort anzeigen.

```
query drmedia wherestate=vault format=detailed
```

```

          Datenträgername: DBTP02
                Status: Vault
Datum/Zeit der letzten Aktualisierung: 01/20/1998 13:29:02
                Standort: Ironmnt
          Datenträgerart: DBBackup
        Kopierspeicherpoolname:
Name des Speicherpools für aktive Daten: TSMACTIVEPOOL
        Automat. Kassettenarchiv:
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Feldbeschreibungen

Datenträgername

Der Name des Datenbanksicherungs- oder Kopierspeicherpooldatenträgers.

Status

Der Status des Datenträgers.

Datum/Zeit der letzten Aktualisierung

Das Datum und die Uhrzeit, an dem bzw. zu der der Datenträgerstatus zuletzt aktualisiert wurde. Für Datenträger im Status VAULTRETRIEVE zeigt dieses Feld das Datum und die Uhrzeit an, an dem bzw. zu der ein Datenträger in den Status VAULT, nicht VAULTRETRIEVE, versetzt wurde. Der Server "aktualisiert" keine Datenträger nach VAULTRETRIEVE. Zum Zeitpunkt der Ausgabe des Befehls QUERY DRMEDIA bestimmt der Server dynamisch, ob die Daten auf den Kopierspeicherpooldatenträgern und Datenbanksicherungsdatenträgern nicht mehr gültig sind und ob der Datenträger zur Wiederverwendung oder Entsorgung wieder an den Standort vor Ort versetzt werden kann.

#### Standort

Das Feld Standort wird angezeigt, wenn der Datenträger nicht mountfähig ist oder sich nicht im Speicherarchiv befindet. Das Feld Standort ist leer, wenn der Datenträger mountfähig ist und sich im Speicherarchiv befindet.

#### Datenträgertyp

Gibt den Datenträgertyp an. Gültige Werte:

##### DBBackup

Datenträger mit vollständiger Datenbanksicherung oder Teilsicherung der Datenbank.

##### DBSnapshot

Datenträger mit Datenbankmomentaufnahmesicherung.

##### CopyStgPool

Ein Kopierspeicherpooldatenträger.

##### ContcopyStgPool

Ein Datenträger im Containerkopierspeicherpool.

#### Kopierspeicherpoolname

Für einen Kopierspeicherpooldatenträger der Name des Kopierspeicherpools.

#### Name des Speicherpools für aktive Daten

Für einen Datenträger im Speicherpool für aktive Daten der Name des Speicherpools für aktive Daten.

#### Name des Containerkopierspeicherpools



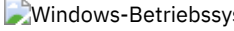
Für einen Datenträger im Containerkopierspeicherpool der Name des Containerkopierspeicherpools.

#### Automat. Kassettenarchiv

Der Name des automatisierten Kassettenarchivs, wenn sich der Datenträger in einem Kassettenarchiv befindet.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DRMEDIA

| Befehl  | Beschreibung   |
|---|--|
| BACKUP DB   | Sichert die IBM Spectrum Protect-Datenbank auf Datenträgern mit sequenziellem Zugriff.                           |
| BACKUP STGPOOL  | Sichert einen primären Speicherpool in einem Kopierspeicherpool.   |
| CHECKOUT LIBVOLUME  | Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.                                       |
| MOVE DRMEDIA  | Versetzt DRM-Datenträger vor Ort und lagert sie aus.   |
| QUERY DRMSTATUS   | Zeigt DRM-Systemparameter an.  |
| SET DRMACTIVEDATASTGPOOL  | Gibt an, dass Speicherpools für aktive Daten von DRM verwaltet werden.   |
|    SET DRMCOPYCONTAINERSTGPOOL | Gibt die Containerkopierspeicherpools an, die in DRM-Befehlen verwendet werden.                                  |
| SET DRMCOPYSTGPOOL  | Gibt an, dass Kopierspeicherpools von DRM verwaltet werden.  |
| SET DRMDBBACKUPEXPIREDAYS   | Gibt die Kriterien für den Verfall von Datenbanksicherungsreihen an.   |
| SET DRMCMDFILENAME  | Gibt den Namen einer Datei an, in die ausführbare DRM-Befehle gestellt werden sollen.                            |
| SET DRMFILPROCESS   | Gibt an, ob der Befehl MOVE DRMEDIA oder QUERY DRMEDIA Dateien verarbeitet, die den Einheitentyp FILE aufweisen. |

## QUERY DRMSTATUS (Disaster Recovery Manager-Systemparameter abfragen)

Mit diesem Befehl können Informationen über die Systemparameter angezeigt werden, die für Disaster Recovery Manager (DRM) definiert sind.

## Berechtigungsklasse

---

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

---

```
>>-Query DRMStatus-----><
```

## Parameter

---

Keine.

## Beispiel: Informationen zu DRM-Systemparametern anzeigen

---

Informationen zu den DRM-Systemparametern anzeigen:

```
query drmsstatus

      Wiederherstellungsplanpräfix:
        Plananweisungspräfix:
      Ersatzdatenträgererweiterung: @
        Primäre Speicherpools: PRIM1 PRIM2
        Kopienspeicherpools: COPY*
      Speicherpools für aktive Daten: TSMACTIVEPOOL
      Containerkopienspeicherpools: COPYCNRPOOL
      Nicht mount-fähiger Standortname: Local
        Kuriernamenname: Fedex
        Aufbewahrungsortname: Ironmnt
      Verfallszeitraum für DB-Sicherungsreihe: 30 Tag(e)
      Verfallszeitraum für Wiederherstellungsplandatei: 30 Tag(e)
        Kennsatzprüfung?: No
      Einheitentyp FILE verarbeiten?: No
      Befehlsdateiname:
```

## Feldbeschreibungen

---

### Wiederherstellungsplanpräfix

Benutzerdefinierter Präfixabschnitt des Dateinamens für die Wiederherstellungsplandatei.

### Plananweisungspräfix

Benutzerdefinierter Präfixabschnitt der Dateinamen für die Wiederherstellungsanweisungsdateien des Servers.

### Ersatzdatenträgererweiterung

Das Zeichen, das an das Ende der Ersatzdatenträgernamen in der Wiederherstellungsplandatei hinzugefügt wird.

### Primäre Speicherpools

Die primären Speicherpools, die für die Verarbeitung durch den Befehl PREPARE ausgewählt werden können. Ist dieses Feld leer, können alle primären Speicherpools ausgewählt werden.

### Kopienspeicherpools

Die Kopienspeicherpools, die für die Verarbeitung durch die Befehle MOVE DRMEDIA, PREPARE und QUERY DRMEDIA ausgewählt werden können. Ist dieses Feld leer, können alle Kopienspeicherpools ausgewählt werden.

### Speicherpools für aktive Daten

Die Pools für aktive Daten, die für die Verarbeitung durch die Befehle MOVE DRMEDIA, PREPARE und QUERY DRMEDIA ausgewählt werden können. Ist dieses Feld leer, sind keine Pools für aktive Daten auswählbar.

### Containerkopienspeicherpools

Die Containerkopienspeicherpools, die für die Verarbeitung durch die Befehle MOVE DRMEDIA, PREPARE und QUERY DRMEDIA ausgewählt werden können. Ist dieses Feld leer, sind keine Containerkopienspeicherpools auswählbar.

### Nicht mount-fähiger Standortname

Der Name des ausgelagerten Standorts, an dem die zu liefernden Datenträger aufbewahrt werden.

### Kuriernamenname

Der Name des Kuriers, mit dem die Datenträger an den Aufbewahrungsort befördert werden.

### Aufbewahrungsortname

Der Name des Aufbewahrungsorts, an dem die Datenträger aufbewahrt werden.

### Verfallszeitraum für DB-Sicherungsreihe

Die Mindestanzahl Tage, die seit der Erstellung einer Datenbanksreihe vergangen sein müssen, bevor sie für den Verfall ausgewählt werden kann. Unter dem Befehl SET DRMDBBACKUPEXPIREDAYS befinden sich Informationen zu den Kriterien, die für den Verfall

von Datenbanksicherungsserien erfüllt sein müssen.

Verfallszeitraum für Wiederherstellungsplandatei

Die Mindestanzahl Tage, die seit der Erstellung einer Wiederherstellungsplandatei, die auf einem Zielsystem gespeichert ist, vergangen sein müssen, bevor die Datei für den Verfall ausgewählt werden kann. Unter dem Befehl SET DRMRPFEXPIREDAYS befinden sich Informationen zu den Kriterien, die für den Verfall einer Wiederherstellungsplandatei erfüllt sein müssen.

Kennsatzprüfung?

Die Angabe, ob Datenträgerkennsätze für sequenzielle Datenträger gelesen werden, die durch den Befehl MOVE DRMEDIA entnommen wurden. Gültige Werte sind Yes oder No.

Einheitentyp FILE verarbeiten?



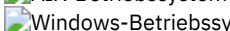
Die Angabe, ob der Befehl MOVE DRMEDIA oder QUERY DRMEDIA Datenbanksicherungs- und Kopierspeicherpooldateiträger verarbeitet, die einer Einheitenklasse mit dem Einheitentyp FILE zugeordnet sind. Gültige Werte sind Yes oder No.

Befehlsdateiname

Der vollständige Pfad und Dateiname, in dem sich die durch den Befehl MOVE DRMEDIA oder QUERY DRMEDIA generierten ausführbaren Befehle befinden.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DRMSTATUS

| Befehl   | Beschreibung  |
|--|---|
| MOVE DRMEDIA   | Versetzt DRM-Datenträger vor Ort und lagert sie aus.  |
| PREPARE  | Erstellt eine Wiederherstellungsplandatei.  |
| QUERY DRMEDIA  | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.                       |
| SET DRMCHECKLABEL  | Gibt an, ob IBM Spectrum Protect während der Verarbeitung des Befehls MOVE DRMEDIA Datenträgerkennsätze lesen soll. |
| SET DRMACTIVEDATASTGPOOL   | Gibt an, dass Speicherpools für aktive Daten von DRM verwaltet werden.  |
|  <br> SET DRMCOPYCONTAINERSTGPOOL | Gibt die Containerkopierspeicherpools an, die in DRM-Befehlen verwendet werden.                                     |
| SET DRMCOPYSTGPOOL   | Gibt an, dass Kopierspeicherpools von DRM verwaltet werden.   |
| SET DRMCMDFILENAME   | Gibt den Namen einer Datei an, in die ausführbare DRM-Befehle gestellt werden sollen.                               |
| SET DRMCOURIERNAME   | Gibt den Kuriernamen für DRM an.  |
| SET DRMDBBACKUPEXPIREDAYS  | Gibt die Kriterien für den Verfall von Datenbanksicherungsserien an.  |
| SET DRMFILEPROCESS   | Gibt an, ob der Befehl MOVE DRMEDIA oder QUERY DRMEDIA Dateien verarbeitet, die den Einheitentyp FILE aufweisen.    |
| SET DRMINSTRPREFIX   | Gibt das Präfix des Pfadnamens für die Wiederherstellungsplananweisungen an.  |
| SET DRMPLANVPOSTFIX  | Gibt die Namen der Ersatzdatenträger in der Wiederherstellungsplandatei an.   |
| SET DRMPLANPREFIX  | Gibt das Präfix des Pfadnamens für den Wiederherstellungsplan an.   |
| SET DRMPRIMSTGPOOL   | Gibt an, dass primäre Speicherpools von DRM verwaltet werden.   |
| SET DRMRPFEXPIREDAYS   | Definiert Verfallskriterien für Wiederherstellungsplandateien.  |
| SET DRMVaultNAME   | Gibt den Namen des Aufbewahrungsorts an, an dem DRM-Datenträger gespeichert werden.                                 |
| SET DRMNOTMOUNTABLENAME  | Gibt den Standortnamen der DRM-Datenträger an, die ausgelagert werden sollen.                                       |

## QUERY ENABLED (Aktivierte Ereignisse abfragen)

Mit diesem Befehl kann eine Liste der aktivierten Ereignisse oder eine Liste der inaktivierten Ereignisse (die kürzere Liste) angezeigt werden.

## Berechtigungsklasse

---

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

---

```
>>-Query--Enabled--+-CONSOLE-----+----->
      +-ACTLOG-----+
      +-EVENTSERVER----+
      +-FILE-----+
      +-FILETEXT-----+
      |           (1) |
      +-NTEVENTLOG-----+
      |           (2) |
      +-SYSLOG-----+
      +-TIVOLI-----+
      '-USEREXIT-----'

>--+-----><
  +-NODename---Knotenname---+
  '-SERVername-----Servername-'
```

Anmerkungen:

1. Dieser Parameter ist nur für das Windows-Betriebssystem verfügbar.
2. Dieser Parameter ist nur für das Linux-Betriebssystem verfügbar.

### Parameter

---

#### Empfänger

Gibt eine Art des Empfängers für aktivierte Ereignisse an. Dieser Parameter ist erforderlich. Gültige Werte sind:

##### ACTLOG

Gibt das IBM Spectrum Protect-Aktivitätenprotokoll als Empfänger an.

##### CONSOLE

Gibt die Standardserverkonsole als Empfänger an.

##### EVENTSERVER

Gibt den Ereignisserver als Empfänger an.

##### FILE

Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist ein Satz in der Datei, und eine Person kann jedes protokollierte Ereignis nicht einfach lesen.


##### FILETEXT

Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.

##### Windows-Betriebssysteme NTEVENTLOG

 Windows-Betriebssysteme Gibt das Windows-Anwendungsprotokoll als Empfänger an.

##### Linux-Betriebssysteme SYSLOG

 Linux-Betriebssysteme Gibt das Linux-Systemprotokoll als Empfänger an.

##### TIVOLI

Gibt Tivoli Management Environment (TME) als Empfänger an.

##### USEREXIT

Gibt eine benutzerdefinierte Routine, in die IBM Spectrum Protect Informationen schreibt, als Empfänger an.

#### NODename

Gibt einen Knotennamen an, der abgefragt werden soll. Der Benutzer kann NODENAME oder SERVERNAME angeben. Wird keiner der Parameter angegeben, bezieht sich die Abfrage auf die Ereignisse, die für den Server aktiviert sind, der diesen Befehl ausführt.

#### SERVername

Gibt einen Servernamen an, der abgefragt werden soll. Der Benutzer kann NODENAME oder SERVERNAME angeben. Wird keiner der Parameter angegeben, bezieht sich die Abfrage auf die Ereignisse, die für den Server aktiviert sind, der diesen Befehl ausführt.

### Beispiel: Den Server nach Konsolereignissen abfragen

---

Den Server nach Serverereignissen abfragen, die für die Konsole aktiviert sind. Es gibt 10000 mögliche Serverereignisse. Es wird eine Liste der aktivierten Ereignisse oder der inaktivierten Ereignisse (die kürzere Liste) angezeigt.

```
query enabled console
```



9998  
Ereignisse für Empfänger CONSOLE aktiviert. Folgende  
Ereignisse sind für Empfänger CONSOLE inaktiviert:

ANR8409, ANR8410

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY ENABLED

| Befehl             | Beschreibung   |
|--------------------|--|
| BEGIN EVENTLOGGING | Startet das Ereignisprotokoll für einen bestimmten Empfänger.  |
| DISABLE EVENTS     | Inaktiviert bestimmte Ereignisse für Empfänger.  |
| ENABLE EVENTS      | Aktiviert bestimmte Ereignisse für Empfänger.  |
| END EVENTLOGGING   | Beendet das Ereignisprotokoll für einen bestimmten Empfänger.  |
| QUERY EVENTRULES   | Zeigt Informationen über Regeln für Server- und Clientereignisse an.   |
| QUERY STATUS       | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## QUERY EVENT (Geplante und abgeschlossene Ereignisse abfragen)

Mit diesem Befehl kann der Status geplanter Ereignisse angezeigt werden. Mit den Parametern für Uhrzeit und Datum können Sie die Abfrage auf Ereignisse begrenzen, die innerhalb der angegebenen Uhrzeiten und Datumsangaben stattfinden sollten. Wird die Ausgabe auf Ereignisse begrenzt, deren geplante Startzeiten innerhalb eines Datums- und Zeitbereichs liegen, wird auch die Zeit für die Verarbeitung dieser Abfrage verkürzt.

Die Befehlsyntax unterscheidet sich bei Abfragen, die sich auf geplante Client-Operationen und geplante Verwaltungsbefehle beziehen.

Tabelle 1. Zugehörige Befehle für QUERY EVENT

| Befehl             | Beschreibung   |
|--------------------|--|
| DEFINE SCHEDULE    | Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl.                                  |
| DELETE EVENT       | Löscht Ereignissätze, die vor einem bestimmten Zeitpunkt erstellt wurden.  |
| QUERY ACTLOG       | Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.   |
| SET EVENTRETENTION | Gibt die Anzahl Tage für die Aufbewahrung von Sätzen geplanter Operationen an.                                   |
| SET RANDOMIZE      | Gibt die Zufallsgenerierung von Startzeiten innerhalb eines Fensters für Zeitpläne im Clientsendeaufrufmodus an. |

- QUERY EVENT (Clientzeitpläne anzeigen)  
Mit dem Befehl QUERY EVENT können geplante und abgeschlossene Ereignisse für ausgewählte Clients angezeigt werden.
- QUERY EVENT (Ereignisse für Verwaltungszeitpläne anzeigen)  
Mit dem Befehl QUERY EVENT können geplante und abgeschlossene Ereignisse für ausgewählte Verwaltungsbefehlszeitpläne angezeigt werden.

## QUERY EVENT (Clientzeitpläne anzeigen)

Mit dem Befehl QUERY EVENT können geplante und abgeschlossene Ereignisse für ausgewählte Clients angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query EVent--Domänename--Zeitplanname----->
```



| Wert                        | Beschreibung   | Beispiel  |
|-----------------------------|--|---|
| BOTM (Anfang dieses Monats) | Der erste Tag des aktuellen Monats.                      | BOTM  |
| BOTM+Tage                   | Der erste Tag des aktuellen Monats plus angegebene Tage. | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren. |

#### BEGINTime

Gibt die Anfangszeit des Bereichs an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start innerhalb dieses Zeitraums geplant ist, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist 00:00.

Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

| Wert                         | Beschreibung   | Beispiel  |
|------------------------------|--|---|
| HH:MM:SS                     | Eine bestimmte Uhrzeit am angegebenen Anfangsdatum                             | 10:30:08  |
| NOW                          | Die aktuelle Uhrzeit am angegebenen Anfangsdatum                               | NOW   |
| NOW+HH:MM <b>oder</b> +HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Anfangsdatum  | NOW+03:00 <b>oder</b> +03:00.<br><br>Wird dieser Befehl um 9:00 Uhr ausgegeben, um Ereignisse abzufragen, deren Start in 3 Stunden geplant ist, kann entweder <code>BEGINTIME=NOW+03:00</code> oder <code>BEGINTIME=+03:00</code> angegeben werden. IBM Spectrum Protect zeigt dann Ereignisse um 12:00 Uhr am angegebenen Anfangsdatum an.   |
| NOW-HH:MM <b>oder</b> -HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Anfangsdatum | NOW-04:00 <b>oder</b> -04:00.<br><br>Wird dieser Befehl um 9:00 Uhr ausgegeben, um Ereignisse abzufragen, deren Start während der letzten 4 Stunden geplant war, kann entweder <code>BEGINTIME=NOW-04:00</code> <code>ENDTIME=NOW</code> oder <code>BEGINTIME=-04:00</code> <code>ENDTIME=NOW</code> angegeben werden. IBM Spectrum Protect zeigt dann Ereignisse um 5:00 Uhr am angegebenen Anfangsdatum an. |

#### ENDDate

Gibt das Enddatum des Zeitraums an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start während dieser Zeit geplant war, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist der für `BEGINDATE` verwendete Wert.

Sie können das Datum unter Verwendung der folgenden Werte angeben:

| Wert                           | Beschreibung  | Beispiel  |
|--------------------------------|---|---|
| MM/TT/JJJJ                     | Ein bestimmtes Datum  | 09/15/1998  |
| TODAY                          | Das aktuelle Datum  | TODAY   |
| TODAY+Tage <b>oder</b> +Tage   | Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY +3 <b>oder</b> +3.  |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage  | TODAY-8 <b>oder</b> -8.<br><br>Sollen Ereignisse abgefragt werden, deren Start während einer einwöchigen Periode, die gestern zu Ende ging, geplant war, kann entweder <code>BEGINDATE=TODAY-8</code> <code>ENDDATE=TODAY-1</code> oder <code>BEGINDATE=-8</code> <code>ENDDATE=-1</code> angegeben werden. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.   | EOLM  |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.   | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.  |

| Wert                        | Beschreibung   | Beispiel  |
|-----------------------------|--|---|
| BOTM (Anfang dieses Monats) | Der erste Tag des aktuellen Monats.                      | BOTM  |
| BOTM+Tage                   | Der erste Tag des aktuellen Monats plus angegebene Tage. | BOTM+9<br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren. |

#### ENDTime

Gibt die Endzeit des Bereichs an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start innerhalb dieser Zeitspanne geplant war, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist 23:59.

Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

| Wert                         | Beschreibung   | Beispiel  |
|------------------------------|--|---|
| HH:MM:SS                     | Eine bestimmte Uhrzeit am angegebenen Enddatum                             | 10:30:08  |
| NOW                          | Die aktuelle Uhrzeit am angegebenen Enddatum                               | NOW   |
| NOW+HH:MM <b>oder</b> +HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum  | NOW+03:00 <b>oder</b> +03:00.<br>Wird dieser Befehl um 9:00 Uhr ausgegeben, um Ereignisse abzufragen, deren Start in 3 Stunden geplant ist, kann entweder <code>BEGINTIME=NOW</code> <code>ENDTIME=NOW+03:00</code> oder <code>BEGINTIME=NOW</code> <code>ENDTIME=+03:00</code> angegeben werden. |
| NOW-HH:MM <b>oder</b> -HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum | NOW-04:00 <b>oder</b> -04:00  |

#### Exceptiononly

Gibt die Art der Informationen an, die über geplante oder abgeschlossene Ereignisse gewünscht werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No

Gibt an, daß die Informationen zu vergangenen und projektierten Ereignissen angezeigt werden.

Yes

Gibt an, daß die Ereignisse angezeigt werden, die fehlgeschlagen sind oder nicht wie geplant verarbeitet wurden.

#### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Die folgenden Werte sind gültig:

Standard

Gibt an, dass Teilinformationen für Ereignisse angezeigt werden.

Detailed

Gibt an, dass die gesamten Informationen für Ereignisse angezeigt werden.

## Teilinformationen zu nicht erfolgreichen Ereignissen anzeigen

Teilinformationen zu allen für DOMAIN1 geplanten Ereignissen, deren Ausführung nicht erfolgreich war, anzeigen. Die Suche soll sich auf den Client JOE beschränken. Außerdem sollen nur die Ereignisse angezeigt werden, deren Ausführung in der Zeit vom 11. Februar 2001 (02/11/2001) bis 12. Februar 2001 (02/12/2001) geplant war.

```
query event domain1 * nodes=joe begindate=02/11/2001
enddate=02/12/2001 exceptiononly=yes
```

| Geplanter Start     | Ist-Start           | Zeitplan-<br>name | Knoten-<br>name | Status |
|---------------------|---------------------|-------------------|-----------------|--------|
| 02/11/1999 01:00:00 | 02/11/1999 01:13:55 | BACK1             | JOE             | Failed |
| 02/12/1999 01:00:00 |                     | DAILYBKP          | JOE             | Missed |

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Teilinformationen zu geplanten Ereignissen für einen Client anzeigen

Die gesamten Informationen für alle Ereignisse anzeigen, die für die Verarbeitung geplant sind. Als Startdatum 10 Tage vor dem heutigen Datum definieren und beim Enddatum den heutigen Tag einschließen.

```
query event * * begindate=today-10 enddate=today
```

| Geplanter Start     | Ist-Start           | Zeitplan-name | Knoten-name  | Status    |
|---------------------|---------------------|---------------|--------------|-----------|
| 02/04/2013 14:00:00 |                     | SCHD_INCR-DM1 | TSM_CET_DM1  | Missed    |
| 02/04/2013 14:00:00 | 02/04/2013 14:12:49 | VDATAMVR1-IN1 | VDATAMVR1-T1 | Completed |
| 02/04/2013 14:30:00 | 02/04/2013 14:33:10 | VDATAMVR1-IN2 | VDATAMVR1-T2 | Completed |
| 02/04/2013 15:00:00 | 02/04/2013 15:01:49 | VDATAMVR1-IN3 | VDATAMVR1-T3 | Completed |
| 02/04/2013 15:30:00 | 02/04/2013 15:42:00 | VDATAMVR1-IN4 | VDATAMVR1-T4 | Completed |
| 02/05/2013 14:00:00 |                     | SCHD_INCR-DM1 | TSM_CET_DM1  | Missed    |
| 02/05/2013 14:00:00 | 02/05/2013 14:05:22 | VDATAMVR1-F1  | VDATAMVR1-F1 | Completed |
| 02/05/2013 14:30:00 | 02/05/2013 14:32:53 | VDATAMVR1-F2  | VDATAMVR1-F2 | Failed 12 |
| 02/05/2013 15:00:00 | 02/05/2013 15:00:38 | VDATAMVR1-F3  | VDATAMVR1-F3 | Completed |
| 02/05/2013 15:30:00 | 02/05/2013 15:36:41 | VDATAMVR1-F4  | VDATAMVR1-F4 | Completed |
| 02/06/2013 14:00:00 |                     | SCHD_INCR-DM1 | TSM_CET_DM1  | Missed    |
| 02/06/2013 14:00:00 | 02/06/2013 14:06:42 | VDATAMVR1-F1  | VDATAMVR1-F1 | Completed |
| 02/06/2013 14:30:00 | 02/06/2013 14:35:41 | VDATAMVR1-F2  | VDATAMVR1-F2 | Completed |
| 02/06/2013 15:00:00 | 02/06/2013 15:08:56 | VDATAMVR1-F3  | VDATAMVR1-F3 | Completed |
| 02/06/2013 15:30:00 | 02/06/2013 15:40:49 | VDATAMVR1-F4  | VDATAMVR1-F4 | Completed |
| 02/07/2013 14:00:00 |                     | SCHD_INCR-DM1 | TSM_CET_DM1  | Missed    |
| 02/07/2013 14:00:00 | 02/07/2013 14:03:43 | VDATAMVR1-F1  | VDATAMVR1-F1 | Completed |
| 02/07/2013 14:30:00 | 02/07/2013 14:35:10 | VDATAMVR1-F2  | VDATAMVR1-F2 | Completed |
| 02/07/2013 15:00:00 | 02/07/2013 15:09:12 | VDATAMVR1-F3  | VDATAMVR1-F3 | Completed |
| 02/07/2013 15:30:00 | 02/07/2013 15:40:21 | VDATAMVR1-F4  | VDATAMVR1-F4 | Completed |
| 02/08/2013 14:00:00 |                     | SCHD_INCR-DM1 | TSM_CET_DM1  | Missed    |
| 02/08/2013 14:00:00 | 02/08/2013 14:10:17 | VDATAMVR1-F1  | VDATAMVR1-F1 | Completed |
| 02/08/2013 14:30:00 | 02/08/2013 14:39:16 | VDATAMVR1-F2  | VDATAMVR1-F2 | Completed |
| 02/08/2013 15:00:00 | 02/08/2013 15:08:17 | VDATAMVR1-F3  | VDATAMVR1-F3 | Completed |
| 02/08/2013 15:30:00 | 02/08/2013 15:41:16 | VDATAMVR1-F4  | VDATAMVR1-F4 | Completed |
| 02/09/2013 14:00:00 |                     | SCHD_INCR-DM1 | TSM_CET_DM1  | Missed    |
| 02/09/2013 14:02:16 |                     | VDATAMVR1-F1  | VDATAMVR1-F1 | Failed 12 |
| 02/09/2013 14:30:00 | 02/09/2013 14:44:26 | VDATAMVR1-F2  | VDATAMVR1-F2 | Failed 12 |
| 02/09/2013 15:00:00 | 02/09/2013 15:06:24 | VDATAMVR1-F3  | VDATAMVR1-F3 | Failed 12 |
| 02/09/2013 15:30:00 | 02/09/2013 15:32:18 | VDATAMVR1-F4  | VDATAMVR1-F4 | Completed |
| 02/11/2013 14:00:00 |                     | SCHD_INCR-DM1 | TSM_CET_DM1  | Missed    |
| 02/11/2013 14:00:00 | 02/11/2013 14:01:05 | VDATAMVR1-F1  | VDATAMVR1-F1 | Failed 12 |
| 02/11/2013 14:30:00 | 02/11/2013 14:31:42 | VDATAMVR1-F2  | VDATAMVR1-F2 | Failed 12 |
| 02/11/2013 15:00:00 | 02/11/2013 15:06:17 | VDATAMVR1-F3  | VDATAMVR1-F3 | Failed 12 |
| 02/11/2013 15:30:00 | 02/11/2013 15:30:19 | VDATAMVR1-F4  | VDATAMVR1-F4 | Completed |
| 02/12/2013 14:00:00 |                     | SCHD_INCR-DM1 | TSM_CET_DM1  | Missed    |
| 02/12/2013 14:00:00 | 02/12/2013 14:03:37 | VDATAMVR1-F1  | VDATAMVR1-F1 | Completed |
| 02/12/2013 14:30:00 | 02/12/2013 14:33:07 | VDATAMVR1-F2  | VDATAMVR1-F2 | Completed |
| 02/12/2013 15:00:00 | 02/12/2013 15:03:56 | VDATAMVR1-F3  | VDATAMVR1-F3 | Completed |
| 02/12/2013 15:30:00 | 02/12/2013 15:36:44 | VDATAMVR1-F4  | VDATAMVR1-F4 | Completed |
| 02/13/2013 14:00:00 |                     | SCHD_INCR-DM1 | TSM_CET_DM1  | Missed    |
| 02/13/2013 14:00:00 | 02/13/2013 14:06:24 | VDATAMVR1-F1  | VDATAMVR1-F1 | Completed |
| 02/13/2013 14:30:00 | 02/13/2013 14:34:50 | VDATAMVR1-F2  | VDATAMVR1-F2 | Completed |
| 02/13/2013 15:00:00 | 02/13/2013 15:15:01 | VDATAMVR1-F3  | VDATAMVR1-F3 | Completed |
| 02/13/2013 15:30:00 | 02/13/2013 15:30:18 | VDATAMVR1-F4  | VDATAMVR1-F4 | Completed |
| 02/14/2013 14:00:00 |                     | SCHD_INCR-DM1 | TSM_CET_DM1  | Future    |
| 02/14/2013 14:00:00 |                     | VDATAMVR1-F1  | VDATAMVR1-F1 | Future    |
| 02/14/2013 14:30:00 |                     | VDATAMVR1-F2  | VDATAMVR1-F2 | Future    |
| 02/14/2013 15:00:00 |                     | VDATAMVR1-F3  | VDATAMVR1-F3 | Future    |

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Ausführliche Informationen zu geplanten Ereignissen für einen Client anzeigen

Die ausführlichen Informationen zu Ereignissen anzeigen, deren Verarbeitung durch den Client DOC zwischen 10:00 Uhr und 11:00 Uhr am 1. November 2005 (11/01/2005) geplant ist. Lautet der Status FAILED (Fehlgeschlagen), wird der Ergebniscode angezeigt.

```
query event domain1 * nodes=doc begindate=11/01/2005
begintime=10:00 endtime=11:00 enddate=11/01/2005
exceptiononly=yes format=detailed
```

| Geplanter Start     | Ist-Start           | Zeitplan-name | Knoten-name | Status    |
|---------------------|---------------------|---------------|-------------|-----------|
| 11/01/2005 10:01:01 | 11/01/2005 10:03:46 | T1            | DOC         | Failed 8  |
| 11/01/2005 10:16:01 | 11/01/2005 10:16:10 | T1            | DOC         | Failed 4  |
| 11/01/2005 10:31:01 | 11/01/2005 10:33:08 | T1            | DOC         | Completed |
| 11/01/2005 10:46:01 |                     | T1            | DOC         | Missed    |
| 11/01/2005 10:57:49 | 11/01/2005 10:58:07 | T0            | DOC         | Failed 12 |

## Feldbeschreibungen

Name der Maßnahmendomäne

Gibt den Namen der Maßnahmendomäne an, der der Zeitplan zugeordnet ist.

Zeitplanname

Gibt den Namen des Zeitplans an, der dieses Ereignis eingeleitet hat.

Knotenname

Gibt den Client an, der für die Ausführung der Operation geplant ist.

Geplanter Start

Gibt das geplante Startdatum und die geplante Uhrzeit für das Ereignis an.

Ist-Start

Gibt das Datum und die Uhrzeit an, an dem bzw. zu der der Client mit der Verarbeitung der geplanten Operation begonnen hat.

Wurde die geplante Operation nicht gestartet, werden keine Informationen angezeigt.

Completed

Gibt an, wann das geplante Ereignis abgeschlossen wurde (Datum und Uhrzeit).

Status

Gibt den Status des Ereignisses zu dem Zeitpunkt an, zu dem der Befehl QUERY EVENT ausgegeben wird. Die folgenden Werte sind gültig:

Completed

Gibt an, dass das geplante Ereignis abgeschlossen ist.

Failed

Gibt an, dass der Client bei der Ausführung der geplanten Operation einen Fehler festgestellt hat und aufeinanderfolgende Wiederholungsversuche fehlgeschlagen sind.

Failed - no restart

Gibt einen temporären Status an, wenn eine Clientsitzung durch einen Übertragungsfehler oder eine Zeitlimitüberschreitung auf dem Server unterbrochen wird. Dieser Status kann in den endgültigen Status "Completed" oder "Failed" geändert werden, wenn das Ereignis abgeschlossen ist.

Future

Gibt an, dass der Beginn des Startfensters für das Ereignis in der Zukunft liegt. Dieser Status gibt außerdem an, dass kein Ereignissatz für dieses Ereignis erstellt wurde.

In Progress

Gibt an, dass das geplante Ereignis gerade ausgeführt wird, aber die Beendigung noch nicht an den Server gemeldet wurde.

Überprüfen Sie regelmäßig den Status auf Beendigung des geplanten Ereignisses. Wird dieser Status nicht in einer angemessenen Zeit aktualisiert, überprüfen Sie dsmsched.log und dsmerror.log des Clients, um zu bestimmen, warum der Client das Ergebnis dieses Ereignisses nicht an den Server gemeldet hat. Ist die geplante Sicherung fehlgeschlagen, führen Sie das geplante Ereignis erneut aus oder führen Sie eine manuelle Teilsicherung aus, um die Datensicherung zu gewährleisten.

Missed

Gibt an, dass das geplante Startfenster für dieses Ereignis abgelaufen ist und mit der Ausführung nicht begonnen wurde.

Pending

Gibt an, dass der Befehl QUERY EVENT innerhalb des Startfensters für das Ereignis ausgegeben wurde, die Verarbeitung der geplanten Operation jedoch nicht begonnen hat.

Restarted

Gibt an, dass der Client versucht hat, die geplante Operation erneut zu verarbeiten.

Severed

Gibt an, dass die Übertragung zum Client unterbrochen wurde, bevor das Ereignis abgeschlossen werden konnte.

Started

Gibt an, dass die Verarbeitung des Ereignisses begonnen hat.

Uncertain

Gibt an, dass der Status des Ereignisses nicht ermittelt werden kann. Der Server gibt immer dann `Uncertain` an, wenn der Befehl QUERY EVENT keinen Ereignissatz finden kann. Ein Ereignissatz wird nicht gefunden, wenn der Satz gelöscht wurde oder der Server während des geplanten Startfensters nicht verfügbar war (der Zeitplan wurde nie gestartet). Sätze mit dem Status "Uncertain" werden nicht in der Datenbank gespeichert. Sollen diese Sätze nicht angezeigt werden, ist entweder `EXCEPTIONSONLY=YES` anzugeben oder der Zeitplan zu löschen, wenn er nicht mehr benötigt wird.

Achtung: Wenn eine geplante Operation verarbeitet wird und innerhalb der angegebenen Dauer nicht erneut gestartet wird, zeigt das Feld Status `Gestartet` an. Wird die Operation über die angegebene Dauer hinaus fortgesetzt, wird kein Ereignissatz erstellt. Wird nach Ablauf der angegebenen Dauer eine Abfrage ausgegeben, wird der Status als `Fehlgeschlagen` angezeigt, auch wenn die Operation noch ausgeführt wird. Nach Abschluss der Operation wird ein Ereignissatz erstellt, und eine nachfolgende Abfrage zeigt das Ergebnis in dem Statusfeld an.

Ergebnis

Gibt den Rückkehrcode an, der anzeigt, ob der Zeitplan erfolgreich verarbeitet wurde. Wenn der Rückkehrcode einen anderen Wert als 0 hat, prüfen Sie das Serveraktivitätenprotokoll sowie das Fehlerprotokoll und das Planungsprotokoll des Clients.

| Rückkehrcode | Erläuterung |
|--------------|-------------|
|--------------|-------------|

| Rückkehrcode | Erläuterung   |
|--------------|---|
| 0            | Alle Operationen wurden erfolgreich abgeschlossen.  |
| 4            | Die Operation wurde abgeschlossen, einige Dateien wurden jedoch nicht verarbeitet.  |
| 8            | Die Operation wurde mit mindestens einer Warnung abgeschlossen.   |
| 12           | Die Operation wurde mit mindestens einer Fehlernachricht abgeschlossen. Die Anzahl Fehlernachrichten schließt keine Benachrichtigungen über übersprungene Dateien ein.  |
| -99          | Die Operation ist fehlgeschlagen, da die Sitzung zwischen dem Client und dem Server aus einem unbekanntem Grund beendet wurde. Es ist nicht bekannt, ob der Client die Verbindung zum Server wiederherstellen kann, um das geplante Ereignis auszuführen. |

Verfügt ein Zeitplan über ACTION=COMMAND als Parameter, und ist der Befehl kein IBM Spectrum Protect-Befehl, kann der Befehl andere Werte im Feld Ergebnis generieren.

Ursache

Gibt die Ursache des Rückkehrcodes an.

## QUERY EVENT (Ereignisse für Verwaltungszeitpläne anzeigen)

Mit dem Befehl QUERY EVENT können geplante und abgeschlossene Ereignisse für ausgewählte Verwaltungsbefehlszeitpläne angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query EVerit--Zeitplanname--Type----Administrative----->
      .-BEGINDate----aktuelles_Datum-.  .-BEGINTime----00:00-.
>-+-----+-----+-----+-----+-----+----->
      '-BEGINDate----Datum-'           '-BEGINTime----Zeit--'

      .-ENDDate----Datum-.  .-ENDTime----23:59-.
>-+-----+-----+-----+-----+-----+----->
      '-ENDDate----Datum-'           '-ENDTime----Zeit--'

      .-EXceptiononly----No------.
>-+-----+-----+-----+-----+-----+----->
      '-EXceptiononly----No--+-'
                                     '-Yes-'

      .-Format----Standard-----.
>-+-----+-----+-----+-----+-----+-----><
      '-Format----+-Standard--+'
                                     '-Detailed-'
```

### Parameter

Zeitplanname (Erforderlich)

Gibt den Namen des Zeitplans an, für den Ereignisse angezeigt werden. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

Type=Administrative (Erforderlich)

Gibt an, dass die Abfrage Ereignisse für Verwaltungszeitpläne anzeigt.

BEGINDate

Gibt das Anfangsdatum des Zeitraums an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start innerhalb dieses Zeitraums geplant ist, werden angezeigt. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum.

Sie können das Datum unter Verwendung der folgenden Werte angeben:

| Wert       | Beschreibung         | Beispiel   |
|------------|----------------------|------------|
| MM/TT/JJJJ | Ein bestimmtes Datum | 09/15/1998 |
| TODAY      | Das aktuelle Datum   | TODAY      |

| Wert                             | Beschreibung  | Beispiel   |
|----------------------------------|---|--|
| TODAY+Tage <b>oder</b><br>+Tage  | Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY +3 <b>oder</b> +3.   |
| TODAY-Tage <b>oder</b> -<br>Tage | Das aktuelle Datum minus der Anzahl der angegebenen Tage  | TODAY-7 <b>oder</b> -7.<br><br>Sollen Ereignisse abgefragt werden, deren Start während der vergangenen sieben Tage geplant war, BEGINDATE=TODAY-7 ENDDATE=TODAY oder BEGINDATE=-7 ENDDATE=TODAY angeben. |
| EOLM (Ende des letzten Monats)   | Der letzte Tag des Vormonats.   | EOLM   |
| EOLM-Tage                        | Der letzte Tag des Vormonats minus angegebene Tage.   | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.   |
| BOTM (Anfang dieses Monats)      | Der erste Tag des aktuellen Monats.   | BOTM   |
| BOTM+Tage                        | Der erste Tag des aktuellen Monats plus angegebene Tage.  | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.  |

#### BEGINTime

Gibt die Anfangszeit des Bereichs an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start innerhalb dieses Zeitraums geplant ist, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist 00:00.

Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

| Wert                             | Beschreibung   | Beispiel  |
|----------------------------------|--|---|
| HH:MM:SS                         | Eine bestimmte Uhrzeit am angegebenen Anfangsdatum                             | 10:30:08  |
| NOW                              | Die aktuelle Uhrzeit am angegebenen Anfangsdatum                               | NOW   |
| NOW+HH:MM <b>oder</b><br>+HH:MM  | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Anfangsdatum  | NOW+03:00 <b>oder</b> +03:00.<br><br>Wird dieser Befehl um 9:00 Uhr ausgegeben, um Ereignisse abzufragen, deren Start in 3 Stunden geplant ist, kann entweder BEGINTIME=NOW+03:00 oder BEGINTIME=+03:00 angegeben werden. IBM Spectrum Protect zeigt dann Ereignisse um 12:00 Uhr am angegebenen Anfangsdatum an.   |
| NOW-HH:MM <b>oder</b> -<br>HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Anfangsdatum | NOW-04:00 <b>oder</b> -04:00.<br><br>Wird dieser Befehl um 9:00 Uhr ausgegeben, um Ereignisse abzufragen, deren Start während der letzten 4 Stunden geplant war, kann entweder BEGINTIME=NOW-04:00 ENDTIME=NOW oder BEGINTIME=-04:00 ENDTIME=NOW angegeben werden. IBM Spectrum Protect zeigt dann Ereignisse um 5:00 Uhr am angegebenen Anfangsdatum an. |

#### ENDDate

Gibt das Enddatum des Zeitraums an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start während dieser Zeit geplant war, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist der für BEGINDATE verwendete Wert.

Sie können das Datum unter Verwendung der folgenden Werte angeben:

| Wert       | Beschreibung         | Beispiel   |
|------------|----------------------|------------|
| MM/TT/JJJJ | Ein bestimmtes Datum | 09/15/1998 |
| TODAY      | Das aktuelle Datum   | TODAY      |



| Wert                             | Beschreibung  | Beispiel  |
|----------------------------------|---|---|
| TODAY+Tage <b>oder</b><br>+Tage  | Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY +3 <b>oder</b> +3.  |
| TODAY-Tage <b>oder</b> -<br>Tage | Das aktuelle Datum minus der Anzahl der angegebenen Tage  | TODAY-8 <b>oder</b> -8.<br><br>Sollen Ereignisse abgefragt werden, deren Start während einer einwöchigen Periode, die gestern zu Ende ging, geplant war, kann entweder BEGINDATE=TODAY-8 ENDDATE=TODAY-1 oder BEGINDATE=-8 ENDDATE=-1 angegeben werden. |
| EOLM (Ende des letzten Monats)   | Der letzte Tag des Vormonats.   | EOLM  |
| EOLM-Tage                        | Der letzte Tag des Vormonats minus angegebene Tage.   | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.  |
| BOTM (Anfang dieses Monats)      | Der erste Tag des aktuellen Monats.   | BOTM  |
| BOTM+Tage                        | Der erste Tag des aktuellen Monats plus angegebene Tage.  | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.   |

#### ENDTime

Gibt die Endzeit des Bereichs an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start innerhalb dieser Zeitspanne geplant war, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist 23:59. Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

| Wert                             | Beschreibung   | Beispiel  |
|----------------------------------|--|---|
| HH:MM:SS                         | Eine bestimmte Uhrzeit am angegebenen Enddatum                             | 10:30:08  |
| NOW                              | Die aktuelle Uhrzeit am angegebenen Enddatum                               | NOW   |
| NOW+HH:MM <b>oder</b><br>+HH:MM  | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum  | NOW+03:00 <b>oder</b> +03:00.<br><br>Wird dieser Befehl um 9:00 Uhr ausgegeben, um Ereignisse abzufragen, deren Start in 3 Stunden geplant ist, kann entweder BEGINTIME=NOW ENDTIME=NOW+03:00 oder BEGINTIME=NOW ENDTIME=+03:00 angegeben werden. |
| NOW-HH:MM <b>oder</b> -<br>HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum | NOW-04:00 <b>oder</b> -04:00  |

#### EXceptiononly

Gibt die Art der Informationen an, die über geplante oder abgeschlossene Ereignisse gewünscht werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No

Gibt an, daß die Informationen zu vergangenen und projektierten Ereignissen angezeigt werden.

Yes

Gibt an, daß die Ereignisse angezeigt werden, die fehlgeschlagen sind oder nicht wie geplant verarbeitet wurden.

#### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

Standard

Gibt an, dass Teilinformationen für Ereignisse angezeigt werden.

Detailed

Gibt an, dass die gesamten Informationen für Ereignisse angezeigt werden.

## Beispiel: Ereignisse für einen bestimmten Verwaltungszeitplan auflisten

Teilinformationen für alle Ereignisse anzeigen, die für den Verwaltungszeitplan DOSADMIN geplant waren. Die Abfrage auf Ereignisse begrenzen, die am 30. März 1999 (03/30/1999) geplant sind. Den folgenden Befehl ausgeben:

```
query event dosadmin type=administrative
begindate=03/30/1999
enddate=03/30/1999
```

| Geplanter Start     | Ist-Start           | Zeitplan-<br>klasse | Status    |
|---------------------|---------------------|---------------------|-----------|
| 03/30/1999 00:00:00 | 03/30/1999 00:00:01 | DOSADMIN            | Completed |
| 03/30/1999 04:00:00 | 03/30/1999 04:00:01 | DOSADMIN            | Completed |
| 03/30/1999 12:00:00 |                     | DOSADMIN            | Future    |
| 03/30/1999 16:00:00 |                     | DOSADMIN            | Future    |

## Feldbeschreibungen

### Geplanter Start

Gibt das geplante Startdatum und die geplante Uhrzeit für das Ereignis an.

### Ist-Start

Gibt das Datum und die Uhrzeit an, an dem bzw. zu der der Client mit der Verarbeitung der geplanten Operation begonnen hat. Wurde die Ausführung des Zeitplans noch nicht gestartet, werden keine Informationen angezeigt.

### Zeitplanname

Gibt den Namen des Zeitplans an, der dieses Ereignis eingeleitet hat.

### Status

Für Verwaltungsbefehle oder Scripts, die WAIT=YES angeben, ist der Status eines geplanten Ereignisses STARTED, bis die mit dem Befehl oder dem Script angegebene Operation abgeschlossen ist. Der endgültige Status des geplanten Ereignisses hängt vom Rückkehrcode der Operation ab. Ist jedoch WAIT=YES angegeben und führt der Zeitplan ein Script aus, das PREVIEW=YES angibt, lautet der endgültige Status COMPLETED, es sei denn, das Script enthielt einen Syntaxfehler.

Für Verwaltungsbefehle oder Scripts, die WAIT=NO angeben, ist der Status eines geplanten Ereignisses COMPLETED, wenn der geplante Befehl oder das Script gestartet wurde. Der Erfolg des Zeitplans ist nicht vom Erfolg der Operation abhängig, die mit dem Befehl oder dem Script ausgeführt wurde.

## QUERY EVENTRULES (Regeln für Server- oder Clientereignisse abfragen)

Mit diesem Befehl kann die History von Ereignissen, die von einem bestimmten Empfänger aktiviert oder inaktiviert wurden, für den Server oder einen Client-Knoten angezeigt werden.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```

.*-----
>>-Query--EVENTRULes--+-----><
| .,-----|
| v-----|
+---+--CONSOLE-----+
| +-ACTLOG-----+
| +-EVENTSERVER-----+
| +-FILE-----+
| +-FILETEXT-----+
| | (1) |
| +-NTEVENTLOG-----+
| | (2) |
| +-SYSLOG-----+
| +-TIVOLI-----+
| '-USEREXIT-----'
+-NODENAME----Knotenname---+
'-SERVERNAME----Servername-'

```

Anmerkungen:

1. Dieser Parameter ist nur für das Windows-Betriebssystem verfügbar.
2. Dieser Parameter ist nur für das Linux-Betriebssystem verfügbar.

## Parameter

---

### Empfänger

Gibt den Namen eines oder mehrerer Empfänger für aktivierte Ereignisse an. Dieser Parameter ist wahlfrei.

Es kann ein Platzhalterzeichen verwendet werden, um alle Empfänger anzugeben.

Gültige Werte sind:

#### CONSOLE

Gibt die Standardkonsole als Empfänger an.

#### ACTLOG

Gibt das IBM Spectrum Protect-Aktivitätenprotokoll als Empfänger an.

#### EVENTSERVER


Gibt den Ereignisserver als Empfänger an.

#### FILE


Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist ein Satz in der Datei, und eine Person kann jedes protokollierte Ereignis nicht einfach lesen.

#### FILETEXT

Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.

 Windows-BetriebssystemeNTEVENTLOG

 Windows-BetriebssystemeGibt das Windows-Anwendungsprotokoll als Empfänger an.

 Linux-BetriebssystemeSYSLOG

 Linux-BetriebssystemeGibt das Linux-Systemprotokoll als Empfänger an.

#### TIVOLI

Gibt Tivoli Management Environment (TME) als Empfänger an.

#### USEREXIT

Gibt eine benutzerdefinierte Routine, in die IBM Spectrum Protect Informationen schreibt, als Empfänger an.

### NODENAME

Gibt einen Knotennamen an, der abgefragt werden soll. Es kann ein Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Der Benutzer kann NODENAME oder SERVERNAME angeben. Wird keiner der Parameter angegeben, bezieht sich die Abfrage auf Ereignisregeln für den Server, der diesen Befehl ausführt.

### SERVer

Gibt einen Servernamen an, der abgefragt werden soll. Es kann ein Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Der Benutzer kann NODENAME oder SERVERNAME angeben. Wird keiner der Parameter angegeben, bezieht sich die Abfrage auf Ereignisregeln für den Server, der diesen Befehl ausführt.

## Beispiel: Die History von Clientereignissen für die Serverkonsole anzeigen

---

Die History von Clientereignissen anzeigen, die für die Serverkonsole und für Aktivitätenprotokollempfänger aktiviert oder inaktiviert sind.

```
query eventrules console,actlog nodename=*
```

| Datum/Zeit        | Client-Ereignisregeln                         |
|-------------------|---|
| -----             | -----   |
| 05/29/97 13:39:58 | ENABLE EVENTS CONSOLE ANE4001 NODENAMES=JEE   |
| 05/30/97 13:46:25 | DISABLE EVENTS ACTLOG ANE4962 NODENAMES=JEE   |
| 05/30/97 13:46:25 | DISABLE EVENTS ACTLOG ANE4963 NODENAMES=JEE   |
| 05/30/97 13:46:25 | DISABLE EVENTS ACTLOG ANE4965 NODENAMES=JEE   |
| 05/30/97 13:46:25 | DISABLE EVENTS ACTLOG ANE4966 NODENAMES=JEE   |
| 05/30/97 13:46:25 | DISABLE EVENTS ACTLOG ANE4967 NODENAMES=JEE   |
| 05/30/97 13:46:25 | DISABLE EVENTS ACTLOG ANE4968 NODENAMES=JEE   |
| 05/30/97 14:24:20 | ENABLE EVENTS CONSOLE ANE4015 NODENAMES=RON   |
| 05/30/97 14:24:50 | ENABLE EVENTS CONSOLE ANE4026 NODENAMES=DONNA |
| 05/30/97 14:25:59 | ENABLE EVENTS CONSOLE ANE4015 NODENAMES=DONNA |

## Beispiel: Die History von Clientereignissen für alle Empfänger anzeigen

---

Die History von Serverereignissen anzeigen, die für alle Empfänger aktiviert oder inaktiviert sind.

```
query eventrules
```

| Datum/Zeit        | Server-Ereignisregeln          |
|-------------------|--------------------------------|
| -----             | -----                          |
| 05/22/97 14:35:13 | ENABLE EVENTS CONSOLE ANR2578  |
| 05/30/97 14:29:31 | ENABLE EVENTS CONSOLE ANR0272  |
| 05/30/97 14:31:46 | ENABLE EVENTS USEREXIT ANR0130 |

## Feldbeschreibungen

---

### Datum/Zeit

Gibt das Datum und die Uhrzeit an, an dem bzw. zu der das Ereignis aktiviert oder inaktiviert wurde.

### Client-Ereignisregeln

Gibt die Clientereignisse an, die für die angegebenen Empfänger aktiviert oder inaktiviert wurden.

### Server-Ereignisregeln

Gibt die Serverereignisse an, die für die angegebenen Empfänger aktiviert oder inaktiviert wurden.

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für QUERY ENABLED

| Befehl             | Beschreibung   |
|--------------------|--|
| BEGIN EVENTLOGGING | Startet das Ereignisprotokoll für einen bestimmten Empfänger.                    |
| DISABLE EVENTS     | Inaktiviert bestimmte Ereignisse für Empfänger.                                  |
| ENABLE EVENTS      | Aktiviert bestimmte Ereignisse für Empfänger.                                    |
| END EVENTLOGGING   | Beendet das Ereignisprotokoll für einen bestimmten Empfänger.                    |
| QUERY ENABLED      | Zeigt aktivierte bzw. inaktivierte Ereignisse für einen bestimmten Empfänger an. |

## QUERY EVENTSERVER (Ereignisserver abfragen)

---

Mit diesem Befehl kann der Name des Ereignisserver angezeigt werden.

### Berechtigungsklasse

---

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

---

```
>>-Query EVENTSERVER-----<<
```

### Beispiel: Den Namen des Ereignisserver anzeigen

---

Den Namen des Ereignisserver anzeigen.

```
query eventserver
```

```
ANR1669I Server EVENT  
ist als Ereignisserver definiert.
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für QUERY EVENTSERVER

| Befehl             | Beschreibung  |
|--------------------|---|
| BEGIN EVENTLOGGING | Startet das Ereignisprotokoll für einen bestimmten Empfänger. |
| DEFINE EVENTSERVER | Definiert einen Server als Ereignisserver.                    |
| DEFINE SERVER      | Definiert einen Server für die Übertragung zwischen Servern.  |
| DELETE EVENTSERVER | Löscht Verweise auf den Ereignisserver.                       |
| DELETE SERVER      | Löscht die Definition eines Servers.                          |
| END EVENTLOGGING   | Beendet das Ereignisprotokoll für einen bestimmten Empfänger. |

## QUERY EXPORT (Aktive oder ausgesetzte Exportoperationen abfragen)

---

Mit diesem Befehl können alle wieder anlauffähigen Exportoperationen aufgelistet werden. Ein wiederanlauffähiger Export ist eine Exportoperation zwischen Servern, deren Wert für FILEDATA nicht NONE ist. Es werden nur aktive Exportoperationen zwischen Servern angezeigt, die ausgesetzt werden können.

EXPORT NODE- oder EXPORT SERVER-Operationen mit FILEDATA=NONE werden nicht angezeigt. Außerdem zeigt der Befehl QUERY EXPORT keine Exportoperationen, bei denen die Zieleinheit eine Einheit mit sequenziellen oder virtuellen Datenträgern ist.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```

      .-*-----
>>-Query EXPort----->
      '---Export-ID---'

      .-State----All-----
>+-----+-----+----->
      '-State----+All-----+' '-PROcess----Prozessnummer-'
          +-RUnning---+
          '-SUSPended-'

      .-Format----Standard-----
>+-----+-----+-----><
      '-Format----+Standard-+'
          '-Detailed-'

```

## Parameter

### Export-ID

Dieser optionale Parameter ist die eindeutige Zeichenfolge-ID für die Exportoperation zwischen Servern. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. In diesem Fall werden alle übereinstimmenden Exportoperationen abgefragt. Wird kein Wert für diesen Parameter angegeben und wird auch keine PROZESS-ID angegeben, werden alle Exportoperationen abgefragt.

### StAte

Dieser optionale Parameter fragt den Status der gültigen Exportoperationen zwischen Servern ab. Der Standardwert ist ALL. Gültige Werte sind:

#### ALL

Alle aktiven und ausgesetzten Exportoperationen zwischen Servern werden aufgelistet.

#### RUnning

Alle aktiven Exportoperationen zwischen Servern, die auswählbare Dateien angeben oder Dateien auf den Zielsever exportieren, werden aufgelistet.

#### SUSPended

Alle ausgesetzten Exportoperationen zwischen Servern werden aufgelistet. Die Ausführung dieser ausgesetzten Operationen wurde durch einen Fehler oder durch die Ausgabe des Befehls SUSPEND EXPORT gestoppt.

### PROcess

Dieser optionale Parameter gibt die Nummer einer aktiven Exportoperation zwischen Servern an, die Sie abfragen wollen. Wird PROCESS angegeben, zeigt IBM Spectrum Protect nur die aktive Exportoperation zwischen Servern an, die der Prozessnummer zugeordnet ist. Wird PROCESS nicht angegeben, zeigt IBM Spectrum Protect Informationen zu allen Exportoperationen zwischen Servern an. Sie können diesen Parameter nicht angeben, wenn Sie eine Export-ID oder den Parameter STATE mit dem Wert SUSPENDED angeben.

### Format

Dieser optionale Parameter gibt an, wie die Informationen angezeigt werden. Der Standardwert ist STANDARD. Gültige Werte:

#### Standard

Gibt an, dass Teilinformationen für die angegebenen Exportoperationen angezeigt werden.

#### Detailed

Falls angegeben, werden alle verfügbaren Informationen für die Exportoperationen angezeigt.

## Beispiel: Aktive und ausgesetzte Exportoperationen anzeigen

Informationen für alle Exportoperationen auflisten, die momentan aktiv oder ausgesetzt sind. Geben Sie den folgenden Befehl aus:

```
query export state=all
```

| Export-ID        | Startzeit              | Status                     | Prozess-ID | Befehl   |
|------------------|------------------------|----------------------------|------------|--|
| MYEXPORTNODE     | 01/24/2007<br>10:30:03 | Ausgesetzt                 | --         | Export NODE<br>me,you,them<br>filespace=c\$<br>nametype=unicode<br>filedata=all<br>durunits=indefinite<br>toserver=athens<br>exportid=MYEXPORTNODE |
| EXPORT_HOME_DIRS | 01/25/2007<br>09:30:03 | Aktiv                      | 11         | Export NODE n2,n3,n4<br>filespace=/home<br>nametype=server<br>filedata=all<br>durunits=indefinite<br>toserver=athens<br>exportid=EXPORT_HOME_DIRS  |
| EXPORT_NODE_0001 | 01/25/2007<br>14:30:33 | Aktiv, nicht<br>aussetzbar | --         | Export NODE n5,n6,n7<br>filespace=d\$<br>nametype=unicode<br>filedata=archive<br>durunits=indefinite<br>toserver=athens                            |

Für Felddesreibungen siehe Felddesreibungen.

## Beispiel: Informationen zu einer aktiven Exportoperation anzeigen

Informationen für die momentan aktive Exportoperation mit Prozessnummer "7" auflisten. Den folgenden Befehl ausgeben:

```
query export process=7
```

| Export-ID    | Startzeit              | Status | Prozess-ID | Befehl  |
|--------------|------------------------|--------|------------|---|
| MYEXPORTNODE | 01/24/2007<br>10:30:03 | Aktiv  | 7          | Export NODE<br>me,you,them<br>filespace=c\$<br>nametype=unicode<br>filedata=all<br>toserver=athens<br>exportid=MYEXPORTNODE |

Für Felddesreibungen siehe Felddesreibungen.

## Beispiel: Ausführliche Informationen zu allen ausgesetzten Exportoperationen anzeigen

Informationen für alle Exportoperationen auflisten, die momentan ausgesetzt sind. Geben Sie den folgenden Befehl aus:

```
query export state=suspended format=detailed
```

```
Export-ID : MyExportNode
Startzeit : 01/24/2007 10:30:03
Status : Ausgesetzt
Prozess-ID : --
Befehl: Export NODE m* filespace=c$
nametype=unicode
filedata=all durunits=indefinite
toserver=athens
Phase : Dateiliste vollständig.
Auswählbare Dateien werden exportiert
Gesamtausführungszeit : 3 Tag 0 Stunden 24 Minuten
Ausführungszeit des aktuellen Prozesses :
Anzahl Neustarts der Exportoperation: 0
Datum und Uhrzeit des letzten Neustarts : --
Datum und Uhrzeit der letzten Aussetzung : 01/25/2007 08:30:11
Exportierte Maßnahmendomänen : 0
Exportierte Maßnahmengruppen : 0
Exportierte Zeitpläne : 0
Exportierte Verwaltungsklassen : 0
Exportierte Kopiengruppen : 0
```

```

Exportierte Administratoren : 1
Exportierte Optionsgruppen : 0
Exportierte Knotendefinitionen : 3
Exportierte Dateibereichsdefinitionen : 7
Exportierte Archivierungsdateien : 50.000
Exportierte Sicherungsdateien : 150.000
Exportierte speicher verwaltete Dateien : 0
Übersprungene Archivierungsdateien : 0
Übersprungene Sicherungsdateien : 25
Übersprungene speicher verwaltete Dateien : 0
Summe der übertragenen Byte (MB) : 7.000
Summe der zu übertragenden Dateien : 900.000
Verbleibende Dateien : 700.000

```

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Beispiel: Informationen zu Exportoperation zwischen Servern anzeigen

---

Listen Sie detaillierte Informationen zu allen Exportoperationen auf, die momentan aktiv sind. Geben Sie den folgenden Befehl aus:

```
query export state=running format=detailed
```

```

Export-ID : export_HOME_Dirs
Startzeit : 01/25/2007 09:30:03
Status : Aktiv
Prozess-ID : 11
Befehl: Export NODE n2,n3,n4
        filespace=/home nametype=
        server filedata=all
        toserver=athens
Phase : Auswählbare Dateien angeben
        und exportieren
Gesamtausführungszeit : 0 Tage 22 Stunden 0 Minuten
Ausführungszeit des aktuellen Prozesses : 01:30:00
Anzahl Neustarts der Exportoperation: 4
Datum und Uhrzeit des letzten Neustarts : 02/01/2007 11:00:03
Datum und Uhrzeit der letzten Aussetzung : 01/31/2007 05:01:00
Exportierte Maßnahmendomänen : 0
Exportierte Maßnahmengruppen : 0
Exportierte Zeitpläne : 0
Exportierte Verwaltungsklassen : 0
Exportierte Kopiengruppen : 0
Exportierte Administratoren : 1
Exportierte Optionsgruppen : 0
Exportierte Knotendefinitionen : 3
Exportierte Dateibereichsdefinitionen : 7
Exportierte Archivierungsdateien : 0
Exportierte Sicherungsdateien : 1000
Exportierte speicher verwaltete Dateien : 0
Übersprungene Archivierungsdateien : 0
Übersprungene Sicherungsdateien : 0
Übersprungene speicher verwaltete Dateien : 0
Summe der übertragenen Byte (MB) : 50
Summe der zu übertragenden Dateien : 400.000
Verbleibende Dateien : 399.000

```

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Feldbeschreibungen

---

### Export-ID

Die eindeutige ID, die dieser Exportoperation zwischen Servern zugeordnet ist.

### Startzeit

Der Zeitpunkt (Datum und Uhrzeit), an dem diese Exportoperation zum ersten Mal eingeleitet wurde.

### Status

Der aktuelle Status dieser Exportoperation. Mögliche Werte sind:

#### Aktiv - Nicht aussetzbar

Die Operation ist aktiv und überträgt gerade Definitionen an den Zielsever. Der Prozess kann nicht ausgesetzt werden. Wenn in diesem Status ein Prozessfehler auftritt, können Sie den Prozess nicht erneut starten.

#### Aktiv

Die Operation ist aktiv und sucht gerade nach auswählbaren Dateien oder überträgt gerade Dateidaten an den Zielsever.

#### Aktiv - Aussetzen wird ausgeführt

Die Operation wird gerade als Folge eines Befehls SUSPEND EXPORT ausgesetzt. Die Exportoperation ist vollständig ausgesetzt, wenn alle Daten aus der Exportoperation gesichert sind. Eine Exportoperation in diesem Status antwortet nicht auf die folgenden Befehle:

- CANCEL PROCESS
- CANCEL EXPORT
- RESTART EXPORT
- SUSPEND EXPORT

Ausgesetzt

Die Ausführung der Operation wurde durch einen Fehler gestoppt oder durch den Befehl SUSPEND EXPORT ausgesetzt.

Prozess-ID

Die Prozess-ID für die Exportoperation im Status "Wird initialisiert" oder "Aktiv".

Befehl

Der vollständig ausgegebene Befehl zum Starten dieser Exportoperation zwischen Servern.

Phase

Der aktuelle Schritt, der von der Operation gerade ausgeführt wird. Die gültigen Phasen sind in der Reihenfolge aufgeführt, in der sie ausgeführt werden:

Definitionen auf Zielservers erstellen

Die Operation exportiert Definitionen. Der Prozess kann nicht ausgesetzt werden. Schlägt der Prozess in dieser Phase fehl, kann er nicht erneut gestartet werden.

Auswählbare Dateien angeben und exportieren

Die Operation erstellt eine Liste der auswählbaren Dateien für den Export. Einige Dateien können in dieser Phase auch an den Zielservers übertragen werden. Der Prozess kann in dieser Phase ausgesetzt werden. Schlägt der Prozess in dieser Phase fehl, kann er erneut gestartet werden.

Dateiliste vollständig. Auswählbare Dateien werden exportiert.

Die Erstellung der Liste der auswählbaren Dateien für den Export ist beendet. Die Dateien werden jetzt an das Ziel übertragen. Der Prozess kann in dieser Phase ausgesetzt werden. Schlägt der Prozess in dieser Phase fehl, kann er erneut gestartet werden.

Gesamtausführungszeit

Die Gesamtausführungszeit für diese Exportoperation zwischen Servern. Beispiel: Wurde diese Operation gestartet und dann zweimal ausgesetzt und erneut gestartet, gibt dieser Wert die Gesamtausführungszeit aller drei aktiven Prozesse der Exportoperation an.

Ausführungszeit des aktuellen Prozesses

Die Ausführungszeit des aktiven Prozesses einer Exportoperation zwischen Servern. Für eine ausgesetzte Operation wird kein Wert angezeigt, weil kein aktiver Prozess vorhanden ist.

Anzahl Neustarts der Exportoperation

Gibt an, wie oft die Exportoperation zwischen Servern erneut gestartet wurde.

Datum und Uhrzeit des letzten Neustarts

Das Datum und die Uhrzeit des letzten Neustarts dieser Exportoperation zwischen Servern.

Datum und Uhrzeit der letzten Aussetzung

Das Datum und die Uhrzeit der letzten Aussetzung dieser Exportoperation zwischen Servern.

Exportierte Maßnahmendomänen

Die Anzahl der Maßnahmendomänendefinitionen, die erfolgreich auf den Zielservers exportiert wurden.

Exportierte Maßnahmengruppen

Die Anzahl der Maßnahmengruppendefinitionen, die erfolgreich auf den Zielservers exportiert wurden.

Exportierte Zeitpläne

Die Anzahl der Zeitplandefinitionen, die erfolgreich auf den Zielservers exportiert wurden.

Exportierte Verwaltungsklassen

Die Anzahl der Verwaltungsklassendefinitionen, die erfolgreich auf den Zielservers exportiert wurden.

Exportierte Kopiengruppen

Die Anzahl der Kopiengruppendefinitionen, die erfolgreich auf den Zielservers exportiert wurden.

Exportierte Administratoren

Die Anzahl der Administratordefinitionen, die erfolgreich auf den Zielservers exportiert wurden.

Exportierte Optionsgruppen

Die Anzahl der Optionsgruppendifinitionen, die erfolgreich auf den Zielservers exportiert wurden.

Exportierte Knotendefinitionen

Die Anzahl der Knotendefinitionen, die erfolgreich auf den Zielservers exportiert wurden.

Exportierte Dateibereichsdefinitionen

Die Anzahl der Dateibereichsdefinitionen, die erfolgreich auf den Zielservers exportiert wurden.

Exportierte Archivierungsdateien

Die Anzahl der Archivierungsdateien, die erfolgreich auf den Zielservers exportiert wurden.

Exportierte Sicherungsdateien






- Die Anzahl der Sicherungsdateien, die erfolgreich auf den Zielsever exportiert wurden.
- Exportierte speicherverwaltete Dateien
  - Die Anzahl der speicherverwalteten Dateien, die erfolgreich auf den Zielsever exportiert wurden.
- Übersprungene Archivierungsdateien
  - Die Anzahl der Archivierungsdateien, die zum Exportieren ausgewählt werden konnten, aber übersprungen wurden.
- Übersprungene Sicherungsdateien
  - Die Anzahl der Sicherungsdateien, die zum Exportieren ausgewählt werden konnten, aber übersprungen wurden.
- Übersprungene speicherverwaltete Dateien
  - Die Anzahl der speicherverwalteten Dateien, die zum Exportieren ausgewählt werden konnten, aber übersprungen wurden.
- Summe der übertragenen Byte (MB)
  - Die Gesamtzahl der bisher an den Zielsever übertragenen Byte für diese Exportoperation.
- Summe der zu übertragenden Dateien
  - Die Gesamtzahl der an den Zielsever zu übertragenden Dateien für diese Exportoperation.
- Verbleibende Dateien
  - Die Gesamtzahl der Dateien, die für diese Exportoperation noch an den Zielsever übertragen werden müssen.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY EXPORT

| Befehl         | Beschreibung  |
|----------------|---|
| CANCEL PROCESS | Bricht einen Serverhintergrundprozess ab.   |
| CANCEL EXPORT  | Löscht eine ausgesetzte Exportoperation.  |
| EXPORT NODE    | Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.                       |
| EXPORT SERVER  | Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server. |
| IMPORT NODE    | Schreibt Clientknotendaten von externen Datenträgern zurück.  |
| IMPORT SERVER  | Schreibt den gesamten Server oder einen Teil davon von externen Datenträgern zurück.                                  |
| QUERY PROCESS  | Zeigt Informationen über Hintergrundprozesse an.  |
| RESTART EXPORT | Startet eine ausgesetzte Exportoperation erneut.  |
| SUSPEND EXPORT | Setzt eine aktive Exportoperation aus.  |

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## QUERY EXTENTUPDATES (Aktualisierte Datenbereiche abfragen)

Verwenden Sie diesen Befehl, um Informationen zu Aktualisierungen an Datenbereichen in Verzeichniscontainerspeicherpools anzuzeigen und zu bestimmen, welche Datenbereiche gelöscht werden und welche Datenbereiche zum Löschen auswählbar sind.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query EXTENTUPDates--Poolname-----<<
```

### Parameter

Poolname (Erforderlich)

Gibt den Speicherpool an, der abgefragt werden soll. Sie können zur Angabe dieses Namens keine Platzhalterzeichen verwenden.

### Beispiel: Informationen zu Aktualisierungen an Datenbereichen anzeigen

Zeigen Sie Informationen zu Aktualisierungen an Datenbereichen an, indem Sie den folgenden Befehl ausgeben:

```
query extentupdates
```

Anzahl Bereiche mit anstehender Aktualisierung: 0  
Anzahl nicht referenzierter Bereiche: 0  
Anzahl der zum Löschen auswählbaren Bereiche: 0  
Wiederverwendungsverzögerung (Tage) für Bereiche: 1

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Feldbeschreibungen

Anzahl Bereiche mit anstehender Aktualisierung

Gibt die Anzahl Datenbereichsreferenzen an, für die eine Aktualisierung im Verzeichniscontainerspeicherpool ansteht. Daten, die im Verzeichniscontainerspeicherpool gespeichert werden, erhöhen die Anzahl Referenzen; Daten, die gelöscht werden, verringern die Anzahl Referenzen.

Anzahl nicht referenzierter Bereiche

Gibt die Anzahl Datenbereiche an, die nicht im Verzeichniscontainerspeicherpool referenziert werden. Sie können die Datenbereiche löschen, wenn sie nicht erneut innerhalb des im Befehl DEFINE STGPOOL angegebenen Verzögerungszeitraums für Wiederverwendung referenziert werden.

Anzahl der zum Löschen auswählbaren Bereiche

Gibt die Anzahl Datenbereiche an, die aus dem Speicherpool gelöscht werden können. Für die Datenbereiche wird der im Befehl DEFINE STGPOOL angegebene Verzögerungszeitraum für Wiederverwendung überschritten.

Wiederverwendungsverzögerung (Tage) für Bereiche

Gibt die Wiederverwendungsverzögerung für Datenbereiche in Tagen an.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY EXTENTUPDATES

| Befehl                                | Beschreibung   |
|---------------------------------------|--|
| DEFINE STGPOOL (Verzeichniscontainer) | Definiert einen Verzeichniscontainerspeicherpool.  |
| DELETE STGPOOLDIRECTORY               | Löscht ein Speicherpoolverzeichnis aus einem Verzeichniscontainer- oder Cloud-Containerspeicherpool. |

## QUERY FILESPACE (Dateibereiche abfragen)

Mit diesem Befehl können Informationen über Dateibereiche angezeigt werden, die zu einem Clientknoten gehören. Die Ausgabe dieses Befehls schließt die Ergebnisse der letzten Teilsicherung oder Replikation ein.

Tipp: Verfügt ein Knoten über mehrere Dateibereiche, können Sie einen Befehl DELETE FILESPACE für einen der Dateibereiche ausgeben. Geben Sie jedoch während des Löschprozesses einen Befehl QUERY FILESPACE für den Knoten aus, zeigt die Ausgabe keine Dateibereiche an. Um genaue Informationen zu den verbleibenden Dateibereichen zu erhalten, geben Sie den Befehl QUERY FILESPACE aus, nachdem der Löschprozess beendet wurde.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
.-*--*-----
>>>Query Filespace----->
|                          |
|    .-*-----          |
|'-Knotename-----+'
|          '-Dateibereichsname-'
|
.-Format----Standard----.  .-NAMEType----SERVER-----
>----->
'-Format-----+Standard-+'  '-NAMEType-----+SERVER-++'
          '-Detailed-'          +-Unicode-+
                                '-FSID----'

.-CODEType----BOTH-----
>-----<
'-CODEType-----+Unicode----+'
          +-NONUnicode-+
          '-BOTH-----'
```

## Parameter

---

### Knotenname

Gibt den Clientknoten an, zu dem der Dateibereich gehört. Dieser Name kann mithilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert ist alle Clientknotennamen.

Für diesen Parameter muss ein Wert angegeben werden, wenn ein Dateiname angegeben wird.

### Dateibereichsname

Gibt den Namen des Dateibereichs an, der abgefragt werden soll. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Wird kein Wert angegeben, werden alle Dateibereiche abgefragt.

Wenn ein Server Clients einschließt, die Unicode-fähige Dateibereiche verwenden, muss der Server möglicherweise den eingegebenen Namen konvertieren. Beispielsweise muss der Server gegebenenfalls den Dateibereichsnamen, den Sie eingeben, aus der Zeichenumsetztabelle des Servers in Unicode konvertieren. Weitere Informationen enthält die Beschreibung des Parameters NAMETYPE. Geben Sie keinen Dateibereichsnamen an oder geben Sie nur ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter CODETYPE verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

Bei Dateibereichsnamen muss die Groß-/Kleinschreibung berücksichtigt werden. Mit dem Befehl QUERY FILESPACE kann die korrekte Schreibweise für den abzufragenden Dateibereich bestimmt werden.

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Sie können einen der folgenden Werte angeben:

#### Standard

Gibt an, dass Teilinformationen für den angegebenen Dateibereich angezeigt werden.

#### Detailed

Gibt an, dass die gesamten Informationen für den angegebenen Dateibereich angezeigt werden.

### NAMETYPE

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unterstützung für Unicode verfügt. Sie können diesen Parameter für Unicode-fähige IBM Spectrum Protect-Clients verwenden, die über die Betriebssysteme Windows, Macintosh OS X und NetWare verfügen.

Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen eingeben. Der Standardwert lautet SERVER. Sie können einen der folgenden Werte angeben:

#### SERVER

Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren.

#### UNICODE

Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server Probleme beim Zugriff auf die Systemkonvertierungsroutinen hat.

#### FSID

Der Server interpretiert die Dateibereichsnamen als ihre Dateibereichs-IDs (FSIDs).

### CODETYPE

Angeben, welche Art von Dateibereichen in der Operation berücksichtigt werden soll. Der Standardwert lautet BOTH. Dieser Standardwert bedeutet, dass Dateibereiche unabhängig vom Typ der Codepage eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben. Sie können einen der folgenden Werte angeben:

#### UNICODE

Nur Dateibereiche einschließen, die in Unicode sind.

#### NONUNICODE

Nur Dateibereiche einschließen, die nicht in Unicode sind.

#### BOTH

Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen.

## Beispiel: Alle Dateibereiche auflisten

---

Alle Dateibereiche abfragen, die allen Clientknoten zugeordnet sind.

```
query filespace
```

| Knotenname | Dateibereichsname | FSID | Plattform | Dateibereichstyp | Ist Dateibereich Unicode? | Kapazität | % Ausl. |
|------------|-------------------|------|-----------|------------------|---------------------------|-----------|---------|
| JOE        | \\joe\c\$         | 1    | WinNT     | NTFS             | Yes                       | 2.502,3   | 75,2    |
| JOE        | \\joe\d\$         | 2    | WinNT     | NTFS             | Yes                       | 6.173,4   | 59,6    |

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Beispiel: Ausführliche Dateibereichsinformationen zu einem virtuellen Dateibereich anzeigen

Ausführliche Informationen zu dem Dateibereich /HomeDir anzeigen, der eine virtuelle Dateibereichszuordnung ist und zu dem NAS-Knoten NAS1 gehört.

```
query fileSPACE nas1 /HomeDir
```

| Knotenname | Dateibereichsname | FSID | Plattform | Dateibereichstyp | Ist Dateibereich Unicode? | Kapazität | % Ausl. |
|------------|-------------------|------|-----------|------------------|---------------------------|-----------|---------|
| NAS1       | /HomeDir          | 1    | NetApp    | WAFL (VFS)       | No                        | 2.502,3   | 75,2    |

Für Feldbeschreibungen siehe Feldbeschreibungen.

Wichtig: Möglicherweise werden die erwarteten Ergebnisse nicht angezeigt, nachdem ein ausführliches Format angefordert wurde, da einige Felder von der API-Anwendung ausgefüllt werden müssen. Zu diesen Feldern gehören:

- Dateibereichstyp
- Plattform
- Kapazität
- Auslastung in %
- Startdatum/-zeit der letzten Sicherung
- Fertigstellungsdatum/-zeit der letzten Sicherung

Weitere Informationen zu bestimmten Feldern, die von der API aktualisiert werden, befinden sich im Handbuch *IBM Spectrum Protect: Verwendung der Anwendungsprogrammierschnittstelle*.

## Beispiel: Ausführliche Dateibereichsinformationen zu einem bestimmten Dateibereich und Knoten anzeigen

Ausführliche Informationen zu dem Dateibereich \\joe\c\$ anzeigen, der zum Clientknoten JOE gehört.

```
query fileSPACE joe \\joe\c$ nametype=unicode format=detailed
```

```

Knotenname: JOE
Dateibereichsname: \\joe\c$
Hexadezimaler Dateibereichsname: 5c5c6a6f655c6324
FSID: 1
Name der Kollokationsgruppe: FSGRP1
Plattform: WinNT
Dateibereichstyp: NTFS
Ist Dateibereich Unicode?: Yes
Kapazität: 2.502,3
Auslastung in %: 75,2
Start der letzten Sicherung:
Tage seit Start der letzten Sicherung:
Abschluss der letzten Sicherung:
Tage seit Abschluss der letzten Sicherung:
Startdatum/-zeit der letzten Replikation: 12/02/2012, 12:42:00
Tage seit Start der letzten Knotenreplikation: 30
Fertigstellungsdatum/-zeit der letzten Replikation: 12/02/2012, 12:42:00
Tage seit Abschluss der letzten Replikation: 30
Datum/Zeit der letzten Sicherung des Clients (UTC): 06/02/2013, 09:10:00
Datum/Zeit der letzten Archivierung des Clients (UTC): 06/02/2013, 09:10:00
Name der Replikationsregel für Sicherungsdaten: ACTIVE_DATA
Status der Replikationsregel für Sicherungsdaten: ENABLED
Name der Replikationsregel für Archivierungsdaten: DEFAULT
Status der Replikationsregel für Archivierungsdaten: ENABLED
Name der Replikationsregel für speicher verwaltete Daten: NONE
Status der Replikationsregel für speicher verwaltete Daten: DISABLED

Typ für Gefährdung: Angepasstes Intervall
Gefährdungsintervall: 2,222
Stillgelegt: Nein

```

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Feldbeschreibungen

---

Wichtig: Möglicherweise werden die erwarteten Ergebnisse nicht angezeigt, nachdem ein ausführliches Format angefordert wurde, da einige Felder von der API-Anwendung ausgefüllt werden müssen. Zu diesen Feldern gehören:

- Dateibereichstyp
- Plattform
- Kapazität
- Auslastung in %
- Startdatum/-zeit der letzten Sicherung
- Abschluss der letzten Sicherung

Weitere Informationen zu bestimmten Feldern, die von der API aktualisiert werden, befinden sich im Handbuch *IBM Spectrum Protect: Verwendung der Anwendungsprogrammierschnittstelle*.

Knotenname

Gibt den Namen des Clientknotens an.

Dateibereichsname

Der Name des Dateibereichs, der zu dem Knoten gehört.

Dateibereichsnamen können eine andere Zeichenumsetzungstabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetzungstabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetzungstabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetzungstabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

Hexadezimaler Dateibereichsname

Gibt den hexadezimalen Namen des Dateibereichs für den Clientknoten im UTF-8-Format an.

FSID

Gibt die Dateibereichs-ID des Dateibereichs an.

Name der Kollokationsgruppe

Der Name der Kollokationsgruppe (sofern vorhanden), zu der der Dateibereich gehört.

Plattform

Gibt die Plattform für den Clientknoten an.

Dateibereichstyp

Gibt den Typ des Dateibereichs an.

Ein Dateibereichstyp, dem "(VFS)" angehängt ist, gibt an, dass dieser Dateibereichsname eine virtuelle Dateibereichszuordnung für einen Verzeichnispfad auf einer NAS-Einheit ist.

Ist Dateibereich Unicode?

Gibt an, ob der Dateibereich in Unicode ist.

Kapazität

Gibt den Speicherbereich in Megabyte an, der diesem Dateibereich auf dem Clientknoten zugeordnet ist.

Bei einem Dateibereich, der eine virtuelle Dateibereichszuordnung für einen Verzeichnispfad ist, gibt dieses Feld die Kapazität des Dateibereichs an, in dem sich der Verzeichnispfad befindet.

Auslastung in %

Gibt den Prozentsatz des belegten Dateibereichs an.

Bei einem Dateibereich, der eine virtuelle Dateibereichszuordnung für einen Verzeichnispfad ist, wird die prozentuale Auslastung als Prozentsatz der Kapazität des Dateibereichs berechnet, der von dem Verzeichnis zum Zeitpunkt der letzten Gesamtsicherung belegt wurde.

Startdatum/-zeit der letzten Sicherung

Gibt das Startdatum und die Startzeit der letzten Teilsicherung des Dateibereichs an.

Tage seit Start der letzten Sicherung

Gibt die Anzahl der Tage seit dem Start der letzten Teilsicherung des Dateibereichs an.  
 Abschluss der letzten Sicherung  
 Gibt das Datum und die Uhrzeit an, an dem bzw. zu der die letzte Teilsicherung des Dateibereichs abgeschlossen wurde.  
 Tage seit Abschluss der letzten Sicherung  
 Gibt die Anzahl der Tage seit dem Abschluss der letzten Teilsicherung des Dateibereichs an.  
 Startdatum/-zeit der letzten Replikation  
 Gibt das Datum und die Uhrzeit an, an dem bzw. zu der die letzte Replikation der Dateibereichsdaten gestartet wurde.  
 Tage seit Start der letzten Replikation  
 Gibt die Anzahl der Tage seit dem Start der letzten Replikation der Dateibereichsdaten an.  
 Fertigstellungsdatum/-zeit der letzten Replikation  
 Gibt das Datum und die Uhrzeit an, an dem bzw. zu der die letzte Replikation der Dateibereichsdaten beendet wurde.  
 Tage seit Abschluss der letzten Replikation  
 Gibt die Anzahl der Tage seit dem Ende der letzten Replikation der Dateibereichsdaten an.  
 Datum/Zeit der letzten Sicherung des Clients (UTC)  
 Das Datum und die Uhrzeit (in koordinierter Weltzeit - UTC) der letzten Sicherungsoperation für diesen Dateibereich.  
 Datum/Zeit der letzten Archivierung des Clients (UTC)  
 Das Datum und die Uhrzeit (in koordinierter Weltzeit - UTC) der letzten Archivierungsoperation für diesen Dateibereich.  
 Name der Replikationsregel für Sicherungsdaten  
 Gibt die Replikationsregel an, die für Sicherungsdaten in dem Dateibereich gilt. Die folgenden Werte sind gültig:

**ALL\_DATA**

Repliziert aktive und inaktive Sicherungsdaten. Die Daten werden mit einer normalen Priorität repliziert.

**ACTIVE\_DATA**

Repliziert nur aktive Sicherungsdaten. Die Daten werden mit einer normalen Priorität repliziert.

Achtung: Wenn Sie ACTIVE\_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

- Wenn eine frühere Serverversion als Version 7.1.1 auf dem Quellen- oder Zielreplikationsserver installiert ist.
- Wenn Sie den Befehl REPLICATE NODE mit dem Parameter `FORCERECONCILE=YES` verwenden.
- Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Serverversion vor Version 7.1.1 ausführen.

Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

**ALL\_DATA\_HIGH\_PRIORITY**

Repliziert aktive und inaktive Sicherungsdaten. Die Daten werden mit einer hohen Priorität repliziert.

**ACTIVE\_DATA\_HIGH\_PRIORITY**

Diese Regel entspricht der Replikationsregel ACTIVE\_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden.

**DEFAULT**

Repliziert Sicherungsdaten gemäß der Clientknotenregel für Sicherungsdaten. Lautet die Clientknotenregel für Sicherungsdaten DEFAULT, werden Sicherungsdaten gemäß der Serverregel für Sicherungsdaten repliziert.

**NONE**

Sicherungsdaten in dem Dateibereich werden nicht repliziert.

**Status der Replikationsregel für Sicherungsdaten**

Gibt an, ob die Replikation der Sicherungsdaten in dem Dateibereich aktiviert oder inaktiviert ist. Lautet der Status 'Aktiviert', können Sicherungsdateien für die Replikation ausgewählt werden. Lautet der Status 'Inaktiviert', können Sicherungsdateien nicht für die Replikation ausgewählt werden.

**Name der Replikationsregel für Archivierungsdaten**

Gibt die Replikationsregel an, die für Archivierungsdaten in dem Dateibereich gilt. Die folgenden Werte sind gültig:

**ALL\_DATA**

Repliziert Archivierungsdaten. Die Daten werden mit einer normalen Priorität repliziert.

**ALL\_DATA\_HIGH\_PRIORITY**

Repliziert Archivierungsdaten. Die Daten werden mit einer hohen Priorität repliziert.

**DEFAULT**

Repliziert Archivierungsdaten gemäß der Clientregel für Archivierungsdaten. Lautet die Clientregel für Archivierungsdaten DEFAULT, werden Archivierungsdaten gemäß der Serverregel für Archivierungsdaten repliziert.

**NONE**

Archivierungsdaten in dem Dateibereich werden nicht repliziert.

**Status der Replikationsregel für Archivierungsdaten**

Gibt an, ob die Replikation der Archivierungsdaten in dem Dateibereich aktiviert oder inaktiviert ist. Lautet der Status 'Aktiviert', können Archivierungsdateien für die Replikation ausgewählt werden. Lautet der Status 'Inaktiviert', können Archivierungsdateien nicht für die Replikation ausgewählt werden.

Name der Replikationsregel für speicher verwaltete Daten

Gibt die Replikationsregel an, die für speicher verwaltete Daten in dem Dateibereich gilt. Die folgenden Werte sind gültig:

ALL\_DATA

Repliziert speicher verwaltete Daten. Die Daten werden mit einer normalen Priorität repliziert.

ALL\_DATA\_HIGH\_PRIORITY

Repliziert speicher verwaltete Daten. Die Daten werden mit einer hohen Priorität repliziert.

DEFAULT

Repliziert speicher verwaltete Daten gemäß der Clientregel für speicher verwaltete Daten. Lautet die Clientregel für speicher verwaltete Daten DEFAULT, werden speicher verwaltete Daten gemäß der Serverregel für speicher verwaltete Daten repliziert.

NONE

Speicher verwaltete Daten in dem Dateibereich werden nicht repliziert.

Status der Replikationsregel für speicher verwaltete Daten

Gibt an, ob die Replikation der speicher verwalteten Daten in dem Dateibereich aktiviert oder inaktiviert ist. Lautet der Status 'Aktiviert', können speicher verwaltete Dateien für die Replikation ausgewählt werden. Lautet der Status 'Inaktiviert', können speicher verwaltete Dateien nicht für die Replikation ausgewählt werden.

Typ für Gefährdung

Gibt den Auswertungstyp für Gefährdung an. Die gültigen Werte sind 'Standard', 'Übergangen' oder 'Angepasst'. 'Standard' gibt an, dass der Knoten mit demselben Intervall ausgewertet wird, das für die Knotenklassifizierung mit dem Befehl SET STATUSATRISKINTERVAL angegeben wurde. 'Übergangen' gibt an, dass der Gefährdungsstatus für den Knoten nicht vom Statusmonitor ausgewertet wird. 'Angepasst' gibt an, dass der Knoten mit dem Intervall ausgewertet wird, das mit dem Befehl SET VMATRISKINTERVAL angegeben wurde, und nicht mit dem Intervall, das mit dem Befehl SET STATUSATRISKINTERVAL angegeben wurde.

Gefährdungsintervall

Gibt die Zeit in Stunden zwischen Clientsicherungsaktivitäten an, bevor der Statusmonitor den Client als gefährdet ansieht. Dieses Feld gilt nur, wenn der Typ für Gefährdung 'Angepasst' ist.

Stillgelegt

Gibt an, ob die virtuelle Maschine, die der Dateibereich darstellt, stillgelegt ist.

Datum der Stilllegung

Gibt das Datum an, an dem die virtuelle Maschine, die der Dateibereich darstellt, stillgelegt wurde.

MAC-Adresse

Gibt die MAC-Adresse (MAC = Media Access Control) der Dateibereiche an, die für virtuelle VMware-Maschinen gesichert werden. Wenn die virtuelle Maschine über mehrere MAC-Adressen verfügt, ist dies die Adresse mit dem niedrigsten Wert.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY FILESPACE

| Befehl                  | Beschreibung   |
|-------------------------|--|
| DEFINE VIRTUALFSMAPPING | Zuordnung eines virtuellen Dateibereichs definieren.   |
| DELETE FILESPACE        | Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt. |
| REGISTER NODE           | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.  |
| REMOVE NODE             | Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.   |
| RENAME FILESPACE        | Vergibt einen neuen Namen für einen Clientdateibereich auf dem Server.   |
| UPDATE FILESPACE        | Ändert Knotenreplikationsregeln für Dateibereiche.   |
| UPDATE NODE             | Ändert die Attribute, die einem Clientknoten zugeordnet sind.  |

## QUERY LIBRARY (Kassettenarchiv abfragen)

Mit diesem Befehl können Informationen über Kassettenarchive angezeigt werden.

## Berechtigungsklasse

---

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

---

```

      .-*-----
>>-Query LIBRARY-----+----->
      '-Kassettenarchivname-'

      .-Format-----Standard-----
>-----+-----><
      '-Format-----+Standard+-'
      '-Detailed-'

```

## Parameter

---

### Kassettenarchivname

Gibt den Namen des Kassettenarchivs an, das abgefragt werden soll. Es können Platzhalterzeichen verwendet werden, um Namen anzugeben. Dieser Parameter ist wahlfrei.

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

#### Standard

Gibt an, dass Teilinformationen für das Kassettenarchiv angezeigt werden.

#### Detailed

Gibt an, dass die gesamten Informationen für das Kassettenarchiv angezeigt werden.

## Beispiel: Übersichtsdaten zu einem bestimmten Kassettenarchiv anzeigen

---

Informationen über das Kassettenarchiv AUTO anzeigen. Den folgenden Befehl ausgeben:

```

query library auto


      Kassettenarchivname: AUTO
      Kassettenarchivtyp: SCSI
      ACS-ID:
      Private Kategorie:
      Arbeitsdatenträgerkategorie:
      WORM-Arbeitsdatenträgerkategorie:
      Externer Manager:
      Gemeinsam benutzt: No
      LAN-unabhängig:
      Ladeverzögerung beachten:

```

Für Feldbeschreibungen siehe Feldbeschreibungen.

## Beispiel: Ausführliche Informationen zu einem bestimmten Kassettenarchiv anzeigen

---

Ausführliche Informationen über das Kassettenarchiv EZLIFE anzeigen. Den folgenden Befehl ausgeben:  AIX-Betriebssysteme

 Linux-Betriebssysteme

```
query library ezlife format=detailed
```

 AIX-Betriebssysteme

 Linux-Betriebssysteme

```

      Kassettenarchivname: EZLIFE
      Kassettenarchivtyp: SCSI
      ACS-ID:
      Private Kategorie:
      Arbeitsdatenträgerkategorie:
      WORM-Arbeitsdatenträgerkategorie:
      Externer Manager:
      Gemeinsam benutzt: Yes
      LAN-unabhängig:
      Ladeverzögerung beachten:
      Primärer Kassettenarchivmanager: EZSERVER
      WWN:
      Seriennummer:
      Automatisch kennzeichnen: OVERWRITE

```



Arbeitsdatenträger mit einem neuen Kennsatz versehen: Yes  
Letzte Aktualisierung durch (Administrator): DOCTOR\_MIKE  
Datum/Zeit der letzten Aktualisierung: 2002-12-05 15:24:53

## Windows-Betriebssysteme

```
Kassettenarchivname: EZLIFE
      Kassettenarchivtyp: SCSI
      ACS-ID:
      Private Kategorie:
      Arbeitsdatenträgerkategorie:
WORM-Arbeitsdatenträgerkategorie:
      Externer Manager:
      Gemeinsam benutzt: YES
      LAN-unabhängig:
      Ladeverzögerung beachten:
      Primärer Kassettenarchivmanager: EZSERVER
      WWN:
      Seriennummer:
      Automatisch kennzeichnen: OVERWRITE
      Laufwerke zurücksetzen: No
Arbeitsdatenträger mit einem neuen Kennsatz versehen: Yes
Letzte Aktualisierung durch (Administrator): DOCTOR_MIKE
Datum/Zeit der letzten Aktualisierung: 2000-12-05 15:24:53
```

Für Felddesreibungen siehe Felddesreibungen.

## Felddesreibungen

---

### Kassettenarchivname

Der Name des Kassettenarchivs.

### Kassettenarchivtyp

Der Typ des Kassettenarchivs.

### ACS-ID

Gibt an, dass es sich bei dem Kassettenarchiv um ein StorageTek-Kassettenarchiv handelt, das durch StorageTek Automated Cartridge System Library Software (ACSL) gesteuert wird.

### Private Kategorie

Die Kategorienummer für private Datenträger, die nach Namen geladen werden müssen.

Die Informationen, die in diesem Feld angezeigt werden, gelten nur für einen IBM® 3494 oder 3495 Tape Library Dataserver.

### Arbeitsdatenträgerkategorie

Die Kategorienummer, die für Arbeitsdatenträger in dem Kassettenarchiv verwendet werden soll.

Die Informationen, die in diesem Feld angezeigt werden, gelten nur für einen IBM 3494 oder 3495 Tape Library Dataserver.

### WORM-Arbeitsdatenträgerkategorie

Die Kategorienummer, die für WORM-Arbeitsdatenträger in dem Kassettenarchiv verwendet wird.

Die Informationen, die in diesem Feld angezeigt werden, gelten nur für einen IBM 3494 oder 3495 Tape Library Dataserver.

### Externer Manager

Der Standort des externen Kassettenarchivmanagers, an den der Server Zugriffsanforderungen für Datenträger senden kann.

### Gemeinsam benutzt

Gibt an, ob dieses Kassettenarchiv mit anderen IBM Spectrum Protect-Servern in einem Speicherbereichsnetz (Storage Area Network = SAN) gemeinsam benutzt wird.

### LAN-unabhängig

Gibt an, ob ein externes Kassettenarchiv für LAN-unabhängige Operationen verwendet wird.

### Ladeverzögerung beachten

Gibt an, ob der Server den Wert verwendet, der für Ladeverzögerung in der Einheitenklasse definiert ist, die diesem externen Kassettenarchiv zugeordnet ist.

### Primärer Kassettenarchivmanager

Der Name des Servers, der für die Steuerung des Zugriffs auf Kassettenarchivressourcen zuständig ist.

### WWN



Der weltweit verwendete Fibre Channel-Name für das Kassettenarchiv.


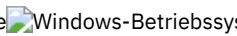
### Seriennummer

Gibt die Seriennummer des Kassettenarchivs an, das abgefragt wird.

### Automatisch kennzeichnen

Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen.

 AIX-Betriebssysteme  Windows-Betriebssysteme Laufwerke zurücksetzen

  Gibt an, ob der Server das Ziel zurücksetzt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird.

Arbeitsdatenträger mit einem neuen Kennsatz versehen

Gibt an, ob der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht wurden und wieder als Arbeitsdatenträger verwendet werden.

Letzte Aktualisierung durch (Administrator)

Gibt an, wer die letzte Aktualisierung des Kassettenarchivs ausgeführt hat.

Datum/Zeit der letzten Aktualisierung

Das Datum und die Uhrzeit der letzten Aktualisierung.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY LIBRARY

| Befehl         | Beschreibung  |
|----------------|---|
| AUDIT LIBRARY  | Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet. |
| DEFINE LIBRARY | Definiert ein automatisiertes oder manuelles Kassettenarchiv.                                       |
| DEFINE PATH    | Definiert einen Pfad von einer Quelle zu einem Ziel.  |
| DELETE LIBRARY | Löscht ein Kassettenarchiv.   |
| QUERY PATH     | Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.                                     |
| UPDATE LIBRARY | Ändert die Attribute eines Kassettenarchivs.  |

## QUERY LIBVOLUME (Datenträger im Kassettenarchiv abfragen)

Mit diesem Befehl können Informationen über einen oder mehrere Datenträger angezeigt werden, die in ein automatisiertes Kassettenarchiv zurückgestellt werden, damit sie vom IBM Spectrum Protect-Server verwendet werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

>>-Query LIBVolume--+-*-----+----->
                        '-Kassettenarchivname-'

.-*-----.-Format----Standard----.
>--+-----+-----+-----<
  '-Datenträgername-' '-Format----+Standard-+'
                        '-Detailed-'

```

### Parameter

**Kassettenarchivname**

Gibt den Namen des Kassettenarchivs an. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Kassettenarchive.

**Datenträgername**

Gibt den Datenträgernamen an. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Datenträger.

**Format**

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

**Standard**

Gibt an, dass Teilinformationen angezeigt werden.

**Detailed**

Gibt an, dass die gesamten Informationen angezeigt werden.

### Beispiel: Zurückgestellte Datenträger für ein bestimmtes Kassettenarchiv auflisten

Informationen über alle Datenträger anzeigen, die in das Kassettenarchiv TAPE zurückgestellt werden. Für Felddesreibungen siehe Felddesreibungen.

```
query libvolume tape
```

| Kassetten-<br>archivname | Datenträger-<br>name | Status  | Eigner | Letzte<br>Verwendung | Ausgangs-<br>element | Einheiten-<br>typ |
|--------------------------|----------------------|---------|--------|----------------------|----------------------|-------------------|
| TAPE                     | 000114               | Scratch |        |                      | 1,000                | LTO               |
| TAPE                     | NY1602               | Scratch |        |                      | 1,001                | DLT               |

## Beispiel: Ausführliche Informationen zu einem bestimmten Kassettenarchiv anzeigen

Ausführliche Informationen zu dem Datenträger JJY008 anzeigen. Für Felddesreibungen siehe Felddesreibungen.

```
query libvolume jjy008 format=detailed
```

```

Kassettenarchivname: HPW3494
Datenträgername: JJY008
Status: Private
Eigner: SUNSET
Letzte Verwendung: Data
Ausgangselement:
Einheitentyp:
Verbleibende Reinigungen:
Datenträgertyp:
    
```

## Felddesreibungen

### Kassettenarchivname

Der Name des Kassettenarchivs, in dem sich der Speicherdatenträger befindet.

### Datenträgername

Der Name des Speicherdatenträgers.

### Status

Der Status des Speicherdatenträgers laut Datenträgerbestand im Kassettenarchiv. Lautet der Status 'Private', wird der Datenträger von IBM Spectrum Protect verwendet. Lautet der Status 'Scratch', steht der Datenträger für andere Benutzer zur Verfügung.

### Owner

Der Eignerserver des Datenträgers, wenn der Datenträger den Status 'Private' hat.

### Letzte Verwendung

Der Typ der Daten auf dem Datenträger. Dieses Feld gilt nur für Datenträger im Status 'Private'. Für Speicherpooldatenträger zeigt dieses Feld **Data**. Für Datenbanksicherungsdatenträger (Gesamt-, Teil- oder Momentaufnahmesicherung) zeigt dieses Feld **DbBackup**.

### Ausgangselement

Die Elementadresse des Kassettenarchivschrachts, der den Datenträger enthält.

### Einheitentyp

Der Typ der Einheit, auf der der Datenträger verwendet wird. Dieses Feld zeigt einen Wert nur für Datenträger an, die in ein Kassettenarchiv zurückgestellt wurden, das gemischte Datenträger verwenden kann.

### Verbleibende Reinigungen

Für Reinigungskassetten die Anzahl der verbleibenden Reinigungen.

### Datenträgertyp

Der Typ des Datenträgers (z. B. 8-mm-Band).

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY LIBVOLUME

| Befehl             | Beschreibung  |
|--------------------|---|
| AUDIT LIBRARY      | Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet. |
| CHECKIN LIBVOLUME  | Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.                            |
| CHECKOUT LIBVOLUME | Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.                          |

| Befehl           | Beschreibung   |
|------------------|--|
| DEFINE VOLUME    | Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll. |
| LABEL LIBVOLUME  | Kennzeichnet Datenträger in manuellen oder automatisierten Kassettenarchiven.                                  |
| QUERY LIBRARY    | Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.  |
| UPDATE LIBVOLUME | Ändert den Status eines Speicherdatenträgers.  |

## QUERY LICENSE (Lizenzinformationen anzeigen)

Mit diesem Befehl können Informationen über die Lizenzprüfung, die Lizenzbedingungen und ihre Einhaltung angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query LICense-----><
```

### Parameter

Keine.

Um die Lizenzinformationen anzuzeigen, geben Sie den folgenden Befehl aus:

```
query license
```

Die folgende Beispielausgabe wird angezeigt:

```
ANR2017I Administrator SERVER_CONSOLE hat folgenden Befehl ausgegeben: QUERY LICENSE
                          Letzte Lizenzprüfung: 10/17/2016 14:28:08
                          Anzahl Data Protection for Oracle im Gebrauch: 0
                          Anzahl Data Protection for Oracle im Testmodus: 0
Anzahl Data Protection for Microsoft SQL im Gebrauch: 0
                          Anzahl of Data Protection for Microsoft SQL im Testmodus: 0
                          Anzahl Data Protection for Microsoft Exchange im Gebrauch: 0
                          Anzahl Data Protection for MS Exchange im Testmodus: 0
                          Anzahl TDP for Lotus Notes in Gebrauch: 12
                          Anzahl TDP for Lotus Notes im Testmodus: 0
Anzahl Data Protection for Lotus Domino im Gebrauch: 0
                          Anzahl Data Protection for Lotus Domino im Testmodus: 0
                          Anzahl TDP for Informix in Gebrauch: 1
                          Anzahl TDP for Informix im Testmodus: 0
                          Anzahl TDP for SAP R/3 in Gebrauch: 0
                          Anzahl TDP for SAP R/3 im Testmodus: 0
                          Anzahl TDP for ESS in Gebrauch: 0
                          Anzahl TDP for ESS im Testmodus: 0
                          Anzahl TDP for ESS R/3 in Gebrauch: 0
                          Anzahl TDP for ESS R/3 im Testmodus: 0
                          Anzahl TDP for EMC Symmetrix in Gebrauch: 0
                          Anzahl TDP for EMC Symmetrix im Testmodus: 0
                          Anzahl TDP for EMC Symmetrix R/3 in Gebrauch: 6
                          Anzahl TDP for EMC Symmetrix R/3 im Testmodus: 0
                          Anzahl TDP for WAS in Gebrauch: 0
                          Anzahl TDP for WAS im Testmodus: 0
Ist IBM Spectrum Protect for Data Retention im Gebrauch?: Nein
Ist IBM Spectrum Protect for Data Retention lizenziert?: Ja
  Ist IBM Spectrum Protect Basic Edition im Gebrauch?: Ja
  Ist IBM Spectrum Protect Basic Edition lizenziert?: Ja
Ist IBM Spectrum Protect Extended Edition im Gebrauch?: Nein
Ist IBM Spectrum Protect Extended Edition lizenziert?: Ja
                          Serverlizenzeinhaltung: Gültig
```

## Feldbeschreibungen

---

### Letzte Lizenzprüfung

Gibt an, wann die Lizenzprüfung zuletzt durchgeführt wurde (Datum und Uhrzeit).

### Anzahl Data Protection for Oracle im Gebrauch

Gibt die Anzahl der Instanzen von Data Protection for Oracle an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

### Anzahl Data Protection for Oracle im Testmodus

Gibt die Anzahl der Instanzen von Data Protection for Oracle an, die im Testmodus sind.

### Anzahl Data Protection for Microsoft SQL im Gebrauch

Gibt die Anzahl der Instanzen von Data Protection for Microsoft SQL an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

### Anzahl Data Protection for Microsoft SQL im Testmodus

Gibt die Anzahl der Instanzen von Data Protection for Microsoft SQL an, die im Testmodus sind.

### Anzahl Data Protection for Microsoft Exchange im Gebrauch

Gibt die Anzahl der Instanzen von Data Protection for Microsoft Exchange an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

### Anzahl Data Protection for Microsoft Exchange im Testmodus

Gibt die Anzahl der Instanzen von Data Protection for Microsoft Exchange an, die im Testmodus sind.

### Anzahl TDP for Lotus Notes in Gebrauch

Gibt die Anzahl von TDP for Lotus Notes an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

### Anzahl TDP for Lotus Notes im Testmodus

Gibt die Anzahl von TDP for Lotus Notes an, die im Testmodus sind.

### Anzahl Data Protection for Lotus Domino im Gebrauch

Gibt die Anzahl der Instanzen von Data Protection for Lotus Domino an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

### Anzahl Data Protection for Lotus Domino im Testmodus

Gibt die Anzahl der Instanzen von Data Protection for Lotus Domino an, die im Testmodus sind.

### Anzahl TDP for Informix in Gebrauch

Gibt die Anzahl von TDP for Informix an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

### Anzahl TDP for Informix im Testmodus

Gibt die Anzahl von TDP for Informix an, die im Testmodus sind.

### Anzahl TDP for SAP R/3 in Gebrauch

Gibt die Anzahl von TDP for SAP R/3 an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

### Anzahl TDP for SAP R/3 im Testmodus

Gibt die Anzahl von TDP for SAP R/3 an, die im Testmodus sind.

### Anzahl TDP for ESS in Gebrauch

Gibt die Anzahl von TDP for ESS an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

### Anzahl TDP for ESS im Testmodus

Gibt die Anzahl von TDP for ESS an, die im Testmodus sind.

### Anzahl TDP for ESS R/3 in Gebrauch

Gibt die Anzahl von TDP for ESS R/3 an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

### Anzahl TDP for ESS R/3 im Testmodus

Gibt die Anzahl von TDP for ESS R/3 an, die im Testmodus sind.

### Anzahl TDP for EMC Symmetrix in Gebrauch

Gibt die Anzahl von TDP for EMC Symmetrix an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

### Anzahl TDP for EMC Symmetrix im Testmodus

Gibt die Anzahl von TDP for EMC Symmetrix an, die im Testmodus sind.

### Anzahl TDP for EMC Symmetrix R/3 in Gebrauch

Gibt die Anzahl von TDP for EMC Symmetrix R/3 an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

### Anzahl TDP for EMC Symmetrix R/3 im Testmodus

Gibt die Anzahl von TDP for EMC Symmetrix R/3 an, die im Testmodus sind.

### Anzahl TDP for WAS in Gebrauch

Gibt die Anzahl von TDP for WAS an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

### Anzahl TDP for WAS im Testmodus

Gibt die Anzahl von TDP for WAS an, die im Testmodus sind.

Ist IBM Spectrum Protect for Data Retention im Gebrauch?

Gibt an, ob IBM Spectrum Protect for Data Retention im Gebrauch ist. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Ist IBM Spectrum Protect for Data Retention lizenziert?

Gibt an, ob IBM Spectrum Protect for Data Retention lizenziert ist.

Ist IBM Spectrum Protect Basic Edition im Gebrauch?

Gibt an, ob IBM Spectrum Protect Basic Edition im Gebrauch ist. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Ist IBM Spectrum Protect Basic Edition lizenziert?

Gibt an, ob IBM Spectrum Protect Basic Edition lizenziert ist.

Ist IBM Spectrum Protect Extended Edition im Gebrauch?

Gibt an, ob IBM Spectrum Protect Extended Edition im Gebrauch ist. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Ist IBM Spectrum Protect Extended Edition lizenziert?

Gibt an, ob IBM Spectrum Protect Extended Edition lizenziert ist.

Serverlizenzeinhaltung

Gibt an, ob die Serverlizenz gültig ist.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY LICENSE

| Befehl                 | Beschreibung   |
|------------------------|--|
| AUDIT LICENSES         | Prüft die Einhaltung der definierten Lizenzen.   |
| QUERY AUDITOCCUPANCY   | Zeigt die Serverspeicherauslastung für einen Clientknoten an.  |
| QUERY NODE             | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.  |
| QUERY PVUESTIMATE      | Zeigt Prozessor-Value-Unit-Schätzungen an.<br>Hinweis: Mit dem Befehl QUERY PVUESTIMATE werden Lizenzen zurückgemeldet, indem PVU-Informationen auf Knotenbasis für Servereinheiten bereitgestellt werden. |
| QUERY STATUS           | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.   |
| REGISTER LICENSE       | Registriert eine Lizenz für den IBM Spectrum Protect-Server.   |
| REGISTER NODE          | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.  |
| SET CPUINFOREFRESH     | Gibt die Anzahl der Tage zwischen Clientsuchläufen nach Workstationinformationen an, die für PVU-Schätzungen verwendet werden.   |
| SET LICENSEAUDITPERIOD | Gibt die Anzahl Tage zwischen den automatischen Lizenzprüfungen an.  |
| UPDATE NODE            | Ändert die Attribute, die einem Clientknoten zugeordnet sind.  |

## QUERY LOG (Informationen zum Wiederherstellungsprotokoll anzeigen)

Mit diesem Befehl können Informationen über das Wiederherstellungsprotokoll angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
.-Format----Standard----.
>>-Query LOG--+-----+-----<
'-Format----+Standard+-'
'-Detailed-'
```

## Parameter

---

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Die folgenden Werte sind gültig:

### Standard

Gibt an, dass Teilinformationen angezeigt werden.

### Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

## Beispiel: Übersichtsdaten zu dem Wiederherstellungsprotokoll anzeigen

---

Die Übersichtsdaten zu dem Wiederherstellungsprotokoll anzeigen. Für Felddescriptions siehe Felddescriptions.

```
query log
```

| Gesamtpeicherbereich (MB) | Verw. Speicherbereich (MB) | Freier Speicherbereich (MB) |
|---------------------------|----------------------------|-----------------------------|
| -----<br>38.912           | -----<br>543,3             | -----<br>38.368,7           |

## Beispiel: Ausführliche Informationen zu dem Wiederherstellungsprotokoll anzeigen

---

Ausführliche Informationen zu dem Wiederherstellungsprotokoll anzeigen. Für Felddescriptions siehe Felddescriptions.

```
query log format=detailed
```

```
Verzeichnis für aktive Protokolldateien: /actlog
Gesamtpeicherbereich (MB): 524.032
Verwendeter Speicherbereich (MB): 3.517
Freier Speicherbereich (MB): 520.515

Gesamtgröße des Dateisystems (MB): 564.443
Verwendeter Speicherbereich im Dateisystem (MB): 527.049
Freier Speicherbereich im Dateisystem (MB): 8.722

Verzeichnis für Archivprotokolle: /archlog
Gesamtgröße des Dateisystems (MB): 603.751,82
Verwendeter Speicherbereich im Dateisystem (MB): 80.642,30
Freier Speicherbereich im Dateisystem (MB): 523.109,52
Archivprotokoll komprimiert: Ja

Spiegelprotokollverzeichnis: /mirrorlog
Gesamtgröße des Dateisystems (MB): 564.443
Verwendeter Speicherbereich im Dateisystem (MB): 527.049
Freier Speicherbereich im Dateisystem (MB): 8.722

Übernahmeverzeichnis für Archivprotokolle: /archfaillog
Gesamtgröße des Dateisystems (MB): 301.372,06
Verwendeter Speicherbereich im Dateisystem (MB): 44.741,80
Freier Speicherbereich im Dateisystem (MB): 256.630,26
```



## Beispiel: Ausführliche Informationen zu dem Wiederherstellungsprotokoll anzeigen, wenn das Spiegelprotokoll und das Archivübernahmeprotokoll nicht definiert sind

---

Die Ausgabe dieses Befehls auf Windows-Systemen hat ein anderes Aussehen. Beispielsweise enthält die Ausgabe Leerzeichen für das Spiegelprotokoll und das Archivübernahmeprotokoll.

Informationen zu dem Wiederherstellungsprotokoll anzeigen, wenn das Spiegelprotokoll und das Archivübernahmeprotokoll nicht definiert sind.

```
query log format=detailed
```



```
Verzeichnis für aktive Protokolldateien: d:\actlog
Gesamtpeicherbereich (MB): 524.032
```

```

Verwendeter Speicherbereich (MB) : 3.517
Freier Speicherbereich (MB) : 520.515

Gesamtgröße des Dateisystems (MB) : 564.443
Verwendeter Speicherbereich im Dateisystem (MB) : 527.049
Freier Speicherbereich im Dateisystem (MB) : 8.722

Verzeichnis für Archivprotokolle: e:\archlog
Gesamtgröße des Dateisystems (MB) : 603.751,82
Verwendeter Speicherbereich im Dateisystem (MB) : 80.642,30
Freier Speicherbereich im Dateisystem (MB) : 523.109,52
Archivprotokoll komprimiert: Ja

Spiegelprotokollverzeichnis:
Gesamtgröße des Dateisystems (MB) :
Verwendeter Speicherbereich im Dateisystem (MB) :
Freier Speicherbereich im Dateisystem (MB) :

Übernahmeverzeichnis für Archivprotokolle:
Gesamtgröße des Dateisystems (MB) :
Verwendeter Speicherbereich im Dateisystem (MB) :
Freier Speicherbereich im Dateisystem (MB) :

```

## Feldbeschreibungen

---

### Gesamtspeicherbereich

Gibt die maximale Größe der aktiven Protokolldatei in Megabyte an.

### Verwendeter Speicherbereich

Gibt den verwendeten Speicherbereich (in MB) für aktive Protokolldateien an.

### Freier Speicherbereich

Gibt den Speicherbereich (in MB) für aktive Protokolldateien an, der nicht von nicht festgeschriebenen Transaktionen verwendet wird.

### Gesamtgröße des Dateisystems

Gibt die Gesamtgröße des Dateisystems in Megabyte an.

### Verwendeter Speicherbereich im Dateisystem

Gibt den verwendeten Speicherbereich im Dateisystem in Megabyte an.

### Freier Speicherbereich im Dateisystem

Gibt den Speicherbereich in Megabyte an, der im Dateisystem verfügbar ist.

### Archivprotokoll komprimiert

Gibt an, ob die Archivprotokolle komprimiert sind.

### Verzeichnis für aktive Protokolldateien

Gibt die Position an, an der aktive Protokolldateien gespeichert werden. Wird das Verzeichnis für aktive Protokolldateien geändert, versetzt der Server alle archivierten Protokolle in das Verzeichnis für Archivprotokolle und alle aktiven Protokolldateien in ein neues Verzeichnis für aktive Protokolldateien.

### Spiegelprotokollverzeichnis

Gibt die Position an, an der der Spiegel der aktiven Protokolldatei aufbewahrt wird.

### Übernahmeverzeichnis für Archivprotokolle

Gibt die Position an, an der der Server Archivprotokolle sichert, wenn die Protokolle nicht im Verzeichnis für Archivprotokolle archiviert werden können.

### Verzeichnis für Archivprotokolle

Gibt die Position an, an der der Server eine Protokolldatei archivieren kann, nachdem alle in dieser Protokolldatei angegebenen Transaktionen abgeschlossen wurden.

## QUERY MACHINE (Maschineninformationen abfragen)

---

Mit diesem Befehl können Informationen über eine oder mehrere Maschinen angezeigt werden. Mit Hilfe dieser Informationen können IBM Spectrum Protect-Client-Maschinen bei einem schwerwiegenden Fehler wiederhergestellt werden.

Achtung: Die Informationen werden von IBM Spectrum Protect nicht verwendet. Sie dienen nur zur Planung der Fehlerbehebung bei Client-Maschinen.

IBM Spectrum Protect zeigt Informationen für mehrere Maschinen in der folgenden Reihenfolge an:

- Entsprechend der angegebenen Priorität.
- Innerhalb einer Priorität, entsprechend dem angegebenen Standort und Maschinennamen.

## Berechtigungsklasse

---

Jeder Administrator kann diesen Befehl ausgeben.



## Syntax

```
.-*-----.  
>>-Query MACHine----->  
      '-Maschinename-' '-BUilding-----Gebäude-'  
  
>----->  
      '-FLoor-----Stockwerk-' '-ROom-----Raum-'  
  
>----->  
      '-PRIority-----Priorität-' '-ADSMServer-----Yes--+'  
                                      '-No--'  
  
.Format-----Standard-----.  
>-----><  
      '-Format-----+Standard-----+'  
                          '+Detailed-----+'  
                          '+RECOVERYInstructions-+'  
                          '-CHaracteristics-----'
```

## Parameter

### Maschinename

Gibt den Namen einer oder mehrerer Maschinen an, die abgefragt werden sollen. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert umfaßt alle Maschinen, die die angegebenen Kriterien erfüllen.

### BUilding

Gibt den Namen oder die Nummer des Gebäudes an, in dem sich die Maschinen befinden. Dieser Parameter ist wahlfrei. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

### FLoor

Gibt den Namen oder die Nummer des Stockwerks an, auf dem sich die Maschinen befinden. Dieser Parameter ist wahlfrei. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

### ROom

Gibt den Namen oder die Nummer des Raums an, in dem sich die Maschinen befinden. Dieser Parameter ist wahlfrei. Der Text kann bis zu 16 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

### PRIority

Gibt die Prioritätsnummer der Maschinen an. Dieser Parameter ist wahlfrei.

### ADSMServer

Gibt an, ob die Maschine einen IBM Spectrum Protect-Server enthält. Dieser Parameter ist wahlfrei. Standardmäßig werden alle Maschinen angezeigt, die die anderen Kriterien erfüllen. Gültige Werte:

#### Yes

Die Maschine enthält einen IBM Spectrum Protect-Server.

#### No

Die Maschinen enthalten keinen IBM Spectrum Protect-Server.

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

#### Standard

Zeigt Teilinformationen für die Maschinen an.

#### Detailed

Zeigt alle Informationen für die Maschinen an.

#### RECOVERYInstructions

Zeigt nur Wiederherstellungsanweisungen für die Maschine an. Diese Option ist nur gültig, wenn eine bestimmte Maschine abgefragt wird.

#### CHaracteristics

Zeigt nur Maschinenkenndaten an. Diese Option ist nur gültig, wenn eine bestimmte Maschine abgefragt wird.

## Beispiel: Informationen zu einer bestimmten Maschine anzeigen

Informationen für die Maschine MACH1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query machine MACH1
```

| Maschi-  | Maschinen- | Gebäude | Stock- | Raum | Knotenname | Wiederherstellungs- |
|----------|------------|---------|--------|------|------------|---------------------|
| nennname | priorität  |         | werk   |      |            | datenträgername     |

-----  
MACH1            1            21            2            2929 VIRGINIA            RECMED1  
-----

## Beispiel: Ausführliche Informationen zu Maschinen mit Priorität 1 anzeigen

Ausführliche Informationen über alle Maschinen mit der Priorität 1 anzeigen, die sich im zweiten Stockwerk des Gebäudes 21 befinden. Für Felddescriptions siehe Felddescriptions.

```
query machine * building=21 floor=2 priority=1  
format=detailed
```

```
                  Maschinenname: MACH1  
          Maschinenpriorität: 1  
                  Gebäude: 21  
                  Stockwerk: 2  
                  Raum: 2929  
                  Server?: Yes  
          Beschreibung: TSM-Server-Maschine  
                  Knotenname: VIRGINIA  
Wiederherstellungsdatenträgername: RECMED1  
                  Kenndaten?: Yes  
          Wiederherstellungsanweisungen?: Yes
```

## Felddescriptions

### Maschinenname

Der Name der Maschine.

### Maschinenpriorität

Die Wiederherstellungspriorität der Maschine.

### Gebäude

Das Gebäude, in dem sich die Maschine befindet.

### Stockwerk

Das Stockwerk, auf dem sich die Maschine befindet.

### Raum

Der Raum, in dem sich die Maschine befindet.

### Server?

Angabe, ob die Maschine einen IBM Spectrum Protect-Server enthält.

### Beschreibung

Eine Beschreibung der Maschine.

### Knotenname

Die IBM Spectrum Protect-Client-Knoten, die dieser Maschine zugeordnet sind.

### Wiederherstellungsdatenträgername

Die Wiederherstellungsdatenträger, die dieser Maschine zugeordnet sind.

### Kenndaten?

Angabe, ob die Kenndaten der Maschine in der Datenbank gespeichert sind.

### Wiederherstellungsanweisungen?

Gibt an, ob Wiederherstellungsanweisungen für eine Maschine in der IBM Spectrum Protect-Datenbank gespeichert sind.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY MACHINE

| Befehl                       | Beschreibung  |
|------------------------------|---|
| DEFINE MACHINE               | Definiert eine Maschine für DRM.  |
| DEFINE MACHNODEASSOCIATION   | Ordnet einen IBM Spectrum Protect-Knoten einer Maschine zu.   |
| DEFINE RECMEDMACHASSOCIATION | Ordnet Wiederherstellungsdatenträger einer Maschine zu.   |
| DELETE MACHINE               | Löscht eine Maschine.   |
| INSERT MACHINE               | Fügt Maschinenkenndaten oder Wiederherstellungsanweisungen in die IBM Spectrum Protect-Datenbank ein. |
| UPDATE MACHINE               | Ändert die Informationen zu einer Maschine.   |

## QUERY MEDIA (Speicherpoolatenträger mit sequenziellem Zugriff abfragen)



Gibt an, dass die Ausgabe der Abfrage auf einen bestimmten Datenträgerstatus beschränkt werden soll. Dieser Parameter ist wahlfrei. Es können mehrere Status in einer Liste angegeben werden, indem jeder Status ohne Leerzeichen durch ein Komma voneinander getrennt wird. Wird für diesen Parameter kein Wert angegeben, werden alle Datenträger in dem angegebenen Speicherpool unabhängig von ihrem Status angezeigt.

Gültige Werte:

FULL

Gibt an, dass Datenträger mit dem Status FULL angezeigt werden.

FILLing

Gibt an, dass Datenträger mit dem Status FILLING angezeigt werden.

EMPTy

Gibt an, dass Datenträger mit dem Status EMPTY angezeigt werden.

WHEREACcEss

Gibt an, dass die Ausgabe auf bestimmte Datenträgerzugriffsmodi beschränkt werden soll. Dieser Parameter ist wahlfrei. Wird kein Wert für diesen Parameter angegeben, wird die Ausgabe nicht auf bestimmte Zugriffsmodi beschränkt.

Gültige Werte:

READWrite

Gibt an, dass Datenträger mit dem Zugriffsmodus READWRITE angezeigt werden.

READOnly

Gibt an, dass Datenträger mit dem Zugriffsmodus READONLY angezeigt werden.

Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

Standard

Gibt an, dass Teilinformationen für die angegebenen Datenträger mit sequenziellem Zugriff aus dem Speicherpool angezeigt werden.

Detailed

Gibt an, dass die gesamten Informationen für die angegebenen Datenträger mit sequenziellem Zugriff aus dem Speicherpool angezeigt werden.

Cmd

Gibt an, dass ausführbare Befehle für die Speicherpooldatenträger erstellt werden, die von dem Befehl QUERY MEDIA verarbeitet werden. Diese Befehle befinden sich in der Datei, die mit dem Parameter CMDFILENAME des Befehls QUERY MEDIA angegeben wird. Sollen die Befehle nur an der Konsole angezeigt werden, geben Sie eine Nullzeichenfolge ("" ) für den Parameter CMDFILENAME an. Wenn FORMAT=CMD, aber keine Befehlsfolge im Parameter CMD angegeben wird, schlägt der Befehl QUERY MEDIA fehl.

WHEREState

Gibt den Status der zu verarbeitenden Datenträger an. Mit diesem Parameter wird die Verarbeitung auf Datenträger beschränkt, die den angegebenen Status haben. Dieser Parameter ist wahlfrei. Standardwert ist ALL. Gültige Werte:

All

Gibt an, dass Datenträger mit jedem Status abgefragt werden. Gültige Statusangaben sind MOUNTABLEINLIB und MOUNTABLENOTINLIB.

MOUNTABLEInlib

Gibt an, dass Datenträger abgefragt werden, die momentan den Status MOUNTABLEINLIB haben. Datenträger mit dem Status MOUNTABLEINLIB befinden sich im Kassettenarchiv, sind vor Ort, enthalten gültige Daten und stehen für die Verarbeitung vor Ort zur Verfügung.

MOUNTABLENotinlib

Gibt an, dass Datenträger abgefragt werden, die momentan den Status MOUNTABLENOTINLIB haben. Datenträger mit dem Status MOUNTABLENOTINLIB befinden sich nicht im Kassettenarchiv, enthalten keine gültigen Daten und stehen für die Verarbeitung vor Ort nicht zur Verfügung.



WHEREOVFloCation

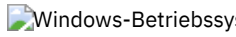
Gibt den Überlaufstandort der Datenträger an, die angezeigt werden sollen. Dieser Parameter ist wahlfrei. Mit diesem Parameter wird die Verarbeitung auf Datenträger beschränkt, die sich an dem angegebenen Standort befinden. Die maximale Länge des Standorts beträgt 255 Zeichen. Wenn der Standort Leerzeichen enthält, muss er in Anführungszeichen eingeschlossen werden.

CMd

Gibt an, dass ausführbare Befehle erstellt werden. Die Befehlsangabe in Anführungszeichen einschließen. Die maximale Länge der Befehlsangabe beträgt 255 Zeichen. Dieser Parameter ist wahlfrei.

Für jeden Datenträger, den der Befehl QUERY MEDIA erfolgreich verarbeitet hat, schreibt der Server die zugeordneten Befehle in eine Datei. Den Dateinamen mit dem Parameter CMDFILENAME angeben.

  Wird kein Dateiname angegeben, generiert der Befehl einen Standarddateinamen, indem die Zeichenfolge `exec.cmds.media` an das Serververzeichnis angehängt wird.

 Wird kein Dateiname angegeben, generiert der Befehl einen Standarddateinamen, indem die Zeichenfolge `exec.cmd.media` an das Serververzeichnis angehängt wird.

Hinweis:

1. Wenn der Befehl, der in die Datei geschrieben wird, 255 Zeichen überschreitet, wird er in mehrere Zeilen aufgeteilt, und an das Ende jeder Zeile (mit Ausnahme der letzten Zeile) wird ein Fortsetzungszeichen (+) eingefügt. Das Fortsetzungszeichen muss möglicherweise entsprechend den Anforderungen des Produkts, das die Befehle ausführt, geändert werden.
2. Wird ein ausführbarer Befehl mit einem anderen Wert als `CMD` für `FORMAT` angegeben, wird die Befehlszeichenfolge ignoriert, und der Befehl `QUERY MEDIA` schreibt keine Befehlszeile.

Geben Sie eine Befehlszeichenfolge und Substitutionsvariablen an:

#### Zeichenfolge

Gibt die Zeichenfolge an, mit der ein ausführbarer Befehl erstellt wird, um den Datenträgernamen und/oder Datenträgerstandort zu verarbeiten. Für die Zeichenfolge kann beliebiger Text im freien Format angegeben werden. Keine eingebetteten Anführungszeichen verwenden. Das folgende Beispiel zeigt eine gültige Angabe eines ausführbaren Befehls:

```
cmd="checkin libvolume &vol"
```

Die folgende Angabe ist ungültig:

```
cmd="checkin libvolume "&vol""
```

#### Substitution

Gibt eine Variable an, für die der Befehl `QUERY MEDIA` einen Wert ersetzen soll. Gültige Substitutionsvariablen:

##### &VOL

Den Datenträgernamen für `&VOL` ersetzen. Kleinbuchstaben können angegeben werden (`&vol`). Zwischen Et-Zeichen (`&`) und `VOL` dürfen keine Leerschritte oder Leerzeichen stehen. Befinden sich an dieser Stelle Leerzeichen, behandelt der Befehl `QUERY MEDIA` diese Zeichen als Zeichenfolge, und es wird keine Substitution definiert. Wird `&VOL` nicht angegeben, wird in dem ausführbaren Befehl kein Datenträgername definiert.

##### &LOC

Den Datenträgerstandort für `&LOC` ersetzen. Kleinbuchstaben können angegeben werden (`&loc`). Zwischen Et-Zeichen (`&`) und `LOC` dürfen keine Leerschritte oder Leerzeichen stehen. Befinden sich an dieser Stelle Leerzeichen, behandelt der Befehl `QUERY MEDIA` diese Zeichen als Zeichenfolge, und es wird keine Substitution definiert. Wird `&LOC` nicht angegeben, wird in dem ausführbaren Befehl kein Standortname definiert.

##### &VOLDSN


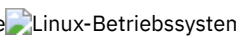
Den Datenträgerdateinamen für `&VOLDSN` ersetzen. Ein Beispiel für einen Dateinamen eines Banddatenträgers aus dem Kopierspeicherpool unter Verwendung des definierten Präfix `IBM Spectrum Protect310` lautet `IBM Spectrum Protect310.BFS`. Wird `&VOLDSN` nicht angegeben, wird in dem ausführbaren Befehl kein Datenträgerdateiname definiert.


##### &NL

Das Zeilenvorschubzeichen für `&NL` ersetzen. Wenn `&NL` angegeben wird, teilt der Befehl `QUERY MEDIA` den Befehl an der Position, an der sich `&NL` befindet; es werden keine Fortsetzungszeichen angehängt. Die Angabe des richtigen Fortsetzungszeichens (falls erforderlich) vor `&NL` ist Aufgabe des Benutzers. Der Benutzer ist außerdem verantwortlich für die Länge der Zeile. Wird `&NL` nicht angegeben und überschreitet der Befehl 255 Zeichen, wird der Befehl in mehrere Zeilen aufgeteilt, und an das Ende jeder Zeile (mit Ausnahme der letzten Zeile) wird ein Fortsetzungszeichen (+) eingefügt.



#### CMDFilename

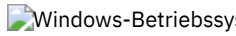
Gibt den vollständigen Pfadnamen an, der die durch `CMD` angegebenen Befehle enthalten wird, wenn `FORMAT=CMD` angegeben wird. Dieser Parameter ist wahlfrei. Die maximale Länge des Dateinamens beträgt 1279 Zeichen.

  Wird "" im Parameter `CMDFILENAME` angegeben, generiert der Befehl `QUERY MEDIA` einen Dateinamen, indem die Zeichenfolge `"exec.cmds.media"` an das Serververzeichnis angehängt wird. Das Serververzeichnis ist das aktuelle Arbeitsverzeichnis des Serverprozesses.

 Wird "" im Parameter `CMDFILENAME` angegeben, generiert der Befehl `QUERY MEDIA` einen Dateinamen, indem die Zeichenfolge `"exec.cmd.media"` an das Serververzeichnis angehängt wird. Das Serververzeichnis ist das aktuelle Arbeitsverzeichnis des Serverprozesses.

Wird für `CMDFILENAME` eine Nullzeichenfolge (""") angegeben, werden die erstellten Befehle nur an der Konsole angezeigt. Die angezeigten Befehle können mit den Umleitungszeichen des Betriebssystems (`>` oder `>>`) in eine Datei umgeleitet werden.

  Wird der Dateiname nicht angegeben, generiert der Befehl einen Standarddateinamen, indem die Zeichenfolge "exec.cmds.media" an das Serververzeichnis angehängt wird.

 Wird der Dateiname nicht angegeben, generiert der Befehl einen Standarddateinamen, indem die Zeichenfolge "exec.cmd.media" an das Serververzeichnis angehängt wird.

Der Befehl QUERY MEDIA ordnet den angegebenen oder generierten Dateinamen automatisch zu. Wenn der Dateiname vorhanden ist, versucht der Befehl QUERY MEDIA ihn zu verwenden, und die eventuell vorhandenen Daten in der Datei werden überschrieben. APPEND=YES kann angegeben werden, um zu verhindern, dass die vorhandenen Daten überschrieben werden. Schlägt der Befehl QUERY MEDIA fehl, nachdem die Befehlsdatei zugeordnet wurde, wird die Datei nicht gelöscht.

#### APPend

Gibt an, dass am Anfang oder Ende der Befehlsdateidaten geschrieben werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, dass die Daten an den Anfang der Befehlsdatei geschrieben werden sollen. Wenn die betreffende Befehlsdatei vorhanden ist, wird ihr Inhalt überschrieben.

Yes

Gibt an, dass die Befehlsdatei angehängt werden soll, indem am Ende der Befehlsdateidaten geschrieben wird.

## Beispiel: Informationen zu einem bestimmten Speicherpool mit sequenziellem Zugriff anzeigen

Alle vollen und teilweise vollen Datenträger anzeigen, die sich im primären Speicherpool mit sequenziellem Zugriff ARCHIVE befinden. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query media * stgpool=archive wherestatus=full, filling
```

| Daten-          | Status                | Standort        | Name des autom.<br>trägername |
|-----------------|-----------------------|-----------------|-------------------------------|
| Speicherarchivs |                       |                 |                               |
| -----           | -----                 | -----           | -----                         |
| TAPE01          | Mountable in Library  |                 | LIB3494                       |
| TAPE03          | Mountable not in Lib. | Room1234/Bldg31 |                               |
| TAPE07          | Mountable in Library  |                 | LIB3494                       |
| TAPE09          | Mountable not in Lib. | Room1234/Bldg31 |                               |

## Beispiel: Informationen zu einem Speicherpool mit sequenziellem Zugriff mit einem bestimmten Präfix anzeigen

Alle vollen Datenträger mit dem Status MOUNTABLENOTINLIB für Speicherpools mit sequenziellem Zugriff, die den Präfixnamen ONSITE haben, detailliert anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query media wherestate=mountablenotinlib stgpool=onsite*  
wherestatus=full format=detailed
```

```
          Datenträgername: TAPE21  
                Status: Mountable not in library  
          Datenträgerstatus: Full  
                Zugriff: ReadOnly  
          Letztes Referenzdatum: 01/30/98  
Datum/Zeit der letzten Aktualisierung: 08/20/1996 13:29:02  
                Standort: Rm569/bldg31  
          Speicherpoolname: ONSITE.ARCHIVE  
Name des automatisierten Kassettenarchivs:  
  
          Datenträgername: TAPE22  
                Status: Mountable not in library  
          Datenträgerstatus: Full  
                Zugriff: ReadOnly  
          Letztes Referenzdatum: 01/30/98  
Datum/Zeit der letzten Aktualisierung: 08/20/1996 15:29:02  
                Standort: Rm569/bldg31  
          Speicherpoolname: ONSITE.ARCHIVEPOOL  
Name des automatisierten Kassettenarchivs:
```

## Beispiel: Befehle zum Zurückstellen generieren

Die Befehle CHECKIN LIBVOLUME für volle und teilweise volle Datenträger generieren, die sich im primären Speicherpool ONSITE.ARCHIVE befinden und im Überlaufstandort Room 2948/Bldg31 aufbewahrt werden.

```
query media * stgpool=onsite.archive format=cmd
wherestatus=full,filling wherestate=mountablenotinlib
whereovflocation=room2948/bldg31
cmd="checkin libvol lib3494 &vol status=private"
cmdfilename=/tsm/move/media/checkin.vols
```

Der Befehl QUERY MEDIA hat die ausführbaren Befehle CHECKIN LIBVOLUME in /tsm/move/media/checkin.vols erstellt, die durch Ausgabe des Befehls MACRO mit /tsm/move/media/checkin.vols als Makronamen ausgeführt werden können.

```
checkin libvol lib3494 TAPE04 status=private
checkin libvol lib3494 TAPE13 status=private
checkin libvol lib3494 TAPE14 status=private
```

## Feldbeschreibungen

### Datenträgername

Gibt den Namen des Datenträgers aus dem primären Speicherpool mit sequenziellem Zugriff an.

### Status

Gibt den Status des Datenträgers an.

### Datenträgerstatus

Gibt den Status des Datenträgers an.

### Zugriff

Gibt den Zugriffsmodus des Datenträgers an.

### Letztes Referenzdatum

Gibt das letzte Lese- oder Schreibdatum (das aktuellere von beiden) des Datenträgers an.

### Datum/Zeit der letzten Aktualisierung

Gibt das Datum und die Uhrzeit an, an dem bzw. zu der der Datenträger zuletzt aktualisiert wurde.

### Standort

Gibt den Speicherort des Datenträgers an. Wenn der Datenträger aus dem Kassettenarchiv ausgegeben wurde und sein Speicherort nicht angegeben oder definiert ist, wird ein Fragezeichen (?) als Standort angezeigt.

### Speicherpoolname

Gibt den Namen des Speicherpools mit sequenziellem Zugriff an, in dem der Datenträger definiert ist.

### Automat. Kassettenarchiv

Gibt den Namen des automatisierten Kassettenarchivs an, wenn sich der Datenträger im Kassettenarchiv befindet.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY MEDIA

| Befehl   | Beschreibung  |
|--|---|
|    MOVE MEDIA | Versetzt Speicherpooldatenträger, die von einem automatisierten Kassettenarchiv verwaltet werden. |

## QUERY MGMTCLASS (Verwaltungsklasse abfragen)

Mit diesem Befehl können Informationen über Verwaltungsklassen angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query Mgmtclass----->
. * - * - * -----
>-+-----+----->
|          . * - * - * -----|
|'-Domänenname-----+-----|
|          |          . * - * - * -----|
|          |'-Name_der_Maßnahmengruppe-----+-----|
|          |          |          . * - * - * -----|
|          |          |          |'-Klassename-----|
```

```

.-Format-----Standard-----
>-----+-----><
'-Format-----+--Standard+--'
      '-Detailed-'

```

## Parameter

### Domänenname

Gibt die Maßnahmendomäne an, die der Verwaltungsklasse zugeordnet ist, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden Verwaltungsklassen in allen Maßnahmendomänen abgefragt. Dieser Parameter muß angegeben werden, wenn explizit der Name einer Verwaltungsklasse angegeben wird.

### Name\_der\_Maßnahmengruppe

Gibt die Maßnahmengruppe an, die der Verwaltungsklasse zugeordnet ist, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden Verwaltungsklassen in allen Maßnahmengruppen abgefragt. Dieser Parameter muß angegeben werden, wenn explizit der Name einer Verwaltungsklasse angegeben wird.

### Klassenname

Gibt die Verwaltungsklasse an, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Verwaltungsklassen abgefragt.

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

#### Standard

Gibt an, dass Teilinformationen angezeigt werden.

#### Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

## Beispiel: Informationen zu allen Verwaltungsklassen anzeigen

Alle Verwaltungsklassen für alle Maßnahmendomänen abfragen. Die Ausgabe soll im Standardformat erstellt werden. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query mgmtclass
```

| Name der<br>Maßnahmen-<br>domäne | Name der<br>Maßnahmen-<br>gruppe | Name<br>Verwal-<br>tungskl. | Standard<br>verwal-<br>tungskl.? | Beschreibung                          |
|----------------------------------|----------------------------------|-----------------------------|----------------------------------|---------------------------------------|
| EMPLOYEE-<br>_RECORDS            | ACTIVE                           | ACTIVEFI-<br>LES            | Yes                              | Modified default<br>management class  |
| EMPLOYEE-<br>_RECORDS            | HOLIDAY                          | ACTIVEFI-<br>LES            | Yes                              | Modified default<br>management class  |
| EMPLOYEE-<br>_RECORDS            | HOLIDAY                          | FILEHIST-<br>ORY            | No                               | Test modified<br>management class     |
| EMPLOYEE-<br>_RECORDS            | VACATION                         | ACTIVEFI-<br>LES            | Yes                              | Original default<br>management class  |
| EMPLOYEE-<br>_RECORDS            | VACATION                         | FILEHIST-<br>ORY            | No                               | Test modified<br>management class     |
| PROG1                            | SUMMER                           | MCLASS1                     | No                               | Technical Support<br>Mgmt Class       |
| PROG2                            | SUMMER                           | MCLASS1                     | No                               | Technical Support<br>Mgmt Class       |
| STANDARD                         | ACTIVE                           | STANDARD                    | Yes                              | Installed default<br>management class |
| STANDARD                         | STANDARD                         | STANDARD                    | Yes                              | Installed default<br>management class |

Um Informationen zu Verwaltungsklassen in einer bestimmten Maßnahmendomäne (z. B. in der Domäne ENGPOLDOM) anzuzeigen, geben Sie den folgenden Befehl aus:

```
query mgmtclass engpoldom * *
```

## Beispiel: Ausführliche Informationen zu einer bestimmten Verwaltungsklasse anzeigen

Die Verwaltungsklasse ACTIVEFILES abfragen, die der Maßnahmengruppe VACATION in der Maßnahmendomäne EMPLOYEE\_RECORDS zugeordnet ist. Die Ausgabe soll im ausführlichen Format erstellt werden. Für Feldbeschreibungen siehe Feldbeschreibungen.



```
query mgmtclass employee_records vacation
activefiles format=detailed
```

```

Name der Maßnahmendomäne: EMPLOYEE_RECORDS
Name der Maßnahmengruppe: VACATION
Name der Verwaltungsklasse: ACTIVEFILES
Standardverwaltungsklasse?: Yes
    Beschreibung: Inst. def. management class
Speicherverwaltungstechnik: None
Auto-Umlagerung bei Nichtbenutzung: 0
Sicherung vor Umlagerung erforderl.?: Yes
    Zielort für umgelagerte Dateien: SPACEMGPOOL
    Letzte Aktualisierung durch
        (Administrator): $$CONFIG_MANAGER$$
Datum/Zeit der letzten Aktualisierung: 05/31/1998 13:15:45
Verwaltendes Profil: EMPLOYEE
Änderungen anstehend: Yes

```

## Feldbeschreibungen

- Name der Maßnahmendomäne  
Die Maßnahmendomäne.
- Name der Maßnahmengruppe  
Die Maßnahmengruppe.
- Name der Verwaltungsklasse  
Die Verwaltungsklasse.
- Standardverwaltungsklasse?  
Angabe, ob die Verwaltungsklasse die Standardverwaltungsklasse für die Maßnahmengruppe ist.
- Beschreibung  
Die Beschreibung der Verwaltungsklasse.
- Speicherverwaltungstechnik  
Die Speicherverwaltungstechnik für die Verwaltungsklasse für IBM Spectrum Protect for Space Management-Clients.
- Auto-Umlagerung bei Nichtbenutzung  
Die Anzahl Tage, die nach dem letzten Zugriff auf eine Datei verstreichen müssen, bevor die Datei für die automatische Umlagerung durch IBM Spectrum Protect for Space Management-Clients ausgewählt werden kann.
- Sicherung vor Umlagerung erforderlich?  
Angabe, ob eine Sicherungsversion einer Datei vorhanden sein muss, bevor eine Datei durch IBM Spectrum Protect for Space Management-Clients umgelagert werden kann.
- Zielort für umgelagerte Dateien  
Der Speicherpool, der der Zielort für Dateien ist, die von IBM Spectrum Protect for Space Management-Clients umgelagert werden.
- Letzte Aktualisierung durch (Administrator)  
Der Administrator oder Server, der die Verwaltungsklasse zuletzt aktualisiert hat. Enthält dieses Feld \$\$CONFIG\_MANAGER\$\$, ist die Verwaltungsklasse einer Domäne zugeordnet, die von dem Konfigurationsmanager verwaltet wird.
- Datum/Zeit der letzten Aktualisierung  
Das Datum und die Uhrzeit, an dem bzw. zu der die Verwaltungsklasse definiert oder zuletzt aktualisiert wurde.
- Verwaltendes Profil  
Das Profil oder die Profile, für die der verwaltete Server subskribiert hat, um die Definition dieser Verwaltungsklasse zu erhalten.
- Änderungen anstehend  
Angabe, ob Änderungen vorgenommen, aber nicht aktiviert werden. Sobald die Änderungen aktiviert werden, wird das Feld auf No zurückgesetzt.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY MGMTCLASS

| Befehl                 | Beschreibung  |
|------------------------|---|
| COPY MGMTCLASS         | Erstellt eine Kopie einer Verwaltungsklasse.  |
| DEFINE MGMTCLASS       | Definiert eine Verwaltungsklasse.   |
| DEFINE PROFASSOCIATION | Ordnet Objekte einem Profil zu.   |
| DELETE MGMTCLASS       | Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe. |
| QUERY DOMAIN           | Zeigt Informationen über Maßnahmendomänen an.   |
| UPDATE MGMTCLASS       | Ändert die Attribute einer Verwaltungsklasse.   |

# QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)

---

Verwenden Sie diesen Befehl, um Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus anzuzeigen.

## Berechtigungsklasse

---

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

---

```
>>-Query MONITORSEttings-----<<
```

## Überwachungseinstellungen anzeigen

---

Ausführliche Informationen zu den Überwachungseinstellungen anzeigen. Ausführliche Informationen befinden sich in Feldbeschreibungen.

```
query monitorsettings
```

Beispielausgabe:

```

                Status überwachen: On
    Statusaktualisierungsintervall (Minuten): 5
                Statusbeibehaltung (Stunden): 48
                Nachrichtenalerts überwachen: On
    Alertaktualisierungsintervall (Minuten): 10
                Alert an E-Mail-Adresse: On
    Alertzusammenfassung an Administratoren senden: On
                Alert von E-Mail-Adresse: DJADMIN@MYDOMAIN.COM
                Alert-SMTP-Host: DJHOST.MYDOMAIN.COM
                Alert-SMTP-Anschluss: 25
                Dauer des Alertstatus 'aktiv' (Minuten): 480
                Dauer des Alertstatus 'inaktiv' (Minuten): 480
                Dauer des Alertstatus 'geschlossen' (Minuten): 60
                Überwachungsadministrator: ADMIN
                Überwachte Gruppe: MONGROUP
                Überwachte Server: SERVER2
                Gefährdungsintervall für Anwendungen: 24
    Übersprungene Dateien als Gefährdung für Anwendungen ansehen?: Yes
                Gefährdungsintervall für virtuelle Maschinen: 24
    Übersprungene Dateien als Gefährdung für virtuelle Maschinen ansehen?: Yes
                Gefährdungsintervall für Systeme: 24
    Übersprungene Dateien als Gefährdung für Systeme ansehen?: Yes
                Implementierungsrepository: /source/packages/deploy
                Maximale Anzahl Implementierungspakete: 4
    Implementierungspaketmanager: On
```

## Feldbeschreibungen

---

Status überwachen

Gibt an, ob die Alertüberwachung auf dem Server aktiviert oder inaktiviert ist.

Statusaktualisierungsintervall (Minuten)

Gibt die Anzahl Minuten zwischen Intervallen an, in denen der Überwachungsserver Ereignisdaten zusammenstellt.

Statusbeibehaltung (Stunden)

Gibt die Anzahl Stunden an, die Statusüberwachungsanzeiger beibehalten werden.

Nachrichtenalerts überwachen

Gibt an, ob Alerts in einer E-Mail an Administratoren gesendet werden.

Alertaktualisierungsintervall (Minuten)

Gibt die Zeit in Minuten an, die der Alertmonitor wartet, bevor der Alert auf dem Server aktualisiert und bereinigt wird.

Alert an E-Mail-Adresse

Gibt an, ob Alerts in einer E-Mail an Administratoren gesendet werden.

Alertzusammenfassung an Administratoren senden

Gibt die Administratoren an, die in einer E-Mail eine Zusammenfassung der vorhandenen Alerts auf dem Server empfangen.

Alert von E-Mail-Adresse

- Gibt die E-Mail-Adresse des Absenders an.
- Alert-SMTP-Host**  
Gibt den SMTP-Host-Mail-Server (SMTP = Simple Mail Transfer Protocol) an, der zum Senden von Alerts in einer E-Mail verwendet wird.
- Alert-SMTP-Anschluss**  
Gibt den Anschluss des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird.
- Dauer des Alertstatus 'aktiv' (Minuten)**  
Gibt die Zeit in Minuten an, die ein Alert aktiv bleibt.
- Dauer des Alertstatus 'inaktiv' (Minuten)**  
Gibt die Zeit in Minuten an, die ein Alert inaktiv bleibt.
- Dauer des Alertstatus 'geschlossen' (Minuten)**  
Gibt die Zeit in Minuten an, die ein Alert geschlossen bleibt, bevor der Alert auf dem Server gelöscht wird.
- Überwachungsadministrator**  
Gibt den Namen des Überwachungsadministrators an, der verwendet wird, um die Verbindung zu den Servern in der überwachten Gruppe herzustellen.
- Überwachte Gruppe**  
Gibt den Namen der überwachten Servergruppe an.
- Überwachte Server**  
Gibt die Namen der Server in der überwachten Servergruppe an. Die Überwachungseinstellungen können auf den überwachten Servern unterschiedlich sein. Ist dies der Fall, geben Sie für jeden Server den Abfragebefehl aus, um die Überwachungseinstellungen anzuzeigen.
- Gefährdungsintervall für Anwendungen**  
Gibt die Anzahl Stunden an, die ein Anwendungsclient keine Aktivität protokollieren kann, bevor er als gefährdet angesehen wird.
- Übersprungene Dateien als Gefährdung für Anwendungen ansehen?**  
Gibt an, dass der Server vom Client übersprungene Dateien als Fehler ansieht und den Client als gefährdet markiert.
- Gefährdungsintervall für virtuelle Maschinen**  
Gibt die Anzahl Stunden an, die ein virtueller Client keine Aktivität protokollieren kann, bevor er als gefährdet angesehen wird.
- Übersprungene Dateien als Gefährdung für virtuelle Maschinen ansehen?**  
Gibt an, dass der Server vom Client übersprungene Dateien als Fehler ansieht und den Client als gefährdet markiert.
- Gefährdungsintervall für Systeme**  
Gibt die Anzahl Stunden an, die ein Systemclient keine Aktivität protokollieren kann, bevor er als gefährdet angesehen wird.
- Übersprungene Dateien als Gefährdung für Systeme ansehen?**  
Gibt an, dass der Server vom Client übersprungene Dateien als Fehler ansieht und den Client als gefährdet markiert.
- Implementierungsrepository**  
Gibt die Position, an der Clientimplementierungspakete heruntergeladen werden, und die Position der Speicherdatenträger an, die für Clientimplementierungspakete verwendet werden.
- Maximale Anzahl Implementierungspakete**  
Gibt die maximale Anzahl Clientimplementierungspakete an, die im Implementierungsrepository für jede Produktversion gespeichert werden.
- Implementierungspaketmanager**  
Gibt an, ob der Implementierungspaketmanager die FTP-Site nach neuen Implementierungspaketen abfragt und neue Pakete herunterlädt, wenn sie verfügbar werden.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY MONITORSETTINGS

| Befehl  | Beschreibung  |
|---|---|
| DEFINE ALERTTRIGGER (Alertauslöser definieren)                                  | Ordnet angegebene Nachrichten einem Alertauslöser zu.                             |
| DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)               | Entfernt eine Nachrichtennummer, die einen Alert auslösen kann.                   |
| DELETE GRPMEMBER (Server aus einer Servergruppe löschen)                        | Löscht einen Server aus einer Servergruppe.                                       |
| DELETE SERVER (Server-Definition löschen)                                       | Löscht die Definition eines Servers.  |
| QUERY ALERTSTATUS (Status eines Alert abfragen)                                 | Zeigt Informationen zu Alerts an, die auf dem Server ausgegeben wurden.           |
| QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)               | Zeigt Nachrichtennummern an, die einen Alert auslösen.                            |
| SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)                    | Gibt an, ob die Alertüberwachung aktiviert oder inaktiviert ist.                  |
| SET DEPLOYREPOSITORY (Downloadpfad für Clientimplementierungspakete definieren) | Gibt die Position an, an der Clientimplementierungspakete heruntergeladen werden. |

| Befehl  | Beschreibung   |
|---|--|
| SET DEPLOYMAXPKGS (Maximale Anzahl Clientimplementierungspakete definieren, die gespeichert werden sollen)  | Gibt die maximale Anzahl Clientimplementierungspakete an, die heruntergeladen und auf dem Server gespeichert werden.         |
| SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)        | Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.         |
| SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)   | Gibt an, ob die Statusüberwachung aktiviert werden soll.   |
| SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll) | Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll. |
| UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)   | Aktualisiert die Attribute eines oder mehrerer Alertauslöser.  |
| UPDATE ALERTSTATUS (Status eines Alert aktualisieren)   | Aktualisiert den Status eines zurückgemeldeten Alert.  |

## QUERY MONITORSTATUS (Überwachungsstatus abfragen)

Mit diesem Befehl können Sie Überwachungsnachrichten anzeigen, die innerhalb des definierten Zeitraums für die Statusbeibehaltung liegen.

Sie können die Ausgabe auf einen angegebenen Status begrenzen, wie z. B. auf Nachrichten mit dem Status 'aktiv'. Werden keine Parameter angegeben, werden alle Nachrichten angezeigt.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

.-Format---Standard-----
>>-Query MONITORStatus-+-----+----->
      '-Format---Standard+-'
                        '-Detailed-'

.-Type---Active-----
>-+-----+----->
  '-Type---All-----'
      +-Active---+
      '-Inactive-'

>-+-----+----->
  '-Activity---Name der Aktivität-'

>-+-----+-----+-----+-----><
  '-Name---Elementname-' | | | | |
                        | | | | |
                        v | | | |
  '-Status---Normal---+---'
                        +-Warning-+
                        '-Error---'

```

### Parameter

#### Format

Gibt den Umfang der Informationen an, die angezeigt werden. Der Standardwert ist STANDARD. Geben Sie einen der folgenden Werte an:

#### Standard

Gibt an, dass nur Teilmeldungen für die angegebenen Nachrichten angezeigt werden.

#### Detailed

Gibt an, dass alle Informationen für die angegebenen Nachrichten angezeigt werden.

#### Type

Dieser Parameter begrenzt die Ausgabe auf Nachrichten mit dem angegebenen Wert für den Typ. Geben Sie einen der folgenden Werte an:

ALL

Zeigt alle Informationen an.

ACTIVE

Zeigt alle aktiven Nachrichten an. Dies ist der Standardwert.

INACTIVE

Zeigt alle inaktiven Nachrichten an.

ACTIVITY

Gibt die Aktivität an, die abgefragt werden soll. Die Beschreibung des Befehls DEFINE STATUSTHRESHOLD enthält ausführliche Informationen zu den verfügbaren Aktivitäten für die Abfrage.

NAME

Gibt den Namen an, der abgefragt werden soll. Der Wert für NAME bezieht sich auf den Namen des Elements mit der angegebenen Aktivität. Beispiel: Für einen Statusanzeiger, der Informationen zu einem Speicherpool mit dem Namen `backuppool` enthält, wird NAME auf `BACKUPPOOL` gesetzt.

STATUS

Gibt den Status der Nachrichten an, der abgefragt werden soll. Es können mehrere Statuswerte in einer Liste angegeben werden, indem die Werte ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird kein Wert für diesen Parameter angegeben, werden Informationen zu allen Statuswerten angezeigt. Geben Sie einen der folgenden Werte an:

Normal

Zeigt alle Nachrichten mit einem normalen Status an.

Warning

Zeigt alle Nachrichten mit einem Warnstatus an.

Error

Zeigt alle Nachrichten mit einem Fehlerstatus an.

## Überwachungseinstellungen anzeigen

---

Ausführliche Informationen zum Überwachungsstatus anzeigen.

```
Query MONITORStatus type=active
```

Beispielausgabe:

```
Servername: SERVER1
Datum der Aktivität: 05.03.2013 15:57:37
Name der Aktivität: Kapazität des primären Platten- und Dateispeichers
Elementname: Kapazität des primären Platten- und Dateispeichers
Numerischer Wert des Elements: 0
Zeichenfolgewart des Elements:
Elementstatus: NORMAL

Servername: SERVER1
Datum der Aktivität: 05.03.2013 15:57:37
Name der Aktivität: Verwendete Kapazität des primären Platten- und Dateispeichers
Elementname: Verwendete Kapazität des primären Platten- und Dateispeichers
Numerischer Wert des Elements: 0
Zeichenfolgewart des Elements:
Elementstatus: NORMAL

Servername: SERVER1
Datum der Aktivität: 05.03.2013 15:57:37
Name der Aktivität: Kapazität des primären Bandspeichers
Elementname: Kapazität des primären Bandspeichers
Numerischer Wert des Elements: 0
Zeichenfolgewart des Elements:
Elementstatus: NORMAL

Servername: SERVER1
Datum der Aktivität: 05.03.2013 15:57:37
Name der Aktivität: Verwendete Kapazität des primären Bandspeichers
Elementname: Verwendete Kapazität des primären Bandspeichers
Numerischer Wert des Elements: 0
Zeichenfolgewart des Elements:
Elementstatus: NORMAL
```

## Überwachungseinstellungen anzeigen

---

Ausführliche Informationen zum Überwachungsstatus anzeigen.

```
query monitorstatus f=d type=active
```

Beispielausgabe:

```
Servername: SERVER1
Datum der Aktivität: 05.03.2013 15:57:37
Name der Aktivität: Kapazität des primären Platten- und Dateispeichers
Elementname: Kapazität des primären Platten- und Dateispeichers
Numerischer Wert des Elements: 0
Zeichenfolgewart des Elements:
Elementstatus: NORMAL
Elementdetails:
Primärer Reparaturvorschlag:
Erster alternativer Reparaturvorschlag:
Zweiter alternativer Reparaturvorschlag:

Servername: SERVER1
Datum der Aktivität: 05.03.2013 15:57:37
Name der Aktivität: Verwendete Kapazität des primären Platten- und
Dateispeichers
Elementname: Verwendete Kapazität des primären Platten- und
Dateispeichers
Numerischer Wert des Elements: 0
Zeichenfolgewart des Elements:
Elementstatus: NORMAL
Elementdetails:
Primärer Reparaturvorschlag:
Erster alternativer Reparaturvorschlag:
Zweiter alternativer Reparaturvorschlag:

Servername: SERVER1
Datum der Aktivität: 05.03.2013 15:57:37
Name der Aktivität: Kapazität des primären Bandspeichers
Elementname: Kapazität des primären Bandspeichers
Numerischer Wert des Elements: 0
Zeichenfolgewart des Elements:
Elementstatus: NORMAL
Elementdetails:
Primärer Reparaturvorschlag:
Erster alternativer Reparaturvorschlag:
Zweiter alternativer Reparaturvorschlag:

Servername: SERVER1
Datum der Aktivität: 05.03.2013 15:57:37
Name der Aktivität: Verwendete Kapazität des primären Bandspeichers
Elementname: Verwendete Kapazität des primären Bandspeichers
Numerischer Wert des Elements: 0
Zeichenfolgewart des Elements:
Elementstatus: NORMAL
Elementdetails:
Primärer Reparaturvorschlag:
Erster alternativer Reparaturvorschlag:
Zweiter alternativer Reparaturvorschlag:
```

## Feldbeschreibungen

---

Servername  
Der Name des Servers.

Datum der Aktivität  
Gibt an, wann die Aktivität zuletzt zurückgemeldet wurde.

Name der Aktivität  
Der Name der Aktivität.

Elementname  
Der Name des Elements.

Numerischer Wert des Elements  
Der numerische Wert des Elements.

Zeichenfolgewart des Elements  
Der Zeichenfolgewart des Elements.

Elementstatus  
Der Status des Elements.

Elementdetails  
Die detaillierten Informationen des Elements.

Primärer Reparaturvorschlag

Der primäre Reparaturvorschlag.

Erster alternativer Reparaturvorschlag

Der zu befolgende Reparaturvorschlag, falls der primäre Vorschlag nicht geeignet ist.

Zweiter alternativer Reparaturvorschlag

Der zu befolgende Reparaturvorschlag, falls der primäre und der erste alternative Vorschlag nicht geeignet sind.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY MONITORSTATUS

| Befehl  | Beschreibung   |
|---|--|
| DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)   | Definiert einen Schwellenwert für die Statusüberwachung.   |
| DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)  | Löscht einen Schwellenwert für die Statusüberwachung.  |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)                                      | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                             |
| QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)   | Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.   |
| SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)        | Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.         |
| SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)   | Gibt an, ob die Statusüberwachung aktiviert werden soll.   |
| SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)   | Gibt das Aktualisierungsintervall für die Statusüberwachung an.  |
| SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll) | Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll. |
| UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)  | Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.   |

## QUERY MOUNT (Informationen zu bereitgestellten Datenträgern mit sequenziellem Zugriff anzeigen)

Mit diesem Befehl können Informationen zum Status eines oder mehrerer bereitgestellter Datenträger mit sequenziellem Zugriff angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
..*-----.  
>>-Query MOUNT-----+----->  
  '-Datenträgername-'  
  
.-Format----Standard----.  
>--+-----+-----<<  
  '-Format----+Standard-+-'  
    '-Detailed-'
```

### Parameter

Datenträgername

Gibt den Namen des bereitgestellten Datenträgers mit sequenziellem Zugriff an. Dieser Name kann mithilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert sind alle bereitgestellten Datenträger.

Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

Standard

Gibt an, dass Teilinformationen angezeigt werden.

Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

## Beispiel: Alle geladenen sequenziellen Datenträger auflisten

---

Informationen zu allen geladenen sequenziellen Datenträgern anzeigen.

```
query mount
```

### AIX-Betriebssysteme

```
ANR8330I 3590 Datenträger D6W992 wurde im Modus R/O
in Laufwerk RMT1 (/dev/rmt1) geladen, Status: IN USE.
ANR8334I 1 Datenträger gefunden.
ANR8331I 8MMTAPE Datenträger WPD000 wurde im Modus
R/W in Laufwerk 8MM.1 (/dev/mt0) geladen, Status: DISMOUNTING.
ANR8334I 1 Datenträger gefunden.
```

### Linux-Betriebssysteme

```
ANR8330I 3590 Datenträger D6W992 wurde im Modus R/O
in Laufwerk RMT1/dev/IBMtape1 geladen, Status: IN USE.
ANR8334I 1 Datenträger gefunden.
ANR8331I 8MMTAPE Datenträger WPD000 wurde im Modus
R/W in Laufwerk 8MM.1 (/dev/tmsmcsi/mt0) geladen, Status: DISMOUNTING.
ANR8334I 1 Datenträger gefunden.
```

### Windows-Betriebssysteme

```
ANR8330I 3590 Datenträger D6W992 wurde im Modus R/O
in Laufwerk RMT1 (/dev/rmt1) geladen, Status: IN USE.
ANR8334I 1 Datenträger gefunden.
ANR8331I 8MMTAPE Datenträger WPD000 wurde im Modus
R/W in Laufwerk 8MM.1 (mt3.0.0.0) geladen, Status: DISMOUNTING.
ANR8334I 1 Datenträger gefunden.
```

Hinweis:

1. Lautet der Status eines Datenträgers FULL oder lautet sein Zugriffsmodus READ-ONLY (R/O), ist der Lademodus des Datenträgers R/O. Um den Status und Zugriffsmodus eines Datenträgers zu bestimmen, geben Sie den Befehl QUERY VOLUME FORMAT=DETAILED aus. Kann ein Datenträger beschrieben werden (d. h., der Status lautet FILLING oder EMPTY), ist der Lademodus des Datenträgers READ/WRITE (R/W), auch wenn der Datenträger nur gelesen wird.
2. In einem Speicherpool, dem der Einheitentyp FILE oder CENTERA zugeordnet ist, kann der Server gleichzeitig mehrere Lesezugriffe und einen Schreibzugriff auf denselben Datenträger ausführen. Daher kann ein Datenträger in einem Speicherpool mit einem Einheitentyp FILE oder CENTERA mehrmals als geladen angezeigt werden.
3. In der Nachricht ANR8448I wird der Laufwerkname als UNKNOWN für Datenträger des Einheitentyps FILE mit einer nicht gemeinsam genutzten Einheitenklasse aufgelistet. Der Grund liegt darin, dass den Datenträgern kein Laufwerk zugeordnet ist; Laufwerknamen werden in dem dateibasierten Speicherarchiv angezeigt.
4. Wenn Sie den Befehl QUERY MOUNT ausgeben, während das Laufwerk gereinigt wird, zeigt die Befehlsausgabe weiterhin den Status DISMOUNTING für den entladenen Datenträger an, bis die Reinigung abgeschlossen ist.

## Beispiel: Ausführliche Informationen zu geladenen sequenziellen Datenträgern anzeigen

---

Ausführliche Informationen zu geladenen Datenträgern anzeigen.

```
query mount format=detailed
```

```
ANR2017I Administrator SERVER_CONSOLE hat folgenden Befehl ausgegeben: QUERY
MOUNT format=detailed
ANR8487I Mountpunkt in Einheitenklasse FILE wartet auf die Beendigung
des Datenträgerladevorgangs -- Eignerserver: SERVER1, Status: WAITING
FOR VOLUME (Sitzung: 0, Prozess: 1).
ANR8488I LTO-Datenträger 015005L4 wurde im Modus R/W in Laufwerk
IBMVT11 (/dev/rmt37) geladen -- Eignerserver: SERVER1, Status: IN
USE (Sitzung: 0, Prozess: 2).
```



ANR8486I Mountpunkt in Einheitenklasse FILE ist reserviert --  
 Eignerserver: SERVER1, Status: RESERVED (Sitzung: 5, Prozess: 0).  
 ANR8334I 3 Übereinstimmungen gefunden.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY MOUNT

| Befehl          | Beschreibung   |
|-----------------|--|
| DISMOUNT VOLUME | Entlädt einen sequenziellen entfernbaren Datenträger anhand des Datenträgernamens. |
| REPLY           | Erlaubt einer Anforderung, die Verarbeitung fortzusetzen.                          |

## QUERY NASBACKUP (NAS-Sicherungsimages abfragen)

Mit diesem Befehl können Informationen zu Dateisystemimageobjekten angezeigt werden, die für einen bestimmten NAS-Knoten und Dateibereich gesichert wurden. Sie können diesen Befehl nur verwenden, um Objekte anzuzeigen, die mit NDMP für einen NAS-Knoten gesichert wurden.

Der Server zeigt alle übereinstimmenden Objekte an, die Daten, an denen diese Objekte gesichert wurden, und Informationen zu einem Inhaltsverzeichnis (TOC) für das Objekt.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-Query NASBackup--Knotenname--Dateibereichsname----->
  .-BEGINDate----TODAY - 7-. .-BEGINTime----00:00:00-.
>+-----+-----+-----+-----+-----+----->
  '-BEGINDate----Datum-----' '-BEGINTime----Zeit-----'

  .-ENDDate----TODAY-. .-ENDTime----23:59:59-.
>+-----+-----+-----+-----+-----+----->
  '-ENDDate----Datum-' '-ENDTime----Zeit-----'

  .-TYPE----BACKUPImage-----
>+-----+-----+-----+-----+-----+-----><
  '-TYPE----BACKUPImage--+'
  '-SNAPMirror--'
```

## Parameter

### Knotenname (Erforderlich)

Gibt den Namen des NAS-Knotens an, für den Sicherungsobjekte angezeigt werden. Sie können zur Angabe dieses Namens keine Platzhalterzeichen verwenden.

### Dateibereichsname (Erforderlich)

Gibt den Namen des Dateibereichs an, für den Sicherungsobjekte angezeigt werden. Sie können zur Angabe dieses Namens Platzhalterzeichen verwenden.

### BEGINDate

Gibt das Anfangsdatum an, ab dem Sicherungsobjekte angezeigt werden sollen. Alle Sicherungsobjekte, die an oder nach dem angegebenen Datum erstellt wurden, werden angezeigt. Der Standardwert ist sieben Tage vor dem aktuellen Datum. Dieser Parameter kann mit dem Parameter BEGINTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Dieser Parameter ist wahlfrei.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert       | Beschreibung         | Beispiel   |
|------------|----------------------|------------|
| MM/TT/JJJJ | Ein bestimmtes Datum | 09/15/2002 |
| TODAY      | Das aktuelle Datum   | TODAY      |

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| TODAY-Tage <i>oder</i> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY-7 <i>oder</i> -7.<br><br>Sollen Informationen zu den Imageobjekten angezeigt werden, die vor einer Woche erstellt wurden, können Sie <code>BEGINDATE=TODAY-7</code> oder <code>BEGINDATE= -7</code> angeben. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.  | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.   |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.  | BOTM   |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage.   | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.  |

#### BEGINTime

Gibt die Anfangszeit an, ab der Sicherungsobjekte angezeigt werden sollen. Alle Sicherungsobjekte, die zu oder nach der angegebenen Zeit erstellt wurden, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist Mitternacht (00:00:00) an dem Datum, das als `BEGINDATE` angegeben wurde.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert                         | Beschreibung   | Beispiel   |
|------------------------------|--|--|
| HH:MM:SS                     | Eine bestimmte Uhrzeit am angegebenen Anfangsdatum                             | 10:30:08   |
| NOW                          | Die aktuelle Uhrzeit am angegebenen Anfangsdatum                               | NOW  |
| NOW+HH:MM <i>oder</i> +HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Anfangsdatum  | NOW+03:00 <i>oder</i> +03:00.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe <code>BEGINTIME=NOW+3</code> oder <code>BEGINTIME=+3</code> ausgegeben, zeigt der Server Imageobjekte mit der Uhrzeit 12:00 Uhr oder später am Anfangsdatum an.       |
| NOW-HH:MM <i>oder</i> -HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Anfangsdatum | NOW-04:00 <i>oder</i> -04:00.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe <code>BEGINTime=NOW-3:30</code> oder <code>BEGINTime= -3:30</code> ausgegeben, zeigt der Server Imageobjekte mit der Uhrzeit 5:30 Uhr oder später am Anfangsdatum an. |

#### ENDDate

Gibt das Enddatum an, das zum Auswählen der Sicherungsobjekte verwendet wird, die angezeigt werden sollen. Alle Sicherungsobjekte, die an oder vor dem angegebenen Datum erstellt wurden, werden angezeigt. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum. Dieser Parameter kann mit dem Parameter `ENDTIME` verwendet werden, um ein Enddatum und eine Endzeit anzugeben.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                           | Beschreibung   | Beispiel   |
|--------------------------------|--|--|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 09/15/2002   |
| TODAY                          | Das aktuelle Datum   | TODAY  |
| TODAY-Tage <i>oder</i> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY-1 <i>oder</i> -1.<br><br>Sollen Informationen angezeigt werden, die bis gestern erstellt wurden, kann <code>ENDDATE=TODAY-1</code> oder einfach <code>ENDDATE= -1</code> angegeben werden. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM   |

| Wert                        | Beschreibung   | Beispiel   |
|-----------------------------|--|--|
| EOLM-Tage                   | Der letzte Tag des Vormonats minus angegebene Tage.      | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats) | Der erste Tag des aktuellen Monats.                      | BOTM   |
| BOTM+Tage                   | Der erste Tag des aktuellen Monats plus angegebene Tage. | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

#### ENDTime

Gibt die Endzeit an, die zum Auswählen der Sicherungsobjekte verwendet wird, die angezeigt werden sollen. Alle Sicherungsobjekte, die zu oder vor der angegebenen Zeit erstellt wurden, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist 23:59:59. Dieser Parameter kann zusammen mit dem Parameter ENDDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert                         | Beschreibung   | Beispiel  |
|------------------------------|--|---|
| HH:MM:SS                     | Eine bestimmte Uhrzeit am angegebenen Enddatum                             | 10:30:08  |
| NOW                          | Die aktuelle Uhrzeit am angegebenen Enddatum                               | NOW   |
| NOW+HH:MM <i>oder</i> +HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum  | NOW+03:00 <i>oder</i> +03:00.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW+3:00 oder ENDTIME= +3:00 ausgegeben, zeigt der Server Imageobjekte mit der Uhrzeit 12:00 Uhr oder später am angegebenen Enddatum an. |
| NOW-HH:MM <i>oder</i> -HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum | NOW-03:30 <i>oder</i> -03:30.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW-3:30 oder ENDTIME= -3:30 ausgegeben, zeigt der Server Imageobjekte mit der Uhrzeit 5:30 Uhr oder später am angegebenen Enddatum an.  |

#### TYPE

Gibt den Typ der NDMP-Sicherungsimages an, für die Informationen angezeigt werden sollen. Der Standardwert für diesen Parameter ist BACKUPIMAGE. Andere Imagetypen stellen Sicherungsmethoden dar, die für einen bestimmten Dateiserver spezifisch sein können. Gültige Werte:

#### BACKUPImage

Gibt an, dass die Ausgabe nur die standardmäßigen NAS-Basis- und -Differenzsicherungsimages zeigen soll. Dies ist der Standardwert für diesen Parameter.

#### SNAPMirror

Gibt an, ob Informationen zu NetApp SnapMirror-Images angezeigt werden sollen. SnapMirror-Images sind Gesamtsicherungsimages auf Blockebene eines Dateisystems. Ein SnapMirror-Image kann nur in ein Dateisystem zurückgeschrieben werden, das als SnapMirror-Zieldatenträger vorbereitet wurde. Weitere Informationen enthält die Dokumentation zu Ihrem NetApp-Dateiserver. Dieser Parameter ist nur für NetApp- und IBM N-Series-Dateiserver gültig.

## Beispiel:

Geben Sie den Befehl QUERY NASBACKUP aus, um Informationen zu dem Knoten nas1 und dem Dateibereich /vol/vol1 anzuzeigen.

```
query nasbackup nas1 /vol/vol1
```

```

Knoten- Dateiber.- Objekt- Objekt- Erstell.- Hat Verwalt.- Image-
name Name typ gröÙe Datum Inhalts- Klassen- speicher-
(MB) (MB) verzeichnis name poolname
-----
NAS1 vol/vol1 Gesamtimage 1050,5 10/22/2002 YES DEFAULT NASBACKUPS

```

|      |          |                     |        |                        |     |          |            |
|------|----------|---------------------|--------|------------------------|-----|----------|------------|
| NAS1 | vol/vol1 | Differenz-<br>image | 9,1    | 10/22/2002<br>11:03:21 | YES | DEFAULT  | NASBACKUPS |
| NAS1 | vol/vol1 | Gesamtimage         | 1050,5 | 10/22/2006<br>10:43:00 | YES | STANDARD | FILEPOOL   |
| NAS1 | vol/vol1 | Differenz-<br>image | 9,1    | 10/25/2006<br>11:53:21 | YES | STANDARD | FILEPOOL   |

## Beispiel:

Geben Sie den Befehl QUERY NASBACKUP aus, um Informationen zu allen NetApp SnapMirror-auf-Band-Images für den Knoten nas2 und den Dateibereich /vol/vol2 anzuzeigen.

```
query nasbackup nas2 /vol/vol2 type=snapmirror
```

| Knoten-<br>name | Dateiber-<br>Name | Objekt-<br>typ | Objekt-<br>größe<br>(MB) | Erstell.-<br>Datum     | Verwalt.-<br>Klassen-<br>name | Image-<br>speicher-<br>poolname |
|-----------------|-------------------|----------------|--------------------------|------------------------|-------------------------------|---------------------------------|
| NAS2            | vol/vol2          | SnapMirror     | 1050,5                   | 04/02/2008<br>10:50:57 | STANDARD                      | MYPOOL                          |
| NAS2            | vol/vol2          | SnapMirror     | 1450,5                   | 04/02/2008<br>11:03:21 | STANDARD                      | MYPOOL                          |

## Feldbeschreibungen

- Knotenname  
Der Name des Clientknotens.
- Dateibereichsname  
Der Name des Dateibereichs.
- Objektyp  
Der Typ des gesicherten Objekts.
- Objektgröße (MB)  
Die Größe des Objekts in Megabyte.
- Erstellungsdatum  
Das Datum, an dem die Sicherung erstellt wurde.
- Name der Verwaltungsklasse  
Der Name der Verwaltungsklasse.
- Imagespeicherpoolname  
Der Name des Speichers, in dem sich die Sicherung befindet.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY NASBACKUP

| Befehl   | Beschreibung  |
|--|---|
| BACKUP NODE                                    | Sichert einen NAS-Knoten (NAS = Network Attached Storage).                    |
| BACKUP NAS (IBM Spectrum Protect-Clientbefehl) | Erstellt eine Sicherung der NAS-Knotendaten.                                  |
| QUERY TOC                                      | Zeigt Details zum Inhaltsverzeichnis für ein angegebenes Sicherungsimagen an. |
| RESTORE NODE                                   | Schreibt einen NAS-Knoten (NAS = Network Attached Storage) zurück.            |

## QUERY NODE (Knoten abfragen)

Mit diesem Befehl können Informationen zu einem oder zu mehreren registrierten Knoten angezeigt werden.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
.-*-----.
```

```

>>-Query Node-----+-----+-----+-----+----->
      '-Knotenname-' |           .-,-------. |
                        |           v           | |
                        '-D0main-----Domänenname-+-'

      .-Format-----Standard-----.
>-----+-----+-----+-----+----->
      '-Format-----+Standard-+-'
                '-Detailed-'

                                .-Type-----Client-----.
>-----+-----+-----+-----+-----<
      '-AUTHentication-----+Local-+-' '-Type-----+Client-+-'
                '-LDap--'                +-NAS-----+
                                        +-Server-+
                                        '-Any-----'

```

## Parameter

### Knotenname

Gibt den Namen des abzufragenden Clientknotens an. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Alle übereinstimmenden Clientknoten werden abgefragt. Wird kein Wert für diesen Parameter angegeben, werden alle Clientknoten abgefragt. Der Parameter ist wahlfrei.

### D0main

Gibt eine Liste mit Maßnahmendomänen an, auf die sich die Clientknotenabfrage beschränken soll. In diesem Fall werden dann nur Knoten angezeigt, die einer der angegebenen Maßnahmendomänen zugeordnet sind. Dieser Parameter ist wahlfrei. Die Einträge in der Liste ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um eine Domäne anzugeben. Alle Clients, die einer übereinstimmenden Domäne zugeordnet sind, werden angezeigt. Wird kein Wert für diesen Parameter angegeben, wird die Abfrage für alle Maßnahmendomänen ausgeführt.

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Sie können einen der folgenden Werte angeben:

#### Standard

Gibt an, dass Teilinformationen für die angegebenen Clientknoten angezeigt werden.

#### Detailed

Gibt an, dass die gesamten Informationen für die angegebenen Clientknoten angezeigt werden.

### Type

Gibt den Typ des Knotens an, der in den Abfrageergebnissen berücksichtigt werden soll. Der Parameter ist wahlfrei. Der Standardwert ist CLIENT. Sie können einen der folgenden Werte angeben:

#### Any

Gibt einen beliebigen Typ des Knotens an.

#### Client

Gibt Clientknoten an, die Clients für Sichern/Archivieren, IBM Spectrum Protect for Space Management-Clients oder Anwendungsclients sind.

#### NAS

Gibt NAS-Knoten an.

#### Server

Gibt Clientknoten an, die andere -Server sind.

### Authentication

Gibt die Kennwortauthentifizierungsmethode für den Knoten an.

#### Local

Zeigt die Knoten an, die sich mit dem IBM Spectrum Protect-Server authentifizieren.

#### LDap

Zeigt die Knoten an, die sich mit einem LDAP-Verzeichnissever authentifizieren. Bei dem Knotenkennwort muss die Groß-/Kleinschreibung beachtet werden.

## Beispiel: Informationen zu registrierten Clientknoten anzeigen

Informationen zu allen registrierten Clientknoten anzeigen.

```
query node
```

| Knotenname | Plattform | Maßnah-<br>mendomäne | Tage seit<br>letz. Zugr. | Tage seit<br>Kennwort-<br>vergabe | Gesperrt? |
|------------|-----------|----------------------|--------------------------|-----------------------------------|-----------|
| CLIENT1    | AIX       | STANDARD             | 6                        | 6                                 | No        |
| GEORGE     | AIX       | STANDARD             | 1                        | 1                                 | No        |
| JANET      | AIX       | STANDARD             | 1                        | 1                                 | No        |
| JARED      | Linux86   | STANDARD             | 1                        | 1                                 | No        |
| JOE2       | Mac       | STANDARD             | <1                       | <1                                | No        |
| TOMC       | WinNT     | STANDARD             | 1                        | 1                                 | No        |

## Beispiel: Ausführliche Informationen zu einem Clientknoten anzeigen

Die gesamten Informationen zum Clientknoten Joe anzeigen.

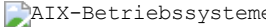

```
query node joe format=detailed
```

```

Knotenname: JOE
  Plattform: WinNT
  Client-OS-Stufe: 4.00
  Client-Version: Version 5, Release 4, Stufe 0.0
  Anwendungsversion: Version 6, Release 4, Stufe 0.4
  Name der Maßnahmendomäne: STANDARD
  Letzter Zugriff: 09/24/2012 18:55:46
  Tage seit letztem Zugriff: 6
  Datum/Zeit der Kennwortvergabe: 09/24/2012 18:26:43
  Tage seit Kennwortvergabe: 6
  Zahl der ungültigen Anmeldeversuche: 0
  Gesperrt?: No
  Kontaktinformationen:
    Komprimierung: Client
    Archivierung löschen?: Yes
    Sicherung löschen?: No
    Registriert am: 09/24/2012 18:26:43
    Registriert durch: SERVER_CONSOLE
  Zuletzt verwendete Übertragungsmethode: Tcp/Ip
  Byte empfangen (letzte Sitzung): 108.731
  Byte gesendet (letzte Sitzung): 698
  Dauer der letzten Sitzung: 0,00
  Inaktiver Wartestatus in % (letzte Sitzung): 0,00
  Auf Übertragung warten in % (letzte Sitzung): 0,00
  Auf Datenträger warten in % (letzte Sitzung): 0,00
  Optionsgruppe:
    URL: http://joe.host.name:1581
    Knotentyp: Client
    Kennwortablaufdauer: 60
    Mountpunkt beibehalten?: No
    Max. zulässige Mountpunkte: 2
    Auto. Dateibereichsumbenennung: No
    Protokoll auswerten: No
    TCP/IP-Name:
    TCP/IP-Adresse: 9.11.153.39
    Global eindeutige ID: 11.9c.54.e0.8a.b5.11.d6.b3.c3.00.06.29.45.c1
    Max. Transaktionsgruppe: 0
    Pfad zum Schreiben von Daten: ANY
    Pfad zum Lesen von Daten: ANY
    Sitzungsstart: ClientOrServer
    Adresse der oberen Ebene:
    Adresse der unteren Ebene: 1501
    Name der Kollokationsgruppe:
    Proxyknotenziel:
    Proxyknotenagent:
    Knotengruppen:
    E-Mail-Adresse:
  Deduplizierung: ServerOnly

```

```

  Benutzer, die Sicherung ausführen dürfen: ALL
  Replikationsstatus: Aktiviert
  Replikationsmodus: Send
  Replikationsregel für Sicherungsdaten: DEFAULT
  Replikationsregel für Archivierungsdaten: ALL_DATA
  Replikationsregel für speicherverwaltete Daten: None
  Primärer Replikationsserver: PRODSERVER1
  Zuletzt repliziert auf Server: DRSERVER1
  Client-OS-Name: WIN: Windows XP
  Clientprozessorarchitektur: x86

```

Installierte Clientprodukte: WIN, FCM, VE  
Clientzielversion: Version 6, Release 2, Stufe 0.0  
Authentifizierung: Local  
SSL erforderlich: No  
Sitzungssicherheit: Strict  
Transportmethode: TLS 1.2  
Große Objekte aufteilen: Yes  
Typ für Gefährdung: Standardintervall  
Gefährdungsintervall:  
Dienstprogramm-URL:  
Replikationswiederherstellung beschädigter Dateien: Yes  
Stillgelegt:  
Datum der Stilllegung:

## Feldbeschreibungen

---

### Knotenname

Der Name des Clientknotens.

### Plattform

Das Betriebssystem des Clientknotens zu dem Zeitpunkt, als der Clientknoten das letzte Mal den Server angesprochen hat. Ein Fragezeichen (?) wird angezeigt, bis der Clientknoten zum ersten Mal auf den Server zugreift und seinen Betriebssystemtyp angibt.

### Client-OS-Stufe

Die Stufe des Betriebssystems für den Client zu dem Zeitpunkt, als der Clientknoten das letzte Mal den Server angesprochen hat.

### Client-Version

Die Version des Clients, die auf dem Clientknoten installiert ist.

Dieses Feld gilt nicht für NAS-Knoten.

### Anwendungsversion

Die Version des Data Protection for VMware-Clients.

### Name der Maßnahmendomäne

Die zugeordnete Maßnahmendomäne des Clientknotens.

### Letzter Zugriff

Das Datum und die Uhrzeit, an dem bzw. zu der der Clientknoten zuletzt auf den Server zugegriffen hat.

### Tage seit letztem Zugriff

Die Anzahl der Tage, die vergangen sind, seit der Clientknoten das letzte Mal auf den Server zugegriffen hat.

### Datum/Zeit der Kennwortvergabe

Das Datum und die Uhrzeit, an dem bzw. zu der das Kennwort für den Clientknoten definiert wurde.

### Tage seit Kennwortvergabe

Die Anzahl der Tage, die vergangen sind, seit das Kennwort für den Clientknoten definiert wurde.

### Zahl der ungültigen Anmeldeversuche

Die Anzahl der ungültigen Anmeldeversuche seit der letzten erfolgreichen Anmeldung. Diese Anzahl kann nur dann ungleich Null sein, wenn der Grenzwert für ungültige Kennworteingaben (SET INVALIDPWLIMIT) größer Null ist. Ist die Anzahl der ungültigen Versuche gleich dem mit dem Befehl SET INVALIDPWLIMIT definierten Grenzwert, wird der Knoten gesperrt.

### Gesperrt?

Angabe, ob dem Clientknoten der Zugriff auf IBM Spectrum Protect verweigert wird.

### Kontaktinformationen

Kontaktinformationen für den Clientknoten.

### Komprimierung

Gibt an, ob die Komprimierung auf dem Clientknoten aktiviert ist.

Dieses Feld gilt nicht für NAS-Knoten.

### Archivierung löschen?

Angabe, ob der Clientknoten seine eigenen Archivierungsdateien löschen darf.

### Sicherung löschen?

Gibt an, ob der Clientknoten seine eigenen Sicherungsdateien löschen darf.

### Registriert am

Das Datum und die Uhrzeit, an dem bzw. zu der der Clientknoten registriert wurde.

### Registriert durch

Der Name des Administrators, der den Clientknoten registriert hat.

### Zuletzt verwendete Übertragungsmethode

Die Übertragungsmethode, die zuletzt vom Clientknoten verwendet wurde, um den Server anzusprechen.

### Byte empfangen (letzte Sitzung)

Die Anzahl der Byte, die während der letzten Sitzung des Clientknotens vom Server empfangen wurden.

Dieses Feld gilt nicht für NAS-Knoten.

#### Byte gesendet (letzte Sitzung)

Die Anzahl Byte, die an den Clientknoten gesendet wurden.

Dieses Feld gilt nicht für NAS-Knoten.

#### Dauer der letzten Sitzung

Die Dauer der letzten Sitzung des Clientknotens in Sekunden.

Dieses Feld gilt nicht für NAS-Knoten.

#### Inaktiver Wartestatus in % (letzte Sitzung)

Der Prozentsatz der gesamten Sitzungszeit, zu dem der Client keine Funktionen ausgeführt hat.

Dieses Feld gilt nicht für NAS-Knoten.

#### Auf Übertragung warten in % (letzte Sitzung)

Der Prozentsatz der gesamten Sitzungszeit, zu dem der Client auf eine Übertragungsantwort von dem Server gewartet hat.

Dieses Feld gilt nicht für NAS-Knoten.

#### Auf Datenträger warten in % (letzte Sitzung)

Der Prozentsatz der gesamten Sitzungszeit, zu dem der Client auf das Laden eines austauschbaren Datenträgers gewartet hat.

Dieses Feld gilt nicht für NAS-Knoten.

#### Optionsgruppe

Der Name der Clientoptionsgruppe.

#### URL

Die URL des IBM Spectrum Protect-Web-Clients, die auf dem Clientsystem konfiguriert ist. Sie können die URL in einem Web-Browser und im Operations Center verwenden, um den Clientknoten über Fernzugriff zu verwalten.

#### Knotentyp

Der Typ des Clientknotens. Die folgenden Werte sind gültig:

- Client: Client für Sichern/Archivieren, IBM Spectrum Protect for Space Management-Client oder Anwendungsclient
- Server: IBM Spectrum Protect-Server
- NAS: NAS-Dateiserver

#### Kennwortablaufdauer

Die Kennwortablaufdauer des Clientknotens.

#### Mountpunkt beibehalten?

Die Angabe, ob der Clientknoten während einer Sitzung einen Mountpunkt beibehält.

#### Max. zulässige Mountpunkte

Die Anzahl der Mountpunkte, die ein Clientknoten für die IBM Spectrum Protect for Space Management-Umlagerung sowie für Sicherungs- und Archivierungsoperationen auf dem Server verwenden kann. Dieser Parameter gilt nicht für Knoten mit dem Typ NAS oder SERVER. Wurde ein Clientknoten für einen Server mit Version 3.7 oder höher registriert, liegt der Wert im Bereich von 0 bis 999, abhängig von dem Wert, der mit dem Parameter MAXNUMMP des Befehls REGISTER NODE definiert wird. Wurde der Clientknoten unter vorherigen Versionen des Servers registriert und wurde der Parameter MAXNUMMP nicht explizit mit dem Befehl UPDATE NODE definiert, wird der Wert auf NOLIMIT gesetzt. Der MAXNUMMP-Wert wird während der Operationen zum Lesen von Clientdaten, wie beispielsweise Zurückschreiben, Abrufen und Zurückrufen durch IBM Spectrum Protect for Space Management, nicht ausgewertet oder umgesetzt. Mountpunkte, die für Operationen zum Lesen von Daten verwendet werden, werden jedoch in Bezug auf versuchte gleichzeitig ablaufende Datenspeicherungsoperationen für denselben Clientknoten ausgewertet. Diese Auswertung kann verhindern, dass die Datenspeicherungsoperationen Mountpunkte anfordern können.

#### Auto. Dateibereichsumbenennung

Gibt an, ob IBM Spectrum Protect den Client zum Umbenennen von Dateibereichen auffordert, wenn für das Clientsystem ein Upgrade auf einen Client erfolgt, der Unicode unterstützt. Dieses Feld ist nur für Clientsysteme gültig, die die Betriebssysteme Windows, Macintosh OS X oder NetWare verwenden.

#### Protokoll auswerten (veraltet)

Gibt an, ob für den Client die Datenprüfung aktiviert ist. Ist für den Client die Datenprüfung aktiviert, gibt dieses Feld an, ob IBM Spectrum Protect nur die Dateidaten oder alle Daten, einschließlich Dateimetadaten, auswertet. Sie können die Datenprüfung aktivieren, indem Sie den Befehl REGISTER NODE oder UPDATE NODE verwenden. Dieses Feld wird nicht mehr verwendet.

#### TCP/IP-Name

Der Hostname des Clientknotens zu dem Zeitpunkt, als der Clientknoten das letzte Mal den Server angesprochen hat. Das Feld ist leer, wenn die Clientsoftware das Melden dieser Informationen an den Server nicht unterstützt.

#### TCP/IP-Adresse

Die TCP/IP-Adresse des Clientknotens zu dem Zeitpunkt, als der Clientknoten das letzte Mal den Server angesprochen hat. Das Feld ist leer, wenn die Clientsoftware das Melden dieser Informationen an den Server nicht unterstützt.



#### Global eindeutige ID

Die global eindeutige ID (Globally Unique Identifier = GUID) zu dem Zeitpunkt, als der Clientknoten das letzte Mal den Server angesprochen hat. Diese GUID identifiziert den Host-Computer, auf dem sich der Knoten befindet.

#### Max. Transaktionsgruppe

Gibt die Anzahl der Dateien pro festgeschriebener Transaktion an, die zwischen einem Client und einem Server übertragen werden. Die Clientleistung kann verbessert werden, indem ein höherer Wert für diese Option verwendet wird.



#### Pfad zum Schreiben von Daten

Gibt den Übertragungspfad an, der verwendet wird, wenn der Client während Speicheroperationen Daten an den Server und/oder den Speicheragenten sendet. Ist kein Pfad verfügbar, kann der Knoten keine Daten senden.

  Gültige Datenübertragungsoptionen sind ANY, LAN oder LAN-unabhängig.

#### Pfad zum Lesen von Daten

Gibt den Übertragungspfad an, der verwendet wird, wenn der Server und/oder Speicheragent während Operationen wie Zurückschreiben oder Abrufen Daten für einen Client lesen. Ist kein Pfad verfügbar, können keine Daten gelesen werden.

  Gültige Datenübertragungsoptionen sind ANY, LAN oder LAN-unabhängig.

#### Sitzungsstart

Steuert, ob der Server oder der Client Sitzungen einleitet. Die beiden folgenden Optionen sind verfügbar:

- ClientOrServer
- Serveronly

#### Adresse der höheren Ebene

Gibt die Client-IP-Adresse an, die der Server anspricht, um geplante Ereignisse einzuleiten, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist.

#### Adresse der unteren Ebene

Gibt die Clientanschlussnummer an, an der der Client für Sitzungen von dem Server empfangsbereit ist, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist.

#### Name der Kollokationsgruppe

Gibt den Namen der Kollokationsgruppe an, zu der ein Knoten gehört. Gehört ein Knoten nicht zu einer Kollokationsgruppe, ist dieses Feld leer.

Tipp: Wenn der Knoten Dateibereiche enthält, die Mitglieder einer Dateibereichskollokationsgruppe sind, bleibt dieses Feld leer. Sie können Dateibereichsnamen suchen, indem Sie den Befehl QUERY FILESPACE ausgeben.

#### Proxyknotenziel

Gibt in einer durch Leerzeichen getrennten Liste an, welche Knoten Proxyknoten (Agenten) für andere Knoten sind. Sind für diesen Typ der Zuordnung keine Knoten vorhanden, ist dieses Feld leer.

#### Proxyknotenagent

Gibt in einer durch Leerzeichen getrennten Liste den ursprünglichen Knotennamen (Zielknotennamen) für eine Proxyknotensitzung an. Sind für diesen Typ der Zuordnung keine Knoten vorhanden, ist dieses Feld leer.

#### Knotengruppen



Gibt den Namen der Knotengruppe an, zu der ein Knoten gehört. Gehört ein Knoten nicht zu einer Knotengruppe, ist dieses Feld leer.


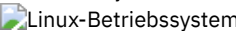
#### E-Mail-Adresse

Gibt die E-Mail-Adresse des Clientknotens an.

#### Deduplizierung

Die Position, an der Daten dedupliziert werden. Der Wert ServerOnly gibt an, dass von diesem Knoten gespeicherte Daten nur auf dem Server dedupliziert werden können. Der Wert Clientorserver gibt an, dass von diesem Knoten gespeicherte Daten entweder auf dem Client oder auf dem Server dedupliziert werden können.

  Benutzer, die Sicherung ausführen dürfen

  Gibt an, ob die ID eines Benutzers ohne Rootberechtigung oder nur eine Rootbenutzer-ID Dateien auf dem Server sichern kann. ALL gibt alle Benutzer an, während ROOT angibt, dass nur die Rootbenutzer-ID Dateien auf dem Server sichern kann. Diese Ausgabe ist nicht verfügbar, wenn das Betriebssystem des Clientknotens als Betriebssystem für einen einzelnen Benutzer betrachtet wird.

#### Replikationsstatus

Gibt an, ob der Knoten für die Replikation aktiviert ist. Die folgenden Werte sind gültig:

##### Aktiviert

Der Knoten ist für die Replikation konfiguriert und für die Replikation bereit.

##### Inaktiviert

Der Knoten ist für die Replikation konfiguriert, aber nicht für die Replikation bereit.

##### Keine.

Der Knoten ist nicht für die Replikation konfiguriert.

#### Replikationsmodus

Gibt an, ob der Knoten als Quelle oder als Ziel der replizierten Daten konfiguriert ist. Ist dieses Feld leer, ist der Knoten nicht für die Replikation konfiguriert. Die folgenden Werte sind gültig:

Send

Der Knoten ist als Quelle der Daten für die Replikation konfiguriert.

Receive

Der Knoten ist als Ziel der Daten für die Replikation konfiguriert.

SyncSend

Die Daten, die zu dem Knoten gehören, müssen mit den Knotendaten synchronisiert werden, die sich auf dem Zielreplikationsserver befinden. Die Synchronisation gilt nur für Knoten, deren Daten von einem Quellenreplikationsserver importiert und auf den Zielreplikationsserver importiert wurden. Die Synchronisation erfolgt während der Replikation.

SyncReceive

Die Daten, die zu dem Knoten gehören, müssen mit den Knotendaten synchronisiert werden, die sich auf dem Quellenreplikationsserver befinden. Die Synchronisation gilt nur für Knoten, deren Daten von einem Quellenreplikationsserver importiert und auf den Zielreplikationsserver importiert wurden. Die Synchronisation erfolgt während der Replikation.

Keine.

Der Knoten ist nicht für die Replikation konfiguriert.

Primärer Replikationsserver

Gibt den Quellenreplikationsserver für den Clientknoten an.

Replikationsregel für Sicherungsdaten

Replikationsregel für Archivierungsdaten

Replikationsregel für speicher verwaltete Daten

Die Replikationsregel, die für Sicherungsdaten, Archivierungsdaten und speicher verwaltete Daten gilt, die zu dem Knoten gehören. Die folgenden Werte sind gültig:

ALL\_DATA

Repliziert Sicherungsdaten, Archivierungsdaten oder speicher verwaltete Daten. Die Daten werden mit normaler Priorität repliziert.

ACTIVE\_DATA

Repliziert aktive Sicherungsdaten. Die Daten werden mit normaler Priorität repliziert.

Achtung: Wenn Sie ACTIVE\_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

- Wenn eine frühere Serverversion als Version 7.1.1 auf dem Quellen- oder Zielreplikationsserver installiert ist.
- Wenn Sie den Befehl REPLICATE NODE mit dem Parameter `FORCERECONCILE=YES` verwenden.
- Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Serverversion vor Version 7.1.1 ausführen.

Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

ALL\_DATA\_HIGH\_PRIORITY

Repliziert Sicherungsdaten, Archivierungsdaten oder speicher verwaltete Daten. Die Daten werden mit hoher Priorität repliziert.

ACTIVE\_DATA\_HIGH\_PRIORITY

Diese Regel entspricht der Replikationsregel ACTIVE\_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden.

DEFAULT

Repliziert Sicherungsdaten, Archivierungsdaten oder speicher verwaltete Daten gemäß der Domänenregel für den Datentyp.

NONE

Es werden keine Daten repliziert. Lautet beispielsweise die Replikationsregel für Archivierungsdaten NONE, werden Archivierungsdaten, die zu dem Knoten gehören, nicht repliziert.

Zuletzt repliziert auf Server

Gibt den Namen des Servers an, auf den der Knoten zuletzt repliziert wurde, und den Namen des Servers an, der während der Ausführung von Zurückschreibungsoperationen für die Übernahme des Clients verwendet wird.

Client-OS-Name

Das Betriebssystem des Clients. Der Assistent für die Clientimplementierung verwendet diese Informationen zum Implementieren eines Pakets auf dem Client. Dieses Feld wird nur für IBM Spectrum Protect-Clients mit Version 6.2.0.0 und höher aufgelistet.

Clientprozessorarchitektur

Die Architektur des Clients. Der Assistent für die Clientimplementierung verwendet diesen Wert, um das Paket zu bestimmen, das beim Aktualisieren des Clients implementiert werden soll. Dieses Feld wird nur für IBM Spectrum Protect-Clients mit Version 6.2.0.0 und höher aufgelistet.

#### Installierte Clientprodukte

Die Produkte, die sich auf dem Knoten befinden. Die folgenden Produkte können aufgelistet werden:

- BA (Client für Sichern/Archivieren)
- VE (Virtual Environments)
- FCM (FlashCopy Manager)

#### Clientzielversion

Die Version des Clients, die zu einem Zeitpunkt installiert wird, der mit dem Befehl DEFINE SCHEDULE oder UPDATE SCHEDULE geplant wird. Dieses Feld wird nur für IBM Spectrum Protect-Clients mit Version 6.2.0.0 und höher aufgelistet.

#### Authentifizierung

Gibt die Kennwortauthentifizierungsmethode an: LOCAL, LDAP oder LDAP (künftig).

| Authentifizierungsziel  | Authentifizierungsmethode |
|---|---------------------------|
| IBM Spectrum Protect-Server   | LOCAL                     |
| LDAP-Verzeichnisserver  | LDAP                      |
| Dieser Knoten ist für die Authentifizierung mit einem LDAP-Verzeichnisserver konfiguriert, aber der Knoten hat sich noch nicht authentifiziert. | LDAP (künftig)            |

#### SSL erforderlich (veraltet)

Gibt an, ob die Sicherheitseinstellung für den Knoten das Protokoll Secure Sockets Layer (SSL) erfordert. Die gültigen Werte sind YES, NO oder Default. Sie müssen über die Berechtigung auf Systemebene verfügen, um die Einstellung von SSLREQUIRED für den Knoten zu aktualisieren. Dieses Feld wird nicht mehr verwendet.

#### Sitzungssicherheit

Gibt die Stufe der Sitzungssicherheit an, die für den Knoten durchgesetzt wird. Die gültigen Werte sind STRICT und TRANSITIONAL.

#### Transportmethode

Gibt die Transportmethode an, die zuletzt für den angegebenen Knoten verwendet wurde. Die gültigen Werte sind TLS 1.2, TLS 1.1 und NONE. Ein Fragezeichen (?) wird angezeigt, bis eine erfolgreiche Authentifizierung ausgeführt wird.

#### Große Objekte aufteilen

Gibt an, ob große Objekte, die von diesem Knoten gespeichert werden, automatisch vom Server in kleinere Teile aufgeteilt werden, um die Serververarbeitung zu optimieren. 'Yes' gibt an, dass der Server große Objekte (über 10 GB) in kleinere Teile aufteilt, wenn sie von einem Clientknoten gespeichert werden. 'No' gibt an, dass dieser Prozess übergangen wird. Der Standardwert ist 'Yes'.

#### Typ für Gefährdung

Gibt den Auswertungstyp für Gefährdung an. Die gültigen Werte sind 'Standard', 'Übergangen' oder 'Angepasst'. 'Standard' gibt an, dass der Knoten mit demselben Intervall ausgewertet wird, das für die Knotenklassifizierung mit dem Befehl SET STATUSATRISKINTERVAL angegeben wurde. 'Übergangen' gibt an, dass der Gefährdungsstatus für den Knoten nicht vom Statusmonitor ausgewertet wird. 'Angepasst' gibt an, dass der Knoten mit dem Intervall ausgewertet wird, das mit dem Befehl SET NODEATRISKINTERVAL angegeben wurde, und nicht mit dem Intervall, das mit dem Befehl SET STATUSATRISKINTERVAL angegeben wurde.

#### Gefährdungsintervall

Gibt die Anzahl der Stunden zwischen zwei Clientsicherungsaktivitäten oder zwei Replikationsaktivitäten an, nach denen der Statusmonitor angibt, dass die Aktivität gefährdet ist. Dieses Feld enthält nur dann einen Wert, wenn das Feld Typ für Gefährdung den Wert Angepasst enthält.

#### Dienstprogramm-URL

Gibt die Adresse der IBM Spectrum Protect-Clientverwaltungsservices an, die auf dem Clientsystem konfiguriert sind. Diese URL wird vom Operations Center verwendet, um auf Clientprotokolldateien zuzugreifen, sodass Sie im Operations Center Clientprobleme über Fernzugriff diagnostizieren können.

#### Replikationswiederherstellung beschädigter Dateien

Gibt an, ob beschädigte Dateien für diesen Knoten von einem Zielreplikationsserver wiederhergestellt werden können.

#### Stillgelegt

Gibt an, ob der Clientknoten stillgelegt ist. Die folgenden Werte sind gültig:

YES

Gibt an, dass der Knoten stillgelegt ist.

Nullwert

Gibt an, dass der Knoten nicht stillgelegt ist.

PENDING

Gibt an, dass der Knoten gerade stillgelegt wird oder der Stilllegungsprozess fehlgeschlagen ist.

Tipp: Wenn Sie den Status eines anstehenden Stilllegungsprozesses bestimmen möchten, führen Sie die Anweisungen in Clientknoten stilllegen aus.

Datum der Stilllegung

Gibt das Datum an, an dem der Clientknoten stillgelegt wurde.

## Beispiel: Informationen zu Knotenrollen anzeigen

---

Die Beispielausgabe ist nur ein Teil der Gesamtanzeige.

```
query node alvin f=d
```

```
Proxyknotenagent:
Knotengruppen:
E-Mail-Adresse:
Deduplizierung: ServerOnly
Benutzer, die Sicherung ausführen dürfen: All
Rolle: Server
Rollenüberschreibung: UseReported
Prozessorhersteller: ORACLE
Prozessormarke: UltraSPARC-T2
Prozessortyp: 4
Prozessormodell:
Anzahl Prozessoren: 1
Hypervisor:
API-Anwendung: NO
Fehler bei der Suche: NO
MAC-Adresse:
```

## Feldbeschreibungen

---

Rolle

Die vom Client zurückgemeldete Prozessorrole.

Rollenüberschreibung

Der mit dem Befehl UPDATE NODE angegebene Überschreibungswert für 'Rolle'.

Prozessorhersteller

Der vom Client zurückgemeldete Prozessorhersteller.

Prozessormarke

Die vom Client zurückgemeldete Prozessormarke.

Prozessortyp

Der vom Client zurückgemeldete Prozessortyp. Dieser Wert gibt die Anzahl der Prozessorkerne an, die für die PVU-Berechnung verwendet werden.

Prozessormodell

Das vom Client zurückgemeldete Prozessormodell.

Anzahl Prozessoren

Die vom Client zurückgemeldete Anzahl Prozessoren.

Hypervisor

Der vom Client zurückgemeldete Hypervisor.

API-Anwendung

Der Clientanzeiger, der angibt, dass der Client eine API-Anwendung ist.

Fehler bei der Suche

Gibt an, ob die letzte Suche nach Prozessorinformationen möglicherweise fehlerhaft ist und untersucht werden muss.

MAC-Adresse

Die vom Client zurückgemeldete MAC-Adresse.

## Beispiel: Alle Knoten anzeigen, die sich mit dem IBM Spectrum Protect-Server authentifizieren

---

Sollen alle Knoten angezeigt werden, die sich lokal authentifizieren, geben Sie den folgenden Befehl an:

```
query node * authentication=local
```

| Knotenname | Plattform | Name der Maßnahmen-domäne | Tage seit letz. Zugr. | Tage seit Kennwortvergabe | Gesperrt? |
|------------|-----------|---------------------------|-----------------------|---------------------------|-----------|
| NODE1      | WinNT     | STANDARD                  | 3                     | 3                         | No        |
| LOCAL      | (?)       | STANDARD                  | 7                     | 7                         | No        |

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für QUERY NODE

| Befehl             | Beschreibung   |
|--------------------|--|
| LOCK NODE          | Verhindert, dass ein Client auf den Server zugreift.   |
| QUERY ADMIN        | Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.                               |
| QUERY REPLNODE     | Zeigt Informationen zum Replikationsstatus eines Clientknotens an.   |
| QUERY STATUS       | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| REGISTER NODE      | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.                              |
| REMOVE NODE        | Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.                     |
| REMOVE REPLNODE    | Entfernt einen Knoten aus der Replikation.   |
| RENAME NODE        | Ändert den Namen eines Clientknotens.  |
| REPLICATE NODE     | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |
| RESET PASSEXP      | Setzt die Kennwortablaufdauer für Knoten oder Administratoren zurück.  |
| SET INVALIDPWLIMIT | Definiert die Anzahl ungültiger Anmeldeversuche, die zulässig sind, bevor ein Knoten gesperrt wird.                  |
| SET MINPWLENGTH    | Legt die Mindestlänge für Clientkennwörter fest.   |
| SET PASSEXP        | Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.                                   |
| UNLOCK NODE        | Ermöglicht einem gesperrten Benutzer in einer bestimmten Maßnahmendomäne wieder den Zugriff auf den Server.          |
| UPDATE NODE        | Ändert die Attribute, die einem Clientknoten zugeordnet sind.  |

## QUERY NODEDATA (Clientdaten auf Datenträgern abfragen)

Verwenden Sie diesen Befehl, um Informationen zu den Daten für einen oder mehrere Knoten in einem Speicherpool mit sequenziellem Zugriff anzuzeigen. QUERY NODEDATA zeigt den Namen des Datenträgers, auf den die Daten eines Knotens geschrieben sind, und den Speicherbereich, der von den Daten auf diesem Datenträger belegt wird. Diese Informationen sind nützlich, wenn bestimmt wird, wie Knoten in zusammengefasste Speicherpools gruppiert werden können.

### Berechtigungsklasse

Einschränkung: Sie können diesen Befehl nicht verwenden, um Informationen für Containerspeicherpools anzuzeigen.

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

      .-,------.
      v           |
>>-Query NODEData-+---Knotenname+-----+----->
                    '-COLLOCGroup----Kollokationsgruppe-'
>--+-----+--+-----+-----+-----<
    '-STGpool----Poolname-'  '-VOLUME----Datenträgername-'

```

### Parameter

Knotenname

Gibt den Namen des Clientknotens an, für den Daten lokalisiert werden sollen. Sie können einen oder mehrere Namen angeben. Werden mehrere Namen angegeben, sind die Namen durch Kommas voneinander zu trennen; verwenden Sie zwischen den Namen keine Leerzeichen. Sie können auch Platzhalterzeichen verwenden, um mehrere Namen anzugeben. Sie müssen entweder einen Knotennamen oder den Namen einer Kollokationsgruppe, aber nicht beide Namen angeben.

#### COLLOCGroup

Gibt den Namen der Kollokationsgruppe an, für die Daten lokalisiert werden sollen. Sie müssen entweder einen Knotennamen oder den Namen einer Kollokationsgruppe, aber nicht beide Namen angeben.

Wichtig: Wenn der Speicherbereich, der für die Ausführung der Abfrage bezüglich einer Kollokationsgruppe erforderlich ist, den SQL-Puffergrenzwert überschreitet, kann der Befehl QUERY NODATA fehlschlagen. Schlägt der Befehl aus diesem Grund fehl, geben Sie den Befehl QUERY COLLOCGROUP aus, um eine Liste der Knoten in der Gruppe anzuzeigen. Geben Sie dann den Befehl QUERY NODATA für jeden Knoten in der Gruppe aus.

#### STGpool

Gibt den Namen des sequenziellen Speicherpools an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Es können Platzhalterzeichen verwendet werden, um die Namen anzugeben. Stimmt ein Platzhalterzeichen mit dem Namen eines Plattenspeicherpools überein, wird der Name des Plattenspeicherpools ignoriert. Wird kein Wert für diesen Parameter angegeben, werden alle sequenziellen Speicherpools abgefragt.

#### VOLUME

Gibt den Datenträger an, der die Daten enthält. Dieser Parameter ist wahlfrei. Es können Platzhalterzeichen verwendet werden, um mehrere Namen anzugeben. Wird kein Wert für diesen Parameter angegeben, werden alle Datenträger in dem Speicherpool abgefragt.

## Platzhalterzeichen verwenden, um Knotendaten für einen Speicherpool mit sequenziellem Zugriff anzuzeigen

Informationen zur Position anzeigen, an der Knotendaten in einem sequenziellen Speicherpool gespeichert sind. Verwenden Sie ein Platzhalterzeichen, um Knotennamen anzugeben. Für Felddesreibungen siehe Felddesreibungen.

```
query nodedata e*
```

| Knotenname | Datenträgername            | Speicherpool-<br>name | Physischer<br>Speicher<br>belegt<br>(MB) |
|------------|----------------------------|-----------------------|--|
| EDU_J2     | E:\tsm\server\00000117.BFS | EDU512                | 0.01                                     |
| EDU_J2     | E:\tsm\server\00000122.BFS | EDU319                | 0.01                                     |
| EDU_J3     | E:\tsm\server\00000116.BFS | EDU512                | 0.01                                     |
| EDU_J3     | E:\tsm\server\00000120.BFS | EDU319                | 0.01                                     |
| EDU_J7     | E:\tsm\server\00000118.BFS | EDU512                | 0.04                                     |
| EDU_J7     | E:\tsm\server\00000123.BFS | EDU319                | 0.04                                     |
| EDU_JJ1    | E:\tsm\server\00000116.BFS | EDU512                | 0.01                                     |
| EDU_JJ1    | E:\tsm\server\00000121.BFS | EDU512                | 0.01                                     |

## Informationen zu Knotendaten für eine bestimmte Kollokationsgruppe anzeigen

Informationen zur Position von Knotendaten in einem sequenziellen Speicherpool für eine bestimmte Kollokationsgruppe anzeigen. In diesem Beispiel sind die Knoten EDU\_J3 und EDU\_JJ1 die einzigen Knoten, die zur Kollokationsgruppe grp1 gehören und Daten in einem Speicherpool mit sequenziellem Zugriff haben.

```
query nodedata collocgroup=grp1
```

| Knotenname | Datenträgername            | Speicherpool-<br>name | Physischer<br>Speicher<br>belegt<br>(MB) |
|------------|----------------------------|-----------------------|--|
| EDU_J3     | E:\tsm\server\00000116.BFS | EDU512                | 0.01                                     |
| EDU_J3     | E:\tsm\server\00000120.BFS | EDU319                | 0.01                                     |
| EDU_JJ1    | E:\tsm\server\00000116.BFS | EDU512                | 0.01                                     |
| EDU_JJ1    | E:\tsm\server\00000121.BFS | EDU512                | 0.01                                     |

Wenn Sie eine Dateibereichskollokationsgruppe angeben, werden nur die Datenträger der Dateibereiche angezeigt, die zu der Kollokationsgruppe gehören. Wenn Sie eine Dateibereichskollokationsgruppe und einen Datenträger angeben, werden die Dateibereiche innerhalb der Kollokationsgruppe, die sich auch auf dem angegebenen Datenträger befinden, angezeigt.

## Felddesreibungen

Knotenname

- Gibt den Namen des Knotens an.
- Datenträgername  
Gibt den Namen des Datenträgers an, der die Knotendaten enthält.
- Speicherpoolname  
Gibt den Namen des Speicherpools an, in dem sich der Datenträger befindet.
- Physischer Speicher belegt (MB)  
Gibt den physischen Speicherbereich an, der von den Knotendaten belegt wird. Der physische Speicherbereich schließt leeren Speicherbereich innerhalb von Aggregaten ein, aus denen Dateien möglicherweise gelöscht oder als verfallen gekennzeichnet wurden.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY NODEDATA

| Befehl              | Beschreibung  |
|---------------------|---|
| DEFINE COLLOGROUP   | Definiert eine Kollokationsgruppe.  |
| DEFINE COLLOCMEMBER | Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.                                     |
| DEFINE STGPOOL      | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.                            |
| DELETE COLLOGROUP   | Löscht eine Kollokationsgruppe.   |
| DELETE COLLOCMEMBER | Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.                                     |
| MOVE NODEDATA       | Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen. |
| QUERY COLLOGROUP    | Zeigt Informationen zu Kollokationsgruppen an.  |
| QUERY NODE          | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.                             |
| QUERY STGPOOL       | Zeigt Informationen zu Speicherpools an.  |
| REMOVE NODE         | Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.              |
| UPDATE COLLOGROUP   | Aktualisiert die Beschreibung einer Kollokationsgruppe.   |
| UPDATE STGPOOL      | Ändert die Attribute eines Speicherpools.   |

## QUERY NODEGROUP (Knotengruppe abfragen)

Verwenden Sie diesen Befehl, um die Knotengruppen anzuzeigen, die auf dem Server definiert sind.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

>>-Query NODEGroup--+-*-----+----->
                        '-Gruppenname-'

.-Format----Standard----.
>-+-----+-----><
  '-Format----+Standard-+-'
    '-Detailed-'

```

### Parameter

Gruppenname

Gibt den Namen der Knotengruppe an, die angezeigt werden soll. Sollen mehrere Namen angegeben werden, ein Platzhalterzeichen verwenden. Dieser Parameter ist wahlfrei. Standardmäßig werden alle Knotengruppen angezeigt.

#### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

#### Standard

Gibt an, dass Teilinformationen angezeigt werden.

#### Detailed

Gibt an, dass die gesamten Informationen angezeigt werden. Um die Knoten in der Knotengruppe anzuzeigen, müssen Sie FORMAT=DETAILED angeben.

## Beispiel: Knotengruppen auf dem Server auflisten

Die Knotengruppen anzeigen, die auf dem Server definiert sind. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query nodegroup
```

| Name der Knotengruppe | Beschreibung der Knotengruppe  |
|-----------------------|--------------------------------|
| DEPT_ED               | Ausbildungsabteilung           |
| GROUP1                | Clientknoten mit geringer Kap. |

## Beispiel: Ausführliche Informationen zu Knotengruppen anzeigen

Vollständige Informationen zu allen Knotengruppen anzeigen und bestimmen, welche Clientknoten zu welchen Knotengruppen gehören. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query nodegroup format=detailed
```

```
Name der Knotengruppe: DEPT_ED
Beschreibung der Knotengruppe: Ausbildungsabteilung
Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
Datum/Zeit der letzten Aktualisierung: 04/21/2006 10:59:03
Knoten in Knotengruppe: EDU_1 EDU_7

Name der Knotengruppe: GROUP1
Beschreibung der Knotengruppe: Clientknoten mit geringer Kap.
Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
Datum/Zeit der letzten Aktualisierung: 04/21/2006 10:59:16
Knoten in Knotengruppe: CHESTER REX NOAH JARED
```

## Feldbeschreibungen

#### Name der Knotengruppe

Der Name der Knotengruppe.

#### Beschreibung der Knotengruppe

Die Beschreibung der Knotengruppe.

#### Letzte Aktualisierung durch (Administrator)

Der Name des Administrators, der die Knotengruppe definiert oder zuletzt aktualisiert hat.

#### Datum/Zeit der letzten Aktualisierung

Das Datum und die Uhrzeit, an dem bzw. zu der ein Administrator die Knotengruppe definiert oder zuletzt aktualisiert hat.

#### Knoten in Knotengruppe

Die Clientknoten in der Knotengruppe.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY NODEGROUP

| Befehl                 | Beschreibung   |
|------------------------|--|
| DEFINE BACKUPSET       | Definiert eine zuvor generierte Sicherungsgruppe für einen Server. |
| DEFINE NODEGROUP       | Definiert eine Gruppe von Knoten.                                  |
| DEFINE NODEGROUPMEMBER | Fügt einer Knotengruppe einen Clientknoten hinzu.                  |
| DELETE BACKUPSET       | Löscht eine Sicherungsgruppe.                                      |
| DELETE NODEGROUP       | Löscht eine Knotengruppe.  |
| DELETE NODEGROUPMEMBER | Löscht einen Clientknoten aus einer Knotengruppe.                  |





Gibt die Einheitenklasse an, die den Einheiten zugeordnet ist, auf denen die Dateibereiche gespeichert sind. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden Speicherpools abgefragt, die einer beliebigen Einheitenklasse zugeordnet sind.

Type

Gibt die Dateitypen an, die in den Dateibereichen abgefragt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Gültige Werte:

ANY

Gibt an, dass alle Typen von Dateien abgefragt werden: Sicherungsversionen von Dateien, archivierte Kopien von Dateien und Dateien, die von IBM Spectrum Protect for Space Management-Clients umgelagert werden.

Backup

Gibt an, daß Sicherungsdateien abgefragt werden.

Archive

Gibt an, daß Archivierungsdateien abgefragt werden.

SPacem

Gibt an, dass speicherverwaltete Dateien (Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden) abgefragt werden.

NAMEType

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unicode-Unterstützung verfügt. Ein Client für Sichern/Archivieren mit Unicode-Unterstützung ist nur für Windows, Macintosh OS 9, Macintosh OS X und NetWare verfügbar. Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen angeben.

Der Standardwert lautet SERVER. Gültige Werte:

SERVER

Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren.

UNICODE

Der Server konvertiert die Dateibereichsnamen aus der Server-Codepage in die Codepage UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in den Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server Probleme beim Zugriff auf die Systemkonvertierungsroutinen hat.

FSID

Der Server interpretiert die Dateibereichsnamen als ihre Dateibereichs-IDs (FSIDs).

CODEType

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben oder wenn Sie keinen Dateibereichsnamen angeben.

Der Standardwert lautet BOTH. Dieser Standardwert bedeutet, dass die Dateibereiche unabhängig von der Art der Zeichenumsetztabelle eingeschlossen werden. Gültige Werte:

UNICODE

Nur Dateibereiche einschließen, die Unicode-fähig sind.

NONUNICODE

Nur Dateibereiche einschließen, die nicht Unicode-fähig sind.

BOTH

Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen.

## Beispiel: Dateibereiche anzeigen, die einem bestimmten Knoten zugeordnet sind

Informationen zum Speicherstandort aller Dateibereiche anzeigen, die dem Knoten DAISY zugeordnet sind. Für Felddesreibungen siehe Felddesreibungen.

```
query occupancy daisy
```

| Knoten-<br>name | Typ  | Dateiber.-<br>Name | FSID | Speicher-<br>pool-<br>name | Anzahl<br>der<br>Dateien | Physischer<br>Speicher<br>belegt<br>(MB) | Logischer<br>Speicher<br>belegt<br>(MB) |
|-----------------|------|--------------------|------|----------------------------|--------------------------|--|---|
| DAISY           | Bkup | DRIVED             | 1    | COPYFILE                   | 38                       | 0,45                                     | 0,42                                    |

## Beispiel: Dateibereiche anzeigen, die einem bestimmten Knoten mit dem Dateityp 'backup' zugeordnet sind

Informationen zu den Dateibereichen anzeigen, die zum Knoten WAYNE gehören und den Dateityp 'backup' haben. Für Felddesreibungen siehe Felddesreibungen.

```
query occupancy wayne type=backup
```

| Knoten-<br>name | Typ  | Dateiber-<br>Name | FSID | Speicher-<br>pool-<br>name | Anzahl<br>der<br>Dateien | Physischer<br>Speicher<br>belegt<br>(MB) | Logischer<br>Speicher<br>belegt<br>(MB) |
|-----------------|------|-------------------|------|----------------------------|--------------------------|--|---|
| WAYNE           | Bkup | DWG1              | 1    | BACKUPPOOL1                | 2.330                    | 53,19                                    | 50,01                                   |
| WAYNE           | Bkup | OS2C              | 2    | BACKUPPOOL1                | 1.554                    | 32,00                                    | 31,30                                   |

## Felddesreibungen

---

### Knotenname

Der Knoten, der Eigner des Dateibereichs ist. Wurde der Knoten zuvor gelöscht, wird der Knotenname DELETED angezeigt.

### Type

Der Datentyp. Gültige Werte:

#### Arch

Daten, die archiviert wurden.

#### Bkup

Daten, die gesichert wurden.

#### SpMg

Daten, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

### Dateibereichsname

Der Name des Dateibereichs, der zu dem Knoten gehört.

Wurde der Dateibereich zuvor gelöscht, wird der Dateibereichsname DELETED angezeigt.

Dateibereichsnamen können eine andere Zeichenumsetzungstabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetzungstabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetzungstabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetzungstabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

### Speicherpoolname

Der Speicherpool, in dem sich der Dateibereich befindet.

### Anzahl Dateien

Die Anzahl der logischen Dateien, die zum Dateibereich gehören und in diesem Speicherpool gespeichert sind. Wird eine Datei mit mehr als 10 GB gespeichert, teilt der Server die Datei in 10-GB-Fragmente auf. Die Anzahl der Fragmente ist ebenfalls in diesem Wert für die Berechnung der Belegung enthalten.

### Belegung des physischen Speichers (MB)

Der physische Speicherbereich, der vom Dateibereich belegt wird. Der physische Speicherbereich schließt leeren Speicherbereich innerhalb von Aggregaten ein, aus denen Dateien möglicherweise gelöscht oder als verfallen gekennzeichnet wurden. Bei diesem Wert ist 1 MB = 1048576 Byte.

Tipp: Dieses Feld zeigt keinen Wert für Speicherpools, die für die Deduplizierung von Daten definiert sind. Wird die Deduplizierung von Daten für einen Speicherpool inaktiviert, wird ein Wert für die physische Belegung erst angezeigt, wenn sich keine deduplizierten Dateien mehr in dem Speicherpool befinden.

### Belegung des logischen Speichers (MB)

Der Speicherbereich, der von logischen Dateien in dem Dateibereich belegt wird. Der logische Speicherbereich ist der Speicherbereich, der tatsächlich zum Speichern von Dateien verwendet wird, ausschließlich des leeren Speicherbereichs innerhalb von Aggregaten. Bei diesem Wert ist 1 MB = 1048576 Byte.

### FSID

Die Dateibereichs-ID (FSID) des Dateibereichs. Der Server ordnet eine eindeutige FSID zu, wenn ein Dateibereich zum ersten Mal auf dem Server gespeichert wird.

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für QUERY OCCUPANCY

| Befehl           | Beschreibung   |
|------------------|--|
| DELETE FILESPACE | Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt. |
| QUERY FILESPACE  | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.  |
| QUERY NODE       | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.  |

## QUERY OPTION (Serveroptionen abfragen)

Mit diesem Befehl können Informationen zu Serveroptionen angezeigt werden.

Die Serveroptionen können durch Editieren der Serveroptionsdatei oder mit dem Befehl SETOPT geändert werden. Wenn die Serveroptionsdatei editiert wird, muss der Server erneut gestartet werden, damit die Änderungen wirksam werden. Alle mit dem Befehl SETOPT vorgenommenen Änderungen werden sofort wirksam.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query OPTion-+-----+-----><
                .-*----- .
                '-Optionsname-'
```

### Parameter

#### Optionsname

Gibt den Namen einer Option in der Serveroptionsdatei an. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Alle übereinstimmenden Serveroptionen werden angezeigt. Wird dieser Parameter nicht angegeben, werden Informationen für alle Optionen angezeigt.

### Beispiel: Alle Serveroptionen anzeigen

Allgemeine Informationen zu allen Serveroptionen anzeigen. Die Ausgabe listet alle Optionen mit ihren angegebenen Werten auf.

```
query option
```

### Beispiel: Optionseinstellungen unter Verwendung eines Platzhalterzeichens anzeigen

Die Optionseinstellungen für alle Optionen anzeigen, die mit L beginnen.

```
query option l*
```

```
Serveroption      Optionswert
-----
Language          AMENG
```

### Beispiel: LDAP-Verzeichnisse anzeigen

Die Einstellungen für alle LDAP-Verzeichnisse anzeigen.

```
query option ldapurl
```

```
Serveroption      Optionswert
-----
LDAP URL          ldap:\\tophoy.tucson.com\cn=tsmdata
LDAP URL          ldap:\\krypton.ibm.com\ou=tsmdata,dc=ibm,dc=com
```

## Feldbeschreibungen

Serveroption  
Gibt den Namen der Option in der Serveroptionsdatei an.

Optionswert  
Gibt den Wert der Option in der Serveroptionsdatei an.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY OPTION

| Befehl | Beschreibung  |
|--------|---|
| SETOPT | Aktualisiert eine Serveroption, ohne den Server zu stoppen und erneut zu starten. |

## QUERY PATH (Pfaddefinition anzeigen)

Verwenden Sie diesen Befehl, um den Pfad zwischen einer Quelle und einem Ziel anzuzeigen.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
.-*-----
>>-Query PATH----->
|               .-*-----|
|'-Quellename-+-----+-'|
|               '-Zielname-'|

.-SRCType---ANY-----
>+-----+----->
|'-SRCType---+ANY-----+|
|               +-DATAMover+
|               '-SERVER----'|

.-DESTType---ANY-----
>+-----+-----+----->
|'-DESTType---+ANY-----+|
|               +-DRIVE--LIBRARY---Kassettenarchivname-+
|               '-LIBRARY-----'|

.-Format----Standard----
>+-----+-----><
|'-Format----+Standard-+|
|               '-Detailed-|
```

## Parameter

### Quellenname

Gibt den Namen einer Quelle an, für die Pfade angezeigt werden sollen. Dieser Parameter ist wahlfrei. Sie können Platzhalterzeichen angeben. Standardmäßig werden Pfade für alle Quellen angezeigt.

Eine Quelle ist eine Einheit zum Versetzen von Daten, ein Server oder ein Speicheragent.

### Zielname

Gibt den Namen eines Ziels an, für das Pfade angezeigt werden sollen. Dieser Parameter ist wahlfrei. Sie können Platzhalterzeichen angeben. Standardmäßig werden Pfade für alle Ziele angezeigt.

### SRCType

Gibt den Typ der Quelle an. Dieser Parameter ist wahlfrei. Standardmäßig werden Pfade für alle Quellentypen angezeigt. Gültige Werte:

#### ANY

Gibt an, dass Pfade mit einem beliebigen Quellentyp angezeigt werden sollen.

#### DATAMover

Gibt an, dass nur Pfade mit dem Quellentyp DATAMOVER angezeigt werden sollen.

**SERVer**

Gibt an, dass nur Pfade mit dem Quellentyp SERVER angezeigt werden sollen. (Eine Quelle, die den Quellentyp SERVER hat, ist ein Speicheragent.)

**DESTType**

Gibt den Typ des Ziels an. Dieser Parameter ist wahlfrei. Standardmäßig werden Pfade für alle Zieltypen angezeigt. Gültige Werte:

**ANY**

Gibt an, dass Pfade mit einem beliebigen Zieltyp angezeigt werden sollen.

**DRive**

Gibt an, dass nur Pfade mit dem Zieltyp DRIVE angezeigt werden sollen. Ist der Zieltyp ein Laufwerk, müssen Sie den Kassettenarchivnamen angeben. Durch die Eingabe eines Namens in dem Parameter LIBRARY können Sie genauer spezifizieren, welche Pfade angezeigt werden.

**LIBRARY**

Gibt an, dass nur Pfade mit dem Zieltyp LIBRARY angezeigt werden.

**LIBRARY**

Gibt den Namen des Kassettenarchivs an, zu dem das Laufwerk gehört. Dieser Parameter ist erforderlich, wenn der Zieltyp ein Laufwerk ist (DESTTYPE=DRIVE).

**Format**

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

**Standard**

Gibt an, dass Teilinformationen angezeigt werden.

**Detailed**

Gibt an, dass die gesamten Informationen angezeigt werden.

## Beispiel: Übersichtsdaten zu Pfaden anzeigen

Informationen zu Pfaden für die Quelle NETAPP1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query path netapp1
```

| Quellenname | Quellentyp | Zielname | Zieltyp | Online |
|-------------|------------|----------|---------|--------|
| NETAPP1     | DATAMOVER  | DRIVE1   | DRIVE   | Yes    |
| NETAPP1     | DATAMOVER  | NASLIB   | LIBRARY | Yes    |

## Beispiel: Ausführliche Informationen zu Pfaden anzeigen

Ausführliche Informationen zu Pfaden für die Quelle NETAPP1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query path netapp1 format=detailed
```

 Linux-Betriebssysteme

```
Quellenname: NETAPP1
Quellentyp: DATAMOVER
Zielname: NASLIB
Zieltyp: LIBRARY
Kassettenarchiv:
  Einheit: /dev/tmsmcsi/mc0
Verzeichnis:
  Online: Yes
Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
Datum/Zeit der letzten Aktualisierung: 06/21/2002 20:52:56
```

```
Quellenname: NETAPP1
Quellentyp: DATAMOVER
Zielname: DRIVE1
Zieltyp: DRIVE
Kassettenarchiv: NASLIB
  Einheit: rst01
Verzeichnis:
  Online: Yes
Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
Datum/Zeit der letzten Aktualisierung: 06/21/2002 20:55:23
```

 AIX-Betriebssysteme  Windows-Betriebssysteme

```
Quellenname: NETAPP1
Quellentyp: DATAMOVER
Zielname: NASLIB
Zieltyp: LIBRARY
Kassettenarchiv:
Einheit: mc0
Verzeichnis:
Online: Yes
Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
Datum/Zeit der letzten Aktualisierung: 06/21/2001 20:52:56
```

```
Quellenname: NETAPP1
Quellentyp: DATAMOVER
Zielname: DRIVE1
Zieltyp: DRIVE
Kassettenarchiv: NASLIB
Einheit: rst01
Verzeichnis:
Online: Yes
Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
Datum/Zeit der letzten Aktualisierung: 06/21/2001 20:55:23
```

## Beispiel: Ausführliche Informationen zu Pfaden für einen z/OS Media-Server anzeigen

---

Ausführliche Informationen zu einem Pfad für einen z/OS Media-Server anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query path format=detailed
```

```
Quellenname: SERVER1
Quellentyp: SERVER
Zielname: ZOSMEDIA
Zieltyp: LIBRARY
Kassettenarchiv:
Knotenname:
Einheit:
Externer Manager:
z/OS Media-Server: MEDSERV1
Übertragungsmethode:
LUN:
Initiator: 0
Verzeichnis:
Online: Yes
Letzte Aktualisierung durch (Administrator): ADMIN
Datum/Zeit der letzten Aktualisierung: 06/08/2011 15:33:39
```

## Feldbeschreibungen

---

### Quellenname

Der Name der Quelle.

### Zielname

Der Name des Ziels.

### Quellentyp

Der Typ der Quelle.

### Zieltyp

Der Typ des Ziels.

### Kassettenarchiv

Der Name des Kassettenarchivs, das das Laufwerk als Ziel enthält.

Dieses Feld ist leer, wenn der Zieltyp ein Kassettenarchiv ist. Der Kassettenarchivname befindet sich im Feld für den Zielnamen, wenn das Ziel ein Kassettenarchiv ist.

### Knotenname

Der Name der Einheit, die das Ziel ist.

### Einheit

Der Name der Einheit, die das Ziel ist.

### Externer Manager

Der Name des externen Managers.

### z/OS Media-Server

Der Name des z/OS Media-Servers.

### Übertragungsmethode

- Gibt den Typ der Übertragungsmethode an.
- LUN  
Gibt den Namen der logischen Einheit an, über den von der Quelle auf die Platte zugegriffen werden kann.
- Initiator  
Gibt den Initiator der Übertragung an.
- Verzeichnis  
Gibt die Verzeichnisposition einer Datei in der Quelle an.
- Online  
Gibt an, ob der Pfad online und für die Verwendung verfügbar ist.
- Letzte Aktualisierung durch (Administrator)  
Die ID des Administrators, der die letzte Aktualisierung ausgeführt hat.
- Datum/Zeit der letzten Aktualisierung  
Das Datum und die Uhrzeit der letzten Aktualisierung.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY PATH

| Befehl      | Beschreibung   |
|-------------|--|
| DEFINE PATH | Definiert einen Pfad von einer Quelle zu einem Ziel. |
| DELETE PATH | Löscht einen Pfad von einer Quelle zu einem Ziel.    |
| UPDATE PATH | Ändert die zu einem Pfad gehörigen Attribute.        |

## QUERY POLICYSET (Maßnahmengruppe abfragen)

Mit diesem Befehl können Informationen über eine oder mehrere Maßnahmengruppen angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query Policyset----->
. -* - * ----- .
>--+-----+----->
|          . -* - * ----- . |
|'-Domänenname--+-----+-'|
|          '-Name_der_Maßnahmengruppe-'|
. -Format-----Standard----- .
>--+-----+-----><
|'-Format-----+Standard--+-'|
|          '-Detailed-'|
```

### Parameter

#### Domänenname

Gibt die Maßnahmendomäne an, die der Maßnahmengruppe zugeordnet ist, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Maßnahmendomänen abgefragt. Dieser Parameter muß angegeben werden, wenn eine explizit benannte Maßnahmengruppe abgefragt wird.

#### Name\_der\_Maßnahmengruppe

Gibt die Maßnahmengruppe an, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird nicht ACTIVE oder der Name einer Maßnahmengruppe angegeben, werden alle Maßnahmengruppen abgefragt.

#### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

Standard

Gibt an, dass Teilmformationen angezeigt werden.

Detailed



Gibt an, dass die gesamten Informationen angezeigt werden.

## Beispiel: Die Maßnahmengruppen für alle Maßnahmendomänen auflisten

---

Alle Maßnahmengruppen für alle Maßnahmendomänen abfragen. Die Ausgabe soll im Standardformat erstellt werden. Für Felddesreibungen siehe Felddesreibungen.

```
query policyset
```

| Name der Maßnahmendomäne | Name der Maßnahmengruppe | Standardverwaltungs-klasse | Beschreibung                  |
|--------------------------|--------------------------|----------------------------|-------------------------------|
| EMPLOYEE-RECORDS         | ACTIVE                   | ACTIVEFILES                | Personnel Department          |
| EMPLOYEE-RECORDS         | HOLIDAY                  | ACTIVEFILES                | Personnel Department          |
| EMPLOYEE-RECORDS         | VACATION                 | ACTIVEFILES                | Personnel Department          |
| PROG1                    | SUMMER                   |                            | Programming Group Policies    |
| PROG2                    | SUMMER                   |                            | Programming Group Policies    |
| STANDARD                 | ACTIVE                   | STANDARD                   | Installed default policy set. |
| STANDARD                 | STANDARD                 | STANDARD                   | Installed default policy set. |

## Beispiel: Ausführliche Informationen zu einer bestimmten Maßnahmengruppe anzeigen

---

Die Maßnahmengruppe VACATION abfragen, die sich in der Maßnahmendomäne EMPLOYEE\_RECORDS befindet. Die Ausgabe soll im ausführlichen Format erstellt werden. Für Felddesreibungen siehe Felddesreibungen.

```
query policyset employee_records vacation  
format=detailed
```

```
          Name der Maßnahmendomäne: EMPLOYEE_RECORDS  
          Name der Maßnahmengruppe: VACATION  
          Standardverwaltungs-klasse: ACTIVEFILES  
          Beschreibung: Personnel Department  
          Letzte Aktualisierung durch  
          (Administrator): $$CONFIG_MANAGER$$  
          Datum/Zeit der letzten Aktualisierung: 05/31/1998 13:15:50  
          Verwaltendes Profil: ADSM_INFO  
          Änderungen anstehend: Yes
```

## Felddesreibungen

---

Name der Maßnahmendomäne

Der Name der Maßnahmendomäne.

Name der Maßnahmengruppe

Der Name der Maßnahmengruppe.

Standardverwaltungs-klasse

Die Verwaltungs-klasse, die der Maßnahmengruppe standardmäßig zugeordnet ist.

Beschreibung

Die Beschreibung der Maßnahmengruppe.

Letzte Aktualisierung durch (Administrator)

Der Name des Administrators oder Servers, der die Maßnahmengruppe zuletzt aktualisiert hat. Enthält dieses Feld

\$\$CONFIG\_MANAGER\$\$, ist die Maßnahmengruppe einer Domäne zugeordnet, die von dem Konfigurationsmanager verwaltet wird.

Datum/Zeit der letzten Aktualisierung

Das Datum und die Uhrzeit, an dem bzw. zu der die Maßnahmengruppe definiert oder zuletzt aktualisiert wurde.

Verwaltendes Profil

Das Profil oder die Profile, die die Domäne verwalten, zu der diese Maßnahmengruppe gehört.

Änderungen anstehend

Angabe, ob Änderungen vorgenommen, aber nicht aktiviert werden. Sobald die Änderungen aktiviert werden, wird das Feld auf No zurückgesetzt.

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für QUERY POLICYSET

| Befehl             | Beschreibung  |
|--------------------|---|
| ACTIVATE POLICYSET | Wertet eine Maßnahmengruppe aus und aktiviert sie.  |
| COPY POLICYSET     | Erstellt eine Kopie einer Maßnahmengruppe.  |
| DEFINE POLICYSET   | Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.   |
| DELETE POLICYSET   | Löscht eine Maßnahmengruppe einschließlich ihrer Verwaltungsklassen und Kopiengruppen aus einer Maßnahmendomäne.        |
| QUERY DOMAIN       | Zeigt Informationen über Maßnahmendomänen an.   |
| UPDATE POLICYSET   | Ändert die Beschreibung einer Maßnahmengruppe.  |
| VALIDATE POLICYSET | Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert. |

## QUERY PROCESS (Serverprozesse abfragen)

Mit diesem Befehl können Informationen zu aktiven Hintergrundprozessen angezeigt werden.

Geben Sie den Befehl CANCEL PROCESS aus, um Hintergrundprozesse abzubrechen. Um ausführliche Informationen zu Knotenreplikationsprozessen anzuzeigen, geben Sie den Befehl QUERY REPLICATION aus.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query PRocess--+-----+----->
                    '-Prozessnummer-'
>--+-----+----->
    '-DESCRiption----Zeichenfolge-'
>--+-----+-----<
    '-STATus----Zeichenfolge-'
```

### Parameter

#### Prozessnummer

Gibt die Nummer des Hintergrundprozesses an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Wird keine Prozessnummer angegeben, werden Informationen zu allen Hintergrundprozessen angezeigt.

#### DESCRiption

Gibt eine Textzeichenfolge an, nach der in der Liste der Beschreibungen von aktiven Prozessen gesucht werden soll. Die Zeichenfolge in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Sie können Text und ein Platzhalterzeichen verwenden, um diese Zeichenfolge anzugeben. Dieser Parameter ist wahlfrei.

#### STATus

Gibt eine Textzeichenfolge an, nach der in der Liste der Status von aktiven Prozessen gesucht werden soll. Die Zeichenfolge in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Sie können Text und ein Platzhalterzeichen verwenden, um diese Zeichenfolge anzugeben. Dieser Parameter ist wahlfrei.

### Beispiel: Einen einzelnen Hintergrundprozess abfragen

Informationen zu Hintergrundprozess 202 anzeigen. Für Felddescriptions siehe Felddescriptions.

```
query process 202
```

```
Prozess-  Prozess-      Prozess-
nummer   beschreibung      status
-----  -
      202  EXPORT SERVER      ANRÖNNNI EXPORT-
                                ID MYEXPORTSERVER
```

```

ANR0648I Folgendes wurde
kopiert: 8 Domänen 2
Maßnahmengruppen, 10
Verwaltungsklassen, 4
Kopiengruppen, 1 Admi-
nistrator 746 Byte
(0 Fehler erkannt) Akt. Eingabe-
datenträger: C:\BUILD\540\
GA\BUILD\NT\I386\DEBUG\
-00000014.BFS, (6 Sekunden)

```

## Beispiel: Alle Hintergrundprozesse abfragen

---

Informationen zu allen Hintergrundprozessen anzeigen. Für Felddescriptions siehe Felddescriptions.

```
query process
```

| Prozess-<br>nummer | Prozess-<br>beschreibung | Prozess-<br>status   |
|--------------------|--------------------------|--|
| 304                | IDENTIFY DUPLICATES      | Speicherpool<br>FILEPOOL, Datenträger<br>/tsmpool2/00006664.<br>BFS, Verarbeitete Dateien:<br>2000, Doppelte Erweiterungen<br>gefunden: 344, Doppelte<br>Byte gefunden: 3.238.123,<br>Aktuelle physische Datei<br>(Byte): 2.626.676.296.<br>Status: Wird verarbeitet   |
| 284                | IDENTIFY DUPLICATES      | Speicherpool<br>FILEPOOL, Datenträger<br>/tsmpool2/00006666.<br>BFS, Verarbeitete Dateien:<br>2000, Doppelte Erweiterungen<br>gefunden: 344, Doppelte<br>Byte gefunden: 3.238.123,<br>Aktuelle physische Datei<br>(Byte): Keine.<br>Status: Inaktiv  |
| 4                  | Replicate Node           | Replizieren von Knoten IRONMAN.<br>Abgeschlossene Dateibereiche: 0.<br>Identifizieren und Replizieren<br>von Dateibereichen: 1. Replizieren<br>von Dateibereichen: 0. Nicht gestartete<br>Dateibereiche: 3. Aktuelle Dateien:<br>11.920. Replizierte Dateien: 0 von<br>0. Aktualisierte Dateien: 0 von 0.<br>Gelöschte Dateien: 0 von 0. Repliziertes<br>Volumen: 11.482 KB von 11.482 KB.<br>Übertragenes Volumen: 11.482 KB.<br>Abgelaufene Zeit: 0 Tag(e), 0 Stunde(n),<br>1 Minute(n). |
| 37                 | Expiration               | 12 Knoten von insgesamt 30 Knoten verarbeitet,<br>411 Objekte geprüft,<br>411 Sicherungsobjekte,<br>0 Archivierungsobjekte,<br>0 DB-Sicherungsdatenträger,<br>0 Wiederherstellungsplandateien werden gelöscht;<br>Die Verarbeitung von 0 Objekten wurde wiederholt und<br>0 Fehler wurden gefunden.  |

## Beispiel: Alle Hintergrundreplikationsprozesse abfragen

---

Informationen zu allen Hintergrundreplikationsprozessen anzeigen. Für Felddescriptions siehe Felddescriptions.

```
query process desc="replicate node"
```

| Prozess-<br>nummer | Prozess-<br>beschreibung | Prozess-<br>status  |
|--------------------|--------------------------|---|
| 4                  | Replicate Node           | Replizieren von Knoten IRONMAN.<br>Abgeschlossene Dateibereiche: 0. |

```

Identifizieren und Replizieren
von Dateibereichen: 1. Replizieren
von Dateibereichen: 0. Nicht gestartete
Dateibereiche: 3. Aktuelle Dateien:
11.920. Replizierte Dateien: 0 von
0. Aktualisierte Dateien: 0 von 0.
Gelöschte Dateien: 0 von 0. Repliziertes
Volumen: 11.482 KB von 11.482 KB.
Übertragenes Volumen: 11.482 KB.
Abgelaufene Zeit: 0 Tag(e), 0 Stunde(n),
1 Minute(n) .

```

## Beispiel: Alle Hintergrundreplikationsprozesse für einen bestimmten Knoten abfragen

Informationen zu allen Hintergrundreplikationsprozessen anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query process desc="replicate node" status=ironman
```

| Prozess-<br>nummer | Prozess-<br>beschreibung | Prozess-<br>status  |
|--------------------|--------------------------|---|
| 4                  | Replicate Node           | Replizieren von Knoten IRONMAN.<br>Abgeschlossene Dateibereiche: 0.<br>Identifizieren und Replizieren<br>von Dateibereichen: 1. Replizieren<br>von Dateibereichen: 0. Nicht gestartete<br>Dateibereiche: 3. Aktuelle Dateien:<br>11.920. Replizierte Dateien: 0 von<br>0. Aktualisierte Dateien: 0 von 0.<br>Gelöschte Dateien: 0 von 0. Repliziertes<br>Volumen: 11.482 KB von 11.482 KB.<br>Übertragenes Volumen: 11.482 KB.<br>Abgelaufene Zeit: 0 Tag(e), 0 Stunde(n),<br>1 Minute(n) . |

## Beispiel: Prüfen, ob ein Replikationswiederherstellungsprozess eingeleitet wurde

Prüfen Sie nach dem Start eines Knotenreplikationsprozesses mit aktivierter Dateiwiederherstellung, ob der Zielreplikationsserver den Dateiwiederherstellungsprozess eingeleitet hat. Geben Sie den Befehl QUERY PROCESS auf dem Zielreplikationsserver aus. Beschreibungen der Felder befinden sich in Feldbeschreibungen.

```
query process
```

| Prozess-<br>nummer | Prozess-<br>beschreibung     | Prozess-<br>status  |
|--------------------|------------------------------|---|
| 4                  | Replicate Node -<br>Recovery | Replizieren von Knoten 3MAUTOIMPORT.<br>Abgeschlossene Dateibereiche: 87.<br>Identifizieren und Replizieren von<br>Dateibereichen: 0.<br>Replizieren von Dateibereichen: 6.<br>Nicht gestartete Dateibereiche: 0.<br>Aktuelle Dateien: 0.<br>Replizierte Dateien: 0 von 14.<br>Aktualisierte Dateien: 0 von 0.<br>Gelöschte Dateien: 0 von 0. Repliziertes<br>Volumen: 0 KB von 11.688 Byte. Übertragenes<br>Volumen: 0 KB. Abgelaufene Zeit:<br>0 Tag(e), 0 Stunde(n), 1 Minute(n) . |



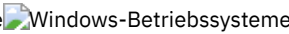
## Beispiel: Prüfen, ob beschädigte Dateien während eines Replikationsprozesses wiederhergestellt werden

Prüfen Sie nach dem Start eines Knotenreplikationsprozesses mit aktivierter Dateiwiederherstellung, ob beschädigte Dateien wiederhergestellt werden. Geben Sie den Befehl QUERY PROCESS auf dem Quellenreplikationsserver aus. Beschreibungen der Felder befinden sich in Feldbeschreibungen.

```
query process
```

| Prozess-<br>nummer | Prozess-<br>beschreibung | Prozess-<br>status                    |
|--------------------|--------------------------|---------------------------------------|
| 6                  | Replicate Node           | Wiederherstellen beschädigter Dateien |

( As Secondary Recovery ) von Server SERVER2, Prozess 4, Anzahl aktiver Sitzungen 10.

## Beispiel: Prüfen, ob die Dateien konvertiert werden

Prüfen Sie nach dem Start eines Speicherpoolkonvertierungsprozesses, ob die Dateien konvertiert werden. Beschreibungen der Felder befinden sich in Felddescriptions.

```
query process
```

| Prozess-<br>nummer | Prozess-<br>beschreibung | Prozess-<br>status  |
|--------------------|--------------------------|---|
| 6                  | Convert Stgpool          | Speicherpool FILEPOOL1 wird in Verzeichniscontainer-<br>speicherpool NEWDEDUP1 konvertiert. Konvertierte<br>Datenträger: 1 von 6, Fehlgeschlagene Datenträger: 0,<br>Konvertierte Dateien: 975, Konvertierte Byte: 196,27 MB,<br>Übersprungene Dateien: 0, Übersprungene Byte: 0 B,<br>Summe übertragener Byte: 151,27 MB   |
| 7                  | Convert Stgpool          | Speicherpool DEDUPPOOL wird in Verzeichniscontainer-<br>speicherpool DIRPOOL konvertiert. Konvertierte<br>Dateien: 150 von 360, Konvertierte Byte: 79.598 KB<br>von 388 MB. Nicht konvertierte Dateien: 12.<br>Nicht konvertierte Byte: 27 MB. Aktueller Eingabe-<br>datenträger: /fvt/srv/BK01. Abgelaufene Zeit: 0 Tag(e),<br>0 Stunde(n), 1 Minute(n).                           |
| 8                  | Convert Stgpool          | Speicherpool FILEPOOL1 wird in Verzeichniscontainer-<br>speicherpool NEWDEDUP1 konvertiert. Konvertierte<br>Dateien: 0, Konvertierte Byte: 0 B von 1,00 GB,<br>Übersprungene Dateien: 0, Übersprungene Byte: 0 B,<br>Summe übertragener Byte: 0 B, Aktueller Eingabe-<br>datenträger: /STORAGE/file1/00000005.BFS,<br>Abgelaufene Zeit: 0 Tage, 0 Stunden, 1 Minute.                |
| 10                 | Convert Stgpool          | Speicherpool FILEPOOL1 wird in Verzeichniscontainer-<br>speicherpool NEWDEDUP1 konvertiert. Konvertierte<br>Dateien: 1007, Konvertierte Byte: 285,44 MB von 1,33 GB,<br>Übersprungene Dateien: 0, Übersprungene Byte: 0 B,<br>Summe übertragener Byte: 196,28 MB, Aktueller Eingabe-<br>datenträger: /STORAGE/file1/00000004.BFS,<br>Abgelaufene Zeit: 0 Tage, 0 Stunden, 1 Minute. |

## Beispiel: Versetzung von der lokalen Platte in die Cloud prüfen

Nach dem Start der Datenübertragung von der lokalen Platte in die Cloud prüfen, ob die Daten versetzt werden. Beschreibungen der Felder befinden sich in Felddescriptions.

```
query process
```

| Prozess-<br>nummer | Prozess-<br>beschreibung                     | Prozess-<br>status   |
|--------------------|--|--|
| 4                  | Übertragung von lokaler<br>Platte nach Cloud | Übertragung von lokaler Platte nach Cloud<br>für Verzeichniscontainerspeicherpool CLOUDPOOL.<br>1 Container verarbeitet. 2.100 KB in 4 Datenbereichen<br>übertragen.<br>Abgelaufene Zeit: 0 Tag(e), 0 Stunde(n),<br>1 Minute(n). |

## Felddescriptions

Prozessnummer

Gibt die Nummer an, die dem aktiven Hintergrundprozess zugeordnet ist.

Prozessbeschreibung

Gibt eine Beschreibung des aktiven Hintergrundprozesses an.

Prozessstatus

Gibt den Status des aktiven Hintergrundprozesses an.

Tipp: Wenn ein Knotenreplikationsprozess auf dem Zielreplikationsserver beendet wird, werden nur Informationen zur Prozessbeendigung in der Aktivitätsübersichtstabelle gespeichert. Die vollständige Übersicht für den Replikationsprozess wird in der Aktivitätsübersichtstabelle auf dem Quellenreplikationsserver gespeichert.

## Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für QUERY PROCESS

| Befehl              | Beschreibung   |
|---------------------|--|
| CANCEL EXPORT       | Löscht eine ausgesetzte Exportoperation.                               |
| CANCEL PROCESS      | Bricht einen Serverhintergrundprozess ab.                              |
| IDENTIFY DUPLICATES | Identifiziert doppelte Daten in einem Speicherpool.                    |
| QUERY EXPORT        | Zeigt die Exportoperationen an, die gerade aktiv oder ausgesetzt sind. |
| QUERY REPLICATION   | Zeigt Informationen zu Knotenreplikationsprozessen an.                 |
| QUERY REPLNODE      | Zeigt Informationen zum Replikationsstatus eines Clientknotens an.     |
| RESTART EXPORT      | Startet eine ausgesetzte Exportoperation erneut.                       |
| SUSPEND EXPORT      | Setzt eine aktive Exportoperation aus.                                 |

## QUERY PROFILE (Profil abfragen)

Mit diesem Befehl können Informationen über Profile und zugeordnete Objekte angezeigt werden. Geben Sie diesen Befehl von einem Konfigurationsmanager oder von einem verwalteten Server aus. Mit diesem Befehl können Profilinformationen von jedem Konfigurationsmanager abgerufen werden, der für den Server definiert ist, auch wenn der Server für kein Profil subskribiert.

Wird ein gesperrtes Profil von dem Konfigurationsmanager abgefragt, zu dem das Profil gehört, werden vollständige Profilinformationen angezeigt. Wird ein gesperrtes Profil von einem anderen Server abgefragt, zeigt die Abfrage nur an, daß das Profil gesperrt ist.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
.-*-----.  
>>-Query PROFILE----->  
      '-Profilname-'  
  
      .-Format---Standard----.  
>----->  
      | (1) | '-Format---Standard--+'  
      '-SERVER---Servername-----'      '-Detailed-'  
  
      .-USELocal---Yes-----.  
>-----<  
      '-USELocal---+Yes+-'  
      '-No--'
```

Anmerkungen:

1. Der angegebene Servername hängt von dem Server ab, von dem aus der Befehl ausgegeben wird. Siehe die Beschreibung des Parameters SERVER.

## Parameter

Profilname

Gibt das Profil an, das angezeigt werden soll. Sollen mehrere Namen angegeben werden, ein Platzhalterzeichen verwenden. Dieser Parameter ist wahlfrei. Standardmäßig werden alle Profile angezeigt.

## SERVer

Gibt den Konfigurationsmanager an, dessen Profilinformationen angezeigt werden. Die Anforderungen für den Namen sind davon abhängig, wo die Abfrage ausgegeben wird:

- Von einem Konfigurationsmanager: Dieser Parameter ist wahlfrei. Der Standardwert ist der Name des Konfigurationsmanagers.
- Von einem verwalteten Server: Dieser Parameter ist wahlfrei. Der Standardwert ist der Name des Konfigurationsmanagers für diesen verwalteten Server.
- Von einem Server, der weder ein Konfigurationsmanager noch ein verwalteter Server ist: Sie müssen einen Namen angeben.

## Format

Gibt an, ob Teilinformationen oder ausführliche Informationen angezeigt werden. Der Standardwert ist STANDARD. Gültige Werte:

### Standard

Gibt an, dass Teilinformationen angezeigt werden.

### Detailed

Gibt an, dass ausführliche Informationen angezeigt werden.

## USELocal

Wird die Abfrage von einem verwalteten Server ausgeführt, gibt dieser Parameter an, ob die Profilinformationen von dem Konfigurationsmanager oder dem verwalteten Server abgerufen werden. Sind die Profilinformationen auf dem verwalteten Server nicht vorhanden, werden die Informationen unabhängig von dem Wert dieses Parameters von dem Konfigurationsmanager abgerufen.

Wenn dieser Parameter auf einem Server verwendet wird, der nicht durch den Konfigurationsmanager verwaltet wird, der Eigner des Profils ist, wird der Parameter ignoriert. Der Standardwert ist YES. Gültige Werte:

### Yes

Gibt an, dass die Profilinformationen, falls verfügbar, vom verwalteten Server abgerufen werden. Sind keine Informationen von dem verwalteten Server verfügbar, wird Kontakt mit dem Konfigurationsmanager aufgenommen.

### No

Gibt an, dass die Profilinformationen von dem Konfigurationsmanager abgerufen werden, auch wenn die Informationen auf dem verwalteten Server verfügbar sind. Damit wird sichergestellt, daß aktuelle Informationen über das Profil empfangen werden.

## Beispiel: Profile von einem Konfigurationsmanager auflisten

Profilinformationen von einem Konfigurationsmanager anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query profile
```

| Konfigurations-<br>manager----- | Profilname<br>----- | Gesperrt?<br>----- |
|---------------------------------|---------------------|--------------------|
| SERVER1                         | DEFAULT_PROFILE     | No                 |
| SERVER1                         | ADMIN_INFO          | No                 |
| SERVER1                         | EMPLOYEE            | No                 |
| SERVER1                         | PERSONNEL           | Yes                |

## Beispiel: Ausführliche Profilinformationen für einen verwalteten Server anzeigen

Von einem verwalteten Server aktuelle ausführliche Informationen über das Profil ADMIN\_INFO anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

Anmerkung: Ist das Profil gesperrt, werden die meisten Felder nicht angezeigt.

```
query profile admin_info  
format=detailed uselocal=no
```

```
      Konfigurationsmanager: SERVER1  
          Profilname: ADMIN_INFO  
          Gesperrt: No  
      Beschreibung: Distributed admin. schedules  
Server-Administratoren: DENNIS EMILY ANDREA  
      Maßnahmendomänen: ADMIN RECORDS  
Zeitpläne für Verwaltungsbefehle: ** alle Objekte **  
Server-Befehlsprozeduren:  
Client-Optionsgruppen:  
      Server:  
      Server-Gruppen:
```

## Feldbeschreibungen

|                                  |  |
|----------------------------------|--|
| Konfigurationsmanager            | Der Name des Konfigurationsmanagers, der Eigner des Profils ist. |
| Profilname                       | Der Name des Profils.  |
| Gesperrt?                        | Angabe, ob das Profil gesperrt ist.                              |
| Beschreibung                     | Die Beschreibung des Profils.                                    |
| Server-Administratoren           | Die Administratoren, die dem Profil zugeordnet sind.             |
| Maßnahmendomänen                 | Die Maßnahmendomänen, die dem Profil zugeordnet sind.            |
| Zeitpläne für Verwaltungsbefehle | Die Verwaltungszeitpläne, die dem Profil zugeordnet sind.        |
| Server-Befehlsprozeduren         | Die Server-Befehlsprozeduren, die dem Profil zugeordnet sind.    |
| Client-Optionsgruppen            | Die Client-Optionsgruppen, die dem Profil zugeordnet sind.       |
| Server                           | Die Server, die dem Profil zugeordnet sind.                      |
| Server-Gruppen                   | Die Namen der Server-Gruppen, die dem Profil zugeordnet sind.    |

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY PROFILE

| Befehl                 | Beschreibung  |
|------------------------|---|
| COPY PROFILE           | Erstellt eine Kopie eines Profils.  |
| DEFINE PROFASSOCIATION | Ordnet Objekte einem Profil zu.   |
| DEFINE PROFILE         | Definiert ein Profil für die Verteilung von Informationen an verwaltete Server. |
| DEFINE SUBSCRIPTION    | Subskribiert einen verwalteten Server für ein Profil.                           |
| DELETE PROFASSOCIATION | Löscht die Zuordnung zwischen einem Objekt und einem Profil.                    |
| DELETE PROFILE         | Löscht ein Profil aus einem Konfigurationsmanager.                              |
| LOCK PROFILE           | Verhindert die Verteilung eines Konfigurationsprofils.                          |
| SET CONFIGMANAGER      | Gibt an, ob ein Server ein Konfigurationsmanager ist.                           |
| UNLOCK PROFILE         | Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server.        |
| UPDATE PROFILE         | Ändert die Beschreibung eines Profils.  |

## QUERY PROTECTSTATUS (Status des Speicherpoolschutzes abfragen)

Mit diesem Befehl können Informationen zum Status des Speicherpoolschutzes für Verzeichniscontainerspeicherpools angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
.-*-----.  
>>-Query PROTECTStatus----->  
      '-Poolname-'  
.-Format-----Standard-----.
```



```
>--+-----+-----><
  '-Format-----+Standard--+'
        '-Detailed-'
```

## Parameter

### Poolname

Gibt den Namen des Verzeichniscontainerspeicherpools an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert angegeben, wird der Status aller Verzeichniscontainerspeicherpools angezeigt.

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Geben Sie einen der folgenden Werte an:

#### Standard

Gibt an, dass Teilinformationen angezeigt werden.

#### Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

## Beispiel: Übersichtsdaten zu einem bestimmten Speicherpool anzeigen

Informationen zum Speicherpool mit dem Namen POOL1 anzeigen. Den folgenden Befehl ausgeben:

```
query protectstatus pool1
```

| Name des Quellenservers | Quellenspeicherpool | Name des Zielservers | Zielspeicherpool | Prozent geschützt | Letzter ausgeführter Schutz |
|-------------------------|---------------------|----------------------|------------------|-------------------|-----------------------------|
| NEXT                    | POOL1               | NEXT                 | POOL1COPY        | 96,55             | 02/17/2017 11:15:07         |
| NEXT                    | POOL1               | NEXT1                | POOL2            | 99,99             | 02/17/2017 11:14:53         |
| NEXT                    | POOL1               | UNKNOWN              | UNKNOWN          | UNKNOWN           | 02/17/2017 11:13:44         |
| NEXT1                   | POOL2               | NEXT                 | POOL1            | 100,00            | 02/17/2017 12:56:58         |

Für Felddesreibungen siehe Felddesreibungen.

## Beispiel: Ausführliche Informationen zu einem bestimmten Speicherpool anzeigen

Ausführliche Informationen zum Speicherpool mit dem Namen POOL1 anzeigen. Den folgenden Befehl ausgeben:

```
query protectstatus pool1 format=detailed
```

```
Name des Quellenservers: NEXT
      Quellenspeicherpool: POOL1
      Name des Zielservers: NEXT
      Zielspeicherpool: POOL1COPY
      Prozent geschützt: 96,55
      Geschützte Datenbereiche: 1.747
      Gesamtzahl der Datenbereiche: 1.852
      Geschützte MB: 165,33
      Gesamtzahl MB: 171,23
      Letzter ausgeführter Schutz: 02/17/2017 11:15:07
      Datum/Zeit der letzten Aktualisierung: 02/19/2017 00:27:12
```

Für Felddesreibungen siehe Felddesreibungen.

## Felddesreibungen

### Name des Quellenservers

Der Name des Quellenservers.

### Quellenspeicherpool

Der Name des Verzeichniscontainerspeicherpools auf dem Quellenserver.

### Name des Zielservers

Der Name des Zielservers.

### Zielspeicherpool

Der Name des Verzeichniscontainerspeicherpools auf dem Zielserver.

### Prozent geschützt

Der Prozentsatz der geschützten Daten im Verzeichniscontainerspeicherpool.

### Geschützte Datenbereiche

Die Anzahl Datenbereiche, die im Verzeichniscontainerspeicherpool geschützt werden.

- Gesamtzahl der Datenbereiche  
Die Gesamtzahl der Datenbereiche im Verzeichniscontainerspeicherpool.
- Geschützte MB  
Das Gesamtvolumen der geschützten Daten im Verzeichniscontainerspeicherpool in Megabyte.
- Gesamtzahl MB  
Das Gesamtvolumen der Daten im Verzeichniscontainerspeicherpool in Megabyte.
- Letzter ausgeführter Schutz  
Das Datum und die Uhrzeit, an dem bzw. zu der der Verzeichniscontainerspeicherpool zuletzt geschützt wurde.
- Datum/Zeit der letzten Aktualisierung  
Das Datum und die Uhrzeit, an dem bzw. zu der der Verzeichniscontainerspeicherpool zuletzt aktualisiert wurde.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY PROTECTSTATUS

| Befehl          | Beschreibung                                    |
|-----------------|---|
| PROTECT STGPOOL | Schützt einen Verzeichniscontainerspeicherpool. |

## QUERY PROXYNODE (Proxyberechtigung für einen Clientknoten abfragen)

Verwenden Sie diesen Befehl, um Clientknoten anzuzeigen, die die Berechtigung als Proxy für andere Clientknoten auf dem IBM Spectrum Protect-Server haben.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query PROXynode----TArget-----+-----+-----><
                                     .-*-----
                                     '-Zielknotenname-'
```

### Parameter

**TArget**  
Gibt den Namen des Knotens an, der Ziel des Knotens mit Proxyberechtigung ist. Die Angabe eines Zielknotenname ist optional. Namen mit Platzhalterzeichen können zur Angabe des Zielknotenname verwendet werden. Eine durch Kommas getrennte Auflistung von Knotenname ist ebenfalls zulässig.

### Beispiel: Clientknoten mit Proxy-Berechtigung auflisten

Um alle IBM Spectrum Protect-Clientknoten mit Proxy-Berechtigung für den Zielknoten MYCLUSTER anzuzeigen, geben Sie den folgenden Befehl aus.

```
query proxynode target=mycluster
```

```
Zielknoten      Agentenknoten
-----
FRED            MOE MINIE MICKEY
ALPHA          BETA GAMMA DELTA
```

### Feldbeschreibungen

- Zielknoten**  
Gibt den Namen des Knotens an, der Ziel des Knotens mit Proxyberechtigung ist.
- Agentenknoten**  
Gibt den Namen des Agentenknotens an.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY PROXYNODE

| Befehl | Beschreibung |
|--------|--------------|
|--------|--------------|

| Befehl           | Beschreibung  |
|------------------|---|
| GRANT PROXYNODE  | Erteilt einem Agentenknoten die Proxyberechtigung.  |
| REVOKE PROXYNODE | Entzieht einem Agentenknoten die Proxyberechtigung. |

## QUERY PVUESTIMATE (Prozessor-Value-Unit-Schätzung anzeigen)

Verwenden Sie diesen Befehl, um eine Schätzung der Clienteinheiten und Servereinheiten anzufordern, die von dem IBM Spectrum Protect-Server verwaltet werden. Außerdem wird mit diesem Befehl eine Schätzung der Prozessor-Value-Unit-Summen (PVU-Summen) für die Servereinheiten bereitgestellt.

Dieser Befehl generiert eine PVU-Schätzung, die auf der Anzahl logischer Knoten basiert, die für den IBM Spectrum Protect-Server definiert sind. Dagegen basiert die Berechnung der Lizenzpflichten auf der Anzahl physischer Computer. Möglicherweise ist keine 1:1-Korrelation zwischen der Anzahl logischer Knoten und der Anzahl physischer Computer vorhanden. Der von dem Befehl QUERY PVUESTIMATE generierte Bericht ist eine Schätzung, die rechtlich nicht bindend ist.

Für den Befehl QUERY PVUESTIMATE wird angenommen, dass Knoten auf Microsoft Windows 7-, Microsoft Windows XP Professional- und Apple-Systemen Clienteinheiten sind. Knoten auf allen anderen Plattformen werden als Servereinheiten betrachtet. Der Server, auf dem IBM Spectrum Protect ausgeführt wird, wird ebenfalls als Servereinheit klassifiziert. Sie können jedoch Servereinheiten wieder als Clienteinheiten klassifizieren, falls dies erforderlich ist. Wenn Ihr System Workstations im Ruhezustand, Testworkstations oder andere Workstations umfasst, die bei der PVU-Berechnung ignoriert werden können, können Sie diese als Typ 'Andere' angeben. Um eine Knotenklassifikation zu ändern, verwenden Sie den Befehl UPDATE NODE oder den Befehl REGISTER NODE.

Anmerkung: Die von IBM Spectrum Protect zurückgemeldeten PVU-Informationen werden nicht als annehmbarer Ersatz für das IBM® License Metric Tool angesehen.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

>>-Query PVUESTIMATE Format Standard
'-Format-----Standard+'
'-Format-----Standard+'
'-Detailed-'

```

### Parameter

#### Format

Gibt das Ausgabeformat an. Dieser Parameter ist wahlfrei. Der Standardwert ist Standard. Die folgenden Werte können verwendet werden:

#### Standard

Gibt die Standardausgabe an.

#### Detailed

Gibt die Detailausgabe an.

### Beispiel: Die geschätzte Anzahl der Einheiten und PVU anzeigen

Die geschätzte Anzahl der Clienteinheiten und Servereinheiten sowie die geschätzte PVU für die Servereinheiten für einen IBM Spectrum Protect-Server anzeigen. Den folgenden Befehl ausgeben:

```
query pvuestimate
```

Tabelle 1. Beispielausgabe für mehrere Produkte, die von einem IBM Spectrum Protect-Server verwaltet werden

| Produkt                               | Anzahl Clienteinheiten | Anzahl Servereinheiten | Prozessor-Value-Unit (PVU) der Servereinheiten |
|---------------------------------------|------------------------|------------------------|--|
| IBM Spectrum Protect Extended Edition | 1.000                  | 905                    | 90.500   |

| Produkt   | Anzahl Clienteinheiten | Anzahl Servereinheiten | Prozessor-Value-Unit (PVU) der Servereinheiten |
|---|------------------------|------------------------|--|
| IBM Spectrum Protect for Storage Area Networks                                  | 50                     | 10                     | 1.000  |
| IBM Spectrum Protect for Space Management                                       | 0                      | 0                      | 0  |
| IBM Spectrum Protect for Mail   | 0                      | 25                     | 5.000  |
| IBM Spectrum Protect for Databases  | 0                      | 1.025                  | 20.500   |
| IBM Spectrum Protect for Enterprise Resource Planning                           | 0                      | 25                     | 5.000  |
| IBM Spectrum Protect for System Backup and Recovery                             | 0                      | 0                      | 0  |
| Andere Knotenklassifikationen   | Anzahl                 |                        |  |
| Knoten vor Version 6.3, für die momentan keine PVU-Informationen verfügbar sind | 10                     |                        |  |
| Knoten mit Version 6.3 oder höher ohne PVU-Abgleich                             | 9                      |                        |  |
| Vom Administrator als "andere Einheit" klassifizierte Knoten                    | 8                      |                        |  |
| Als nicht lizenzierte API-Anwendung definierte Knoten                           | 6                      |                        |  |

Die folgende Liste enthält Details zu den Beispielfeldern:

**Produkt**

Der Name des IBM Spectrum Protect-Produkts.

**Anzahl Clienteinheiten**

Die geschätzte Anzahl der Clienteinheiten, die von dem Produkt verwaltet werden. Standardmäßig werden nur Knoten auf Microsoft Windows 7-, Microsoft Windows XP Professional- und Apple-Systemen als Clienteinheiten betrachtet.

**Anzahl Servereinheiten**

Die geschätzte Anzahl der Servereinheiten, die von dem Produkt verwaltet werden. Standardmäßig werden Knoten auf allen Plattformen mit Ausnahme von Microsoft Windows 7-, Microsoft Windows XP Professional- und Apple-Systemen als Servereinheiten betrachtet. Diese Anzahl enthält auch den Server, auf dem IBM Spectrum Protect ausgeführt wird.

**Prozessor-Value-Unit (PVU) der Servereinheiten**

Die geschätzten PVUs aller Knoten, die als Servereinheiten verbunden sind.

**Knoten vor Version 6.3, für die momentan keine PVU-Informationen verfügbar sind**

Einheiten, die keine Prozessorinformationen an den Server zurückmelden.

**Knoten mit Version 6.3 oder höher ohne PVU-Abgleich**

Einheiten, die nicht alle erforderlichen Werte zurückmelden, oder einige Werte wurden als "Unbekannt" zurückgemeldet.

**Vom Administrator als "andere Einheit" klassifizierte Knoten**

Knoten, die vom Administrator mit dem Befehl `update node roleoverride=other` von der PVU-Berechnung ausgeschlossen werden.

**Als nicht lizenzierte API-Anwendung definierte Knoten**

Knoten, wie beispielsweise DB2-Sicherungsanwendungen oder angepasste API-Anwendungen.

## Beispiel: Ausführliche Knoteninformationen anzeigen

Informationen zu einzelnen Knoten anzeigen, indem der Wert 'Detailed' (d) für den Parameter Format angegeben wird. Den folgenden Befehl ausgeben:

```
tsm: PATMOS_630> query pvuestimate f=d
```

Tabelle 2. Knotenklassifikationen für bestimmte Produkte

| Produkt                               | Anzahl Clienteinheiten | Anzahl Servereinheiten | Prozessor-Value-Unit (PVU) der Servereinheiten |
|---------------------------------------|------------------------|------------------------|--|
| IBM Spectrum Protect Extended Edition | 1.000                  | 905                    | 90.500   |
| - banode1                             | 1                      |                        |  |
| - banode2                             |                        | 1                      | 200  |
| - banode3                             | 1                      |                        |  |
| - banode3                             |                        | 1                      | 100  |

| Produkt   | Anzahl Clienteinheiten | Anzahl Servereinheiten | Prozessor-Value-Unit (PVU) der Servereinheiten |
|---|------------------------|------------------------|--|
| IBM Spectrum Protect for Storage Area Networks        | 50                     | 10                     | 1.000  |
| - stagent1  |                        | 1                      | 50   |
| - stagent2  |                        | 1                      | 100  |
| IBM Spectrum Protect for Space Management             | 0                      | 0                      | 0  |
| IBM Spectrum Protect for Mail                         | 0                      | 25                     | 5.000  |
| - mailnode1   |                        | 1                      | 200  |
| - mailnode2   |                        | 1                      | 100  |
| IBM Spectrum Protect for Databases                    | 0                      | 1.025                  | 20.500   |
| - dbnode1   |                        | 1                      | 200  |
| - dbnode2   |                        | 1                      | 100  |
| IBM Spectrum Protect for Enterprise Resource Planning | 0                      | 25                     | 5.000  |
| - erpnode1  |                        | 1                      | 50   |
| - erpnode2  |                        | 1                      | 100  |
| IBM Spectrum Protect for System Backup and Recovery   | 0                      | 0                      | 0  |

| Andere Knotenklassifikationen   | Anzahl |
|---|--------|
| Knoten vor Version 6.3, für die momentan keine PVU-Informationen verfügbar sind | 10     |
| - oldnode1  | 1      |
| - oldnode2  | 1      |
| - mailnote44  | 1      |
| - erpnode66   | 1      |
| Knoten mit Version 6.3 oder höher ohne PVU-Abgleich                             | 10     |
| - badcitnode1   | 1      |
| - badcitnode2   | 1      |
| - mailnode23  | 1      |
| - erpnode34   | 1      |
| Vom Administrator als "andere Einheit" klassifizierte Knoten                    | 8      |
| - overriddennode1   | 1      |
| - overriddennode2   | 1      |
| - mailnode77  |        |
| Als nicht lizenzierte API-Anwendung definierte Knoten                           | 6      |
| - vendorapinode1  | 1      |

| Andere Knotenklassifikationen | Anzahl |
|-------------------------------|--------|
| - vendorapinode2              | 1      |

## Zugehörige Befehle

Tabelle 3. Zugehörige Befehle für QUERY PVUESTIMATE

| Befehl                 | Beschreibung   |
|------------------------|--|
| AUDIT LICENSES         | Prüft die Einhaltung der definierten Lizenzen.   |
| QUERY LICENSE          | Zeigt Informationen über Lizenzen und Prüfvorgänge an.   |
| QUERY NODE             | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.  |
| REGISTER LICENSE       | Registriert eine Lizenz für den IBM Spectrum Protect-Server.   |
| REGISTER NODE          | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.  |
| SET CPUINFOREFRESH     | Gibt die Anzahl der Tage zwischen Clientsuchläufen nach Workstationinformationen an, die für PVU-Schätzungen verwendet werden. |
| SET LICENSEAUDITPERIOD | Gibt die Anzahl Tage zwischen den automatischen Lizenzprüfungen an.  |
| UPDATE NODE            | Ändert die Attribute, die einem Clientknoten zugeordnet sind.  |

## QUERY RECOVERYMEDIA (Wiederherstellungsdatenträger abfragen)

Mit diesem Befehl können Informationen über die Datenträger (beispielsweise Boot-Datenträger) angezeigt werden, die für die Wiederherstellung einer Maschine benötigt werden. Datenträger werden in alphabetischer Reihenfolge nach Namen angezeigt.

Hinweis: Die Informationen werden von IBM Spectrum Protect nicht verwendet. Sie dienen nur zur Planung der Fehlerbehebung bei Client-Maschinen.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

>>-Query RECOVERYMedia-+-----+----->
                        .-*-----+
                        '-Datenträgername-'

>+-----+-----+-----+----->
  '-Type---+---BOot---+'  '-LOcation---+---Position-'
      '-Other-'

  .-Format----Standard----.
>+-----+-----+-----+-----><
  '-Format---+---Standard---+'
      '-Detailed-'

```

### Parameter

#### Datenträgername

Gibt den Namen des Wiederherstellungsdatenträgers an. Es können Platzhalterzeichen verwendet werden, um den Namen anzugeben. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Wiederherstellungsdatenträger.

#### Type

Gibt den Typ des Datenträgers an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, werden alle Wiederherstellungsdatenträger abgefragt. Gültige Werte:

#### BOot

Nur Boot-Datenträger werden abgefragt.

Other

Alle Datenträger, außer Boot-Datenträger, werden abgefragt.

Location

Gibt den Standort des Wiederherstellungsdatenträgers an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Es können bis zu 255 Zeichen angegeben werden. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Gültige Werte:

Standard

Zeigt Teilinformationen an. Dies ist der Standardwert.

Detailed

Zeigt alle Informationen an.

## Beispiel: Übersichtsdaten zu einem bestimmten Wiederherstellungsdatenträger anzeigen

---

Informationen für den Wiederherstellungsdatenträger RECMED1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query recoverymedia RECMED1
```

| Wiederherstellungs-<br>datenträgername | Datenträgernamen | Standort             | Maschinename |
|--|------------------|----------------------|--------------|
| -----                                  | -----            | -----                | -----        |
| RECMED1                                | vol1 vol2 vol3   | IRONMOUNTAIN<br>vol4 | MACH1        |

## Beispiel: Ausführliche Informationen zu einem bestimmten Wiederherstellungsdatenträger anzeigen

---

Ausführliche Informationen für den Wiederherstellungsdatenträger RECMED1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query recoverymedia RECMED1 format=detailed
```

```
Wiederherstellungsdatenträgername: RECMED1
                                   Typ: Boot
                                   Datenträgernamen: vol1 vol2 vol3 vol4
                                   Standort: IRONMOUNTAIN
                                   Beschreibung:
                                   Produkt:
Produktinformation:
                                   Maschinename: MACH1
```

## Feldbeschreibungen

---

Wiederherstellungsdatenträgername

Der Name des Wiederherstellungsdatenträgers.

Typ

Angabe, ob es sich bei den Wiederherstellungsdatenträgern um Boot-Datenträger oder um einen anderen Datenträgertyp handelt.

Gültige Werte:

Boot

Die Wiederherstellungsdatenträger sind Boot-Datenträger.

Other

Die Wiederherstellungsdatenträger sind keine Boot-Datenträger.

Datenträgernamen

Die Gruppe der Datenträger, die die Daten enthalten, die zum Wiederherstellen der Maschinen benötigt werden, die diesem Datenträger zugeordnet sind.

Standort

Der Speicherort des Wiederherstellungsdatenträgers.

Beschreibung

Eine Beschreibung des Wiederherstellungsdatenträgers.

Produkt

Das Produkt, das zum Erstellen der Boot-Datenträger verwendet wurde.

Produktinformation

Informationen über das Produkt, das die Boot-Datenträger erstellt hat. Diese Informationen werden eventuell zum Zurückschreiben der Maschine benötigt.

Maschinenname

Die Maschinen, die diesem Wiederherstellungsdatenträger zugeordnet sind.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY RECOVERYMEDIA

| Befehl                       | Beschreibung   |
|------------------------------|--|
| DEFINE RECMEDMACHASSOCIATION | Ordnet Wiederherstellungsdatenträger einer Maschine zu.                                    |
| DEFINE RECOVERYMEDIA         | Definiert die Datenträger, die für die Wiederherstellung einer Maschine erforderlich sind. |
| DELETE RECOVERYMEDIA         | Löscht Wiederherstellungsdatenträger.  |
| UPDATE RECOVERYMEDIA         | Ändert die Attribute von Wiederherstellungsdatenträgern.                                   |

## QUERY REPLICATION (Knotenreplikationsprozesse abfragen)

Verwenden Sie diesen Befehl, um Informationen zu aktiven und beendeten Knotenreplikationsprozessen anzuzeigen.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Wichtig: Es können keine Informationen zu aktiven Replikationsprozessen für Clientknoten angezeigt werden, die aus Import- und Exportoperationen in Replikationsoperationen konvertiert werden. Der Konvertierungsprozess kann lange dauern, aber er erfolgt nur einmal für einen Clientknoten, der konvertiert wird.

Standardmäßig werden Datensätze zu abgeschlossenen Knotenreplikationsprozessen 30 Kalendertage aufbewahrt. Ein *Kalendertag* besteht aus 24 Stunden, von Mitternacht bis Mitternacht.

Um den Aufbewahrungszeitraum anzuzeigen, geben Sie den Befehl QUERY STATUS aus. Überprüfen Sie den Wert im Feld Aufbewahrungszeitraum für Replikationsdatensätze. Um den Aufbewahrungszeitraum zu ändern, geben Sie den Befehl SET REPLETENTION aus.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-Query REPLIcation--Knotenname----->
. -*-----
>+-----+
| (1) |
|-----+--Dateibereichsname--+--|
| | '-----' |
|-----+--FSID-----|
| | (2) |
|-----|
. -NAMEType----SERVER-----
>+-----+
| -NAMEType----+--SERVER----+ |
| | +--UNICODE--+ |
| | | (2) | |
| | | -FSID----- |
. -CODEType----BOTH-----
>+-----+
| -CODEType----+--BOTH-----+ |
| | +--UNICODE----+ |
| | | -NONUNICODE- |
. -DISplay----1-----
>+-----+-----+-----+-----+----->
| -DISplay----+--Anzahl Tage- | | -PROcessid----+--Prozess-ID- |
. -STatus----All----- . -Format----Standard-----
>+-----+-----+-----+----->
```



```
'-Status-----+All-----+' '-Format-----+Standard-+-'  
+-RUnning-+ '-Detailed-'  
+-ENded---+  
'-FAiled--'
```

Anmerkungen:

1. Mischen Sie nicht FSIDs (Dateibereichs-IDs) und Dateibereichsnamen in demselben Befehl.
2. Geben Sie nicht die FSID an, wenn Sie Platzhalterzeichen für den Clientknotennamen verwenden.

## Parameter

---

### Knotenname (Erforderlich)

Gibt den Namen des abzufragenden Clientknotens an. Mit einer Ausnahme können Sie Platzhalterzeichen verwenden, wenn Sie diesen Namen angeben. Wenn der Parameter NAMETYPE den Wert FSID hat, geben Sie keine Platzhalterzeichen für den Clientknotennamen an. Der Wert FSID gibt die Dateibereichs-ID an. Dateibereiche mit identischen Namen können verschiedene IDs in verschiedenen Clientknoten haben.

### Dateibereichsname oder FSID

Gibt den Namen des Dateibereichs oder die ID des Dateibereichs (FSID) an, der abgefragt werden soll. Ein Name oder eine FSID ist optional. Wenn Sie keinen Namen oder keine FSID angeben, werden alle Dateibereiche abgefragt.

#### Dateibereichsname

Gibt den Namen des Dateibereichs an, der Daten enthält, die abgefragt werden sollen. Bei Dateibereichsnamen muss die Groß-/Kleinschreibung berücksichtigt werden. Um die korrekte Schreibweise für den Dateibereich zu bestimmen, geben Sie den Befehl QUERY FILESPACE aus. Mehrere Namen sind ohne Leerzeichen durch Kommas voneinander zu trennen. Wenn Sie einen Namen angeben, können Sie Platzhalterzeichen verwenden.

Ein Server, der über Clients mit Unicode-fähigen Dateibereichen verfügt, muss möglicherweise den Dateibereichsnamen konvertieren. Beispielsweise muss der Server gegebenenfalls einen Namen aus der Zeichenumsetztabelle des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich in der Beschreibung des Parameters NAMETYPE. Geben Sie keinen Dateibereichsnamen an oder geben Sie nur ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter CODETYPE verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

#### FSID

Gibt die Dateibereichs-ID für den Dateibereich an, der abgefragt werden soll. Der Server verwendet FSIDs zum Lokalisieren der Dateibereiche, die repliziert werden sollen. Um die FSID für einen Dateibereich zu bestimmen, geben Sie den Befehl QUERY FILESPACE aus. Mehrere FSIDs sind ohne Leerzeichen durch Kommas voneinander zu trennen. Wenn Sie eine FSID angeben, muss der Wert des Parameters NAMETYPE FSID lauten.

### NAMETYPE

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Sie können diesen Parameter für Unicode-fähige IBM Spectrum Protect-Clients verwenden, die über die Betriebssysteme Windows, Macintosh OS X und NetWare verfügen.

Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen eingeben. Der Standardwert lautet SERVER. Sie können einen der folgenden Werte angeben:

#### SERVER

Der Server verwendet die Zeichenumsetztabelle des Servers, um Dateibereichsnamen zu interpretieren.

#### Unicode

Der Server konvertiert Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind. Die Konvertierung kann auch fehlschlagen, wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

#### FSID

Der Server interpretiert Dateibereichsnamen unter Verwendung ihrer Dateibereichs-IDs.

### CODETYPE

Gibt den Typ der Dateibereiche an, die in der Abfrage berücksichtigt werden sollen. Der Standardwert lautet BOTH. Dieser Standardwert bedeutet, dass Dateibereiche unabhängig von der Art der Zeichenumsetztabelle eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben. Sie können einen der folgenden Werte angeben:

- UNICODE  
Nur Dateibereiche einschließen, die in Unicode sind.
- NONUNICODE  
Dateibereiche einschließen, die nicht nur in Unicode sind.
- BOTH  
Alle Dateibereiche unabhängig von der Art der Zeichenumsetzungstabelle einschließen.

#### DISplay

Gibt die Anzahl der Tage an, für die das Knotenreplikationsprotokoll angezeigt werden soll. Der Standardwert ist 1. Mit diesem Standardwert werden Informationen zu aktiven Knotenreplikationsprozessen und zu Prozessen angezeigt, die während des aktuellen Kalendertags abgeschlossen wurden. Der Maximalwert ist 9999.

Sie können eine Zahl angeben, die kleiner-gleich der Anzahl der Tage ist, die als Aufbewahrungszeitraum für die Replikationsprotokollsätze angegeben wird. Wenn Sie einen Wert angeben, der größer als der Wert des Aufbewahrungszeitraums für die Replikation ist oder größer als die Anzahl der Tage ist, die Replikationsdatensätze erfasst werden, zeigt der Server nur die Anzahl der verfügbaren Replikationsprotokollsätze an. Beispiel: Angenommen, der Aufbewahrungszeitraum für die Replikation beträgt 30 Tage und der Replikationsprozess wird nur 10 Tage ausgeführt. Wenn Sie `DISPLAY=20` angeben, werden nur 10 Tage des Replikationsprotokolls angezeigt.

#### PROcessid

Gibt das Knotenreplikationsprotokoll an, das einem bestimmten Prozess zugeordnet ist, der durch die Prozess-ID angegeben ist. Dieser Parameter ist wahlfrei. Wenn dieser Parameter nicht angegeben wird, werden alle Prozesse für die mit dem Parameter `DISPLAY` angegebene Anzahl der Tage angezeigt.

Ein Neustart des Servers kann zur Folge haben, dass der Server Prozess-IDs wiederverwendet. Die Wiederverwendung von Prozess-IDs kann zu doppelten Prozess-IDs für separate Prozesse führen.

#### STatus

Gibt den Status der Dateibereiche an, die abgefragt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist ALL. Sie können einen der folgenden Werte angeben:

##### ALL

Gibt alle Dateibereiche, die gerade repliziert werden, Dateibereiche, die erfolgreich repliziert wurden, und Dateibereiche an, deren Replikation nicht beendet wurde oder die mit Fehlern repliziert wurden.

##### RUNning

Gibt alle Dateibereiche an, die auf den Zielreplikationsserver repliziert werden.

##### ENded

Gibt alle Dateibereiche, die erfolgreich repliziert wurden, und Dateibereiche an, deren Replikation nicht beendet wurde oder die mit Fehlern repliziert wurden.

##### FAiled

Gibt alle Dateibereiche an, deren Replikation nicht beendet wurde oder die mit Fehlern repliziert wurden.

#### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Sie können einen der folgenden Werte angeben:

##### Standard

Gibt an, dass Teilinformationen für Knotenreplikationsprozesse angezeigt werden.

##### Detailed

Gibt an, dass alle verfügbaren Informationen für die Knotenreplikationsprozesse angezeigt werden.

## Beispiel: Informationen zu Replikationsprozessen für einen Dateibereich anzeigen

Informationen zu Replikationsprozessen für einen Dateibereich im Clientknoten PAYROLL anzeigen. Die Dateibereichs-ID ist 10.

```
query replication ironman
```

| Knotenname | Dateiber.-<br>klasse | FSID | Startzeit            | Endzeit              | Status  | Phase |
|------------|----------------------|------|----------------------|----------------------|---------|-------|
| IRONMAN    | /space               | 2    | 02/08/11<br>21:44:19 | 02/08/11<br>21:48:14 | Beendet | Keine |

```
query replication ironman format=detailed
```

```

Knotenname: IRONMAN
Dateibereichsname: /space
FSID: 2
Startzeit: 02/08/11 21:44:19

```

```

Endzeit: 02/08/11 21:48:14
Status: Beendet
Prozessnummer: 4
Befehl: replicate node ironman
Phase: Keine
Ausführungszeit des Prozesses: 0 Tag(e) 0 Stunde(n)
4 Minute(n)
Beendigungsstatus: Beendet
Ursache der Nicht-Beendigung: Keine
Datum/Zeit der letzten Aktual. von Sicherungsdateien:
Zielserver für Sicherung:
Sicherungsdateien, die keine Aktion erfordert haben: 0
Zu replizierende Sicherungsdateien: 0
Replizierte Sicherungsdateien: 0
Aufgrund von Fehlern nicht replizierte Sicherungsdateien: 0
Noch nicht replizierte Sicherungsdateien: 0
Zu löschende Sicherungsdateien: 0
Gelöschte Sicherungsdateien: 0
Aufgrund von Fehlern nicht gelöschte Sicherungsdateien: 0
Zu aktualisierende Sicherungsdateien: 0
Aktualisierte Sicherungsdateien: 0
Aufgrund von Fehlern nicht aktualisierte Sicherungsdateien: 0
Zu replizierende Byte für Sicherungsdateien (MB): 0
Replizierte Byte für Sicherungsdateien (MB): 0
Übertragene Byte für Sicherungsdateien (MB): 0
Aufgrund von Fehlern nicht replizierte Byte für Sicherungsdateien (MB): 0
Noch nicht replizierte Byte für Sicherungsdateien (MB): 0

Datum/Zeit der letzten Aktual. von Archivierungsdateien: 02/08/11 21:48:14
Zielserver für Archivierung: NIGLINA
Archivierungsdateien, die keine Aktion erfordert haben: 0
Zu replizierende Archivierungsdateien: 39.416
Replizierte Archivierungsdateien: 39.206
Aufgrund von Fehlern nicht replizierte Archivierungsdateien: 210
Noch nicht replizierte Archivierungsdateien: 0
Zu löschende Archivierungsdateien: 0
Gelöschte Archivierungsdateien: 0
Aufgrund von Fehlern nicht gelöschte Archivierungsdateien: 0
Zu aktualisierende Archivierungsdateien: 0
Aktualisierte Archivierungsdateien: 0

Aufgrund von Fehlern nicht aktualisierte Archivierungsdateien: 0
Zu replizierende Byte für Archivierungsdateien (MB): 4.335
Replizierte Byte für Archivierungsdateien (MB): 4.335
Übertragene Byte für Archivierungsdateien (MB): 0
Aufgrund von Fehlern nicht replizierte Byte für Archivierungsdateien (MB): 0
Noch nicht replizierte Byte für Archivierungsdateien (MB): 0

Datum/Zeit der letzten Aktual. von speicherverwalteten Dateien:
Zielserver für Speicherverwaltung:
Speicherverwaltete Dateien, die keine Aktion erfordert haben: 0
Zu replizierende speicherverwaltete Dateien: 0
Replizierte speicherverwaltete Dateien: 0
Aufgrund von Fehlern nicht replizierte speicherverwaltete Dateien: 0
Noch nicht replizierte speicherverwaltete Dateien: 0
Zu löschende speicherverwaltete Dateien: 0
Gelöschte speicherverwaltete Dateien: 0
Aufgrund von Fehlern nicht gelöschte speicherverwaltete Dateien: 0
Zu aktualisierende speicherverwaltete Dateien: 0
Aktualisierte speicherverwaltete Dateien: 0
Aufgrund von Fehlern nicht aktualisierte speicherverwaltete Dateien: 0
Zu replizierende Byte für speicherverwaltete Dateien (MB): 0
Replizierte Byte für speicherverwaltete Dateien (MB): 0
Übertragene Byte für speicherverwaltete Dateien (MB): 0
Aufgrund von Fehlern nicht replizierte Byte für speicherverwaltete Dateien (MB): 0
Noch nicht replizierte Byte für speicherverwaltete Dateien (MB): 0
Gesamtzahl der Dateien, die keine Aktion erfordert haben: 0
Gesamtzahl der zu replizierenden Dateien: 39.416
Gesamtzahl der replizierten Dateien: 39.206
Gesamtzahl der aufgrund von Fehlern nicht replizierten Dateien: 210
Gesamtzahl der noch nicht replizierten Dateien: 0
Gesamtzahl der zu löschenden Dateien: 0
Gesamtzahl der gelöschten Dateien: 0
Gesamtzahl der aufgrund von Fehlern nicht gelöschten Dateien: 0
Gesamtzahl der zu aktualisierenden Dateien: 0
Gesamtzahl der aktualisierten Dateien: 0
Gesamtzahl der aufgrund von Fehlern nicht aktualisierten Dateien: 0

```

Summe der zu replizierenden Byte (MB): 4.335  
Summe der replizierten Byte (MB): 4.335  
Summe übertragener Byte (MB):  
Summe der aufgrund von Fehlern nicht replizierten Byte (MB):  
Summe der noch nicht replizierten Byte (MB):  
Geschätzte Fertigstellung in Prozent: 100  
Geschätzte verbleibende Zeit:  
Geschätzte Zeit der Fertigstellung:

## Feldbeschreibungen

---

### Knotenname

Der Name des Clientknotens, dessen Daten angezeigt werden.

### Dateibereichsname

Der Name des Clientdateibereichs, dessen Daten angezeigt werden.

### FSID

Die Dateibereichs-ID.

### Startzeit

Das Datum und die Uhrzeit, an dem bzw. zu der der Knotenreplikationsprozess gestartet wurde.

### Endzeit

Das Datum und die Uhrzeit, an dem bzw. zu der der Knotenreplikationsprozess beendet wurde.

### Status

Der Status des Knotenreplikationsprozesses. Die folgenden Werte sind gültig:

#### Aktiv

Der Prozess ist aktiv und sucht nach auswählbaren Daten oder sendet Daten an den Zielreplikationsserver.

#### Beendet

Der Prozess wurde beendet oder ist fehlgeschlagen.

#### Fehlgeschlagen

Der Prozess ist fehlgeschlagen.

### Prozessnummer

Die ID für den Knotenreplikationsprozess.

Dieselbe Prozessnummer kann verschiedene Startzeiten haben. Wenn ein Replikationsprozess gestartet und der Server erneut gestartet wird, ordnet der Server Prozessnummern zu, wobei mit Nummer 1 begonnen wird. Replikationsprozesse, die nach einem Serverneustart gestartet werden, können Prozessnummern erhalten, die bereits anderen Replikationsprozessen im Replikationsprotokoll zugeordnet sind. Um eindeutige Replikationsprozesse anzugeben, verwenden Sie die Startzeit.

### Befehl

Der Befehl, der ausgegeben wurde, um den Knotenreplikationsprozess zu starten.

### Phase

Die Phase eines aktiven Knotenreplikationsprozesses. Die folgenden Phasen sind in der Reihenfolge ihres Auftretens aufgelistet:

#### Wird identifiziert

Der Knotenreplikationsprozess hat mit dem Identifizieren von Daten begonnen, die repliziert werden sollen, aber die Daten werden noch nicht an den Zielreplikationsserver gesendet.

#### Wird identifiziert und repliziert

Der Knotenreplikationsprozess identifiziert Daten, die repliziert werden sollen, und überträgt die Daten an den Zielreplikationsserver.

#### Wird repliziert

Der Knotenreplikationsprozess hat die Daten identifiziert und überträgt Dateien an den Zielreplikationsserver.

#### Keine.

Der Knotenreplikationsprozess ist nicht aktiv.

### Ausführungszeit des Prozesses

Die Ausführungszeit des Knotenreplikationsprozesses.

### Beendigungsstatus

Der Status des Knotenreplikationsprozesses. Die folgenden Werte sind gültig:

#### Beendet

Der Knotenreplikationsprozess wurde abgeschlossen.

#### Nicht beendet

Der Knotenreplikationsprozess wurde nicht bis zum Abschluss ausgeführt. Um die Ursache zu bestimmen, überprüfen Sie den Wert im Feld 'Ursache der Nicht-Beendigung'.

### Ursache der Nicht-Beendigung

Der Grund, warum der Knotenreplikationsprozess nicht bis zum Abschluss ausgeführt wurde. Mögliche Werte sind *abgebrochen* und *andere*. Der Wert *andere* kann angeben, dass der Server während der Replikation angehalten wurde oder der Server fehlgeschlagen ist.

Datum/Zeit der letzten Aktual. von Sicherungsdateien

Das Datum und die Uhrzeit, an dem bzw. zu der Statistikdaten für Sicherungsdateien zuletzt aktualisiert wurden. Die angegebene Zeit ist die Zeit, zu der die Dateien in dem Dateibereich für die Replikation identifiziert wurden, oder die Zeit, zu der jeder Dateistapel an den Zielreplikationsserver gesendet wurde.

Datum/Zeit der letzten Aktual. von Archivierungsdateien

Das Datum und die Uhrzeit, an dem bzw. zu der Statistikdaten für Archivierungsdateien zuletzt aktualisiert wurden. Die angegebene Zeit ist die Zeit, zu der die Dateien in dem Dateibereich für die Replikation identifiziert wurden, oder die Zeit, zu der jeder Dateistapel an den Zielreplikationsserver gesendet wurde.

Datum/Zeit der letzten Aktual. von speicher verwalteten Dateien

Das Datum und die Uhrzeit, an dem bzw. zu der Statistikdaten für speicher verwaltete Dateien zuletzt aktualisiert wurden. Die angegebene Zeit ist die Zeit, zu der die Dateien in dem Dateibereich für die Replikation identifiziert wurden, oder die Zeit, zu der jeder Dateistapel an den Zielreplikationsserver gesendet wurde.

Zielserver für Sicherung

Der Name des Zielreplikationsservers für Sicherungsdateien.

Zielserver für Archivierung

Der Name des Zielreplikationsservers für Archivierungsdateien.

Zielserver für Speicher Verwaltung

Der Name des Zielreplikationsservers für speicher verwaltete Dateien.

Sicherungsdateien, die keine Aktion erfordert haben

Die Anzahl der Sicherungsdateien in dem Dateibereich, die nicht repliziert, aktualisiert oder gelöscht werden mussten.

Archivierungsdateien, die keine Aktion erfordert haben

Die Anzahl der Archivierungsdateien in dem Dateibereich, die nicht repliziert, aktualisiert oder gelöscht werden mussten.

Speicher verwaltete Dateien, die keine Aktion erfordert haben

Die Anzahl der speicher verwalteten Dateien in dem Dateibereich, die nicht repliziert, aktualisiert oder gelöscht werden mussten.

Zu replizierende Sicherungsdateien

Die Anzahl der Sicherungsdateien, die auf den Zielreplikationsserver repliziert werden sollten.

Zu replizierende Archivierungsdateien

Die Anzahl der Archivierungsdateien, die auf den Zielreplikationsserver repliziert werden sollten.

Zu replizierende speicher verwaltete Dateien

Die Anzahl der speicher verwalteten Dateien, die auf den Zielreplikationsserver repliziert werden sollten.

Replizierte Sicherungsdateien

Die Anzahl der Sicherungsdateien, die auf den Zielreplikationsserver repliziert wurden.

Replizierte Archivierungsdateien

Die Anzahl der Archivierungsdateien, die auf den Zielreplikationsserver repliziert wurden.

Replizierte speicher verwaltete Dateien

Die Anzahl der speicher verwalteten Dateien, die auf den Zielreplikationsserver repliziert wurden.

Aufgrund von Fehlern nicht replizierte Sicherungsdateien

Die Anzahl der Sicherungsdateien, die aufgrund von Fehlern nicht auf den Zielreplikationsserver repliziert wurden.

Aufgrund von Fehlern nicht replizierte Archivierungsdateien

Die Anzahl der Archivierungsdateien, die aufgrund von Fehlern nicht auf den Zielreplikationsserver repliziert wurden.

Aufgrund von Fehlern nicht replizierte speicher verwaltete Dateien

Die Anzahl der speicher verwalteten Dateien, die aufgrund von Fehlern nicht auf den Zielreplikationsserver repliziert wurden.

Noch nicht replizierte Sicherungsdateien

Die Anzahl der Sicherungsdateien, die noch nicht auf den Zielreplikationsserver repliziert wurden.

Noch nicht replizierte Archivierungsdateien

Die Anzahl der Archivierungsdateien, die noch nicht auf den Zielreplikationsserver repliziert wurden.

Noch nicht replizierte speicher verwaltete Dateien

Die Anzahl der speicher verwalteten Dateien, die noch nicht auf den Zielreplikationsserver repliziert wurden.

Zu löschende Sicherungsdateien

Die Anzahl der Sicherungsdateien, die auf dem Zielreplikationsserver gelöscht werden sollten.

Zu löschende Archivierungsdateien

Die Anzahl der Archivierungsdateien, die auf dem Zielreplikationsserver gelöscht werden sollten.

Zu löschende speicher verwaltete Dateien

Die Anzahl der speicher verwalteten Dateien, die auf dem Zielreplikationsserver gelöscht werden sollten.

Gelöschte Sicherungsdateien

Die Anzahl der Sicherungsdateien, die auf dem Zielreplikationsserver gelöscht wurden.

Gelöschte Archivierungsdateien

Die Anzahl der Archivierungsdateien, die auf dem Zielreplikationsserver gelöscht wurden.

Gelöschte speicher verwaltete Dateien

Die Anzahl der speicher verwalteten Dateien, die auf dem Zielreplikationsserver gelöscht wurden.

Aufgrund von Fehlern nicht gelöschte Sicherungsdateien

Die Anzahl der Sicherungsdateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver gelöscht wurden.

Aufgrund von Fehlern nicht gelöschte Archivierungsdateien

Die Anzahl der Archivierungsdateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver gelöscht wurden.

Aufgrund von Fehlern nicht gelöschte speicherverwaltete Dateien

Die Anzahl der speicherverwalteten Dateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver gelöscht wurden.

Zu aktualisierende Sicherungsdateien

Die Anzahl der Sicherungsdateien, die auf dem Zielreplikationsserver aktualisiert werden sollten. Wenn die Metadaten einer Datei geändert werden, werden die geänderten Felder an den Zielreplikationsserver gesendet.

Zu aktualisierende Archivierungsdateien

Die Anzahl der Archivierungsdateien, die auf dem Zielreplikationsserver aktualisiert werden sollten. Wenn die Metadaten einer Datei geändert werden, werden die geänderten Felder an den Zielreplikationsserver gesendet.

Zu aktualisierende speicherverwaltete Dateien

Die Anzahl der speicherverwalteten Dateien, die auf dem Zielreplikationsserver aktualisiert werden sollten. Wenn die Metadaten einer Datei geändert werden, werden die geänderten Felder an den Zielreplikationsserver gesendet.

Aktualisierte Sicherungsdateien

Die Anzahl der Sicherungsdateien, die auf dem Zielreplikationsserver aktualisiert wurden.

Aktualisierte Archivierungsdateien

Die Anzahl der Archivierungsdateien, die auf dem Zielreplikationsserver aktualisiert wurden.

Aktualisierte speicherverwaltete Dateien

Die Anzahl der speicherverwalteten Dateien, die auf dem Zielreplikationsserver aktualisiert wurden.

Aufgrund von Fehlern nicht aktualisierte Sicherungsdateien

Die Anzahl der Sicherungsdateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver aktualisiert wurden.

Aufgrund von Fehlern nicht aktualisierte Archivierungsdateien

Die Anzahl der Archivierungsdateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver aktualisiert wurden.

Aufgrund von Fehlern nicht aktualisierte speicherverwaltete Dateien

Die Anzahl der speicherverwalteten Dateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver aktualisiert wurden.

Zu replizierende Byte für Sicherungsdateien (MB)

Die Anzahl der Byte für Sicherungsdateien, die auf den Zielreplikationsserver repliziert werden sollten.

Zu replizierende Byte für Archivierungsdateien (MB)

Die Anzahl der Byte für Archivierungsdateien, die auf den Zielreplikationsserver repliziert werden sollten.

Zu replizierende Byte für speicherverwaltete Dateien (MB)

Die Anzahl der Byte für speicherverwaltete Dateien, die auf den Zielreplikationsserver repliziert werden sollten.

Replizierte Byte für Sicherungsdateien (MB)

Die Anzahl der Byte für Sicherungsdateien, die auf den Zielreplikationsserver repliziert wurden.

Wenn eine Datei in einem deduplizierten Speicherpool gespeichert wurde, kann die Anzahl der Byte in der gespeicherten Datei kleiner als die Anzahl der Byte in der ursprünglichen Datei sein. Dieses Feld stellt die Anzahl der physischen Byte in der ursprünglichen Datei dar.

Replizierte Byte für Archivierungsdateien (MB)

Die Anzahl der Byte für Archivierungsdateien, die auf den Zielreplikationsserver repliziert wurden.

Wenn eine Datei in einem deduplizierten Speicherpool gespeichert wurde, kann die Anzahl der Byte in der gespeicherten Datei kleiner als die Anzahl der Byte in der ursprünglichen Datei sein. Dieses Feld stellt die Anzahl der physischen Byte in der ursprünglichen Datei dar.

Replizierte Byte für speicherverwaltete Dateien (MB)

Die Anzahl der Byte für speicherverwaltete Dateien, die auf den Zielreplikationsserver repliziert wurden.

Wenn eine Datei in einem deduplizierten Speicherpool gespeichert wurde, kann die Anzahl der Byte in der gespeicherten Datei kleiner als die Anzahl der Byte in der ursprünglichen Datei sein. Dieses Feld stellt die Anzahl der physischen Byte in der ursprünglichen Datei dar.

Übertragene Byte für Sicherungsdateien (MB)

Die Anzahl der Byte für Sicherungsdateien, die an den Zielreplikationsserver gesendet wurden.

Der Wert in diesem Feld stellt die tatsächliche Anzahl der Dateibyte dar, die an den Zielreplikationsserver gesendet wurden. Dieser Wert wird berechnet, indem die Anzahl der Byte, die aufgrund der Deduplizierung nicht gesendet wurden, von der Anzahl der zu replizierenden Byte subtrahiert wird.

Übertragene Byte für Archivierungsdateien (MB)

Die Anzahl der Byte für Archivierungsdateien, die an den Zielreplikationsserver gesendet wurden.

Der Wert in diesem Feld stellt die tatsächliche Anzahl der Dateibyte dar, die an den Zielreplikationsserver gesendet wurden. Dieser Wert wird berechnet, indem die Anzahl der Byte, die aufgrund der Deduplizierung nicht gesendet wurden, von der Anzahl der zu replizierenden Byte subtrahiert wird.

Übertragene Byte für speicherverwaltete Dateien (MB)

Die Anzahl der Byte für speicher verwaltete Dateien, die an den Zielreplikationsserver gesendet wurden.

Der Wert in diesem Feld stellt die tatsächliche Anzahl der Dateibyte dar, die an den Zielreplikationsserver gesendet wurden. Dieser Wert wird berechnet, indem die Anzahl der Byte, die aufgrund der Deduplizierung nicht gesendet wurden, von der Anzahl der zu replizierenden Byte subtrahiert wird.

Aufgrund von Fehlern nicht replizierte Byte für Sicherungsdateien (MB)

Die Anzahl der Byte für Sicherungsdateien, die aufgrund von Fehlern nicht auf den Zielreplikationsserver repliziert wurden.

Aufgrund von Fehlern nicht replizierte Byte für Archivierungsdateien (MB)

Die Anzahl der Byte für Archivierungsdateien, die aufgrund von Fehlern nicht auf den Zielreplikationsserver repliziert wurden.

Aufgrund von Fehlern nicht replizierte Byte für speicher verwaltete Dateien (MB)

Die Anzahl der Byte für speicher verwaltete Dateien, die aufgrund von Fehlern nicht auf den Zielreplikationsserver repliziert wurden.

Noch nicht replizierte Byte für Sicherungsdateien (MB)

Die Anzahl der Byte für Sicherungsdateien, die noch nicht auf den Zielreplikationsserver repliziert wurden.

Noch nicht replizierte Byte für Archivierungsdateien (MB)

Die Anzahl der Byte für Archivierungsdateien, die noch nicht auf den Zielreplikationsserver repliziert wurden.

Noch nicht replizierte Byte für speicher verwaltete Dateien (MB)

Die Anzahl der Byte für speicher verwaltete Dateien, die noch nicht auf den Zielreplikationsserver repliziert wurden.

Gesamtzahl der Dateien, die keine Aktion erfordert haben

Die Gesamtzahl der Dateien in dem Dateibereich, die nicht repliziert, aktualisiert oder gelöscht werden mussten.

Gesamtzahl der zu replizierenden Dateien

Die Gesamtzahl der Dateien, die auf den Zielreplikationsserver repliziert werden sollten.

Gesamtzahl der replizierten Dateien

Die Gesamtzahl der Dateien, die auf den Zielreplikationsserver repliziert wurden.

Gesamtzahl der aufgrund von Fehlern nicht replizierten Dateien

Die Gesamtzahl der Dateien, die aufgrund von Fehlern nicht repliziert wurden.

Gesamtzahl der noch nicht replizierten Dateien

Die Gesamtzahl der Dateien, die noch nicht auf den Zielreplikationsserver repliziert wurden.

Gesamtzahl der zu löschenden Dateien

Die Gesamtzahl der Dateien, die auf dem Zielreplikationsserver gelöscht werden sollten.

Gesamtzahl der gelöschten Dateien

Die Gesamtzahl der Dateien, die auf dem Zielreplikationsserver gelöscht wurden.

Gesamtzahl der aufgrund von Fehlern nicht gelöschten Dateien

Die Gesamtzahl der Sicherungsdateien, Archivierungsdateien und speicher verwalteten Dateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver gelöscht wurden.

Gesamtzahl der zu aktualisierenden Dateien

Die Gesamtzahl der Dateien, die auf dem Zielreplikationsserver aktualisiert werden sollten. Wenn die Metadaten einer Datei geändert werden, werden die geänderten Felder an den Zielreplikationsserver gesendet.

Gesamtzahl der aktualisierten Dateien

Die Gesamtzahl der Dateien, die auf dem Zielreplikationsserver aktualisiert wurden.

Gesamtzahl der aufgrund von Fehlern nicht aktualisierten Dateien

Die Gesamtzahl der Sicherungsdateien, Archivierungsdateien und speicher verwalteten Dateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver aktualisiert wurden.

Summe der zu replizierenden Byte (MB)

Die Gesamtzahl der Byte, die auf den Zielreplikationsserver repliziert werden sollten.

Summe der replizierten Byte (MB)

Die Gesamtzahl der Byte, die auf den Zielservers repliziert wurden.

Wenn eine Datei in einem deduplizierten Speicherpool gespeichert wurde, kann die Anzahl der Byte in der gespeicherten Datei kleiner als die Anzahl der Byte in der ursprünglichen Datei sein. Dieses Feld stellt die Anzahl der physischen Byte in der ursprünglichen Datei dar.

Summe übertragener Byte (MB)

Die Gesamtzahl der Byte, die an den Zielreplikationsserver übertragen wurden.

Für Dateien, die in einem deduplizierten Speicherpool gespeichert wurden, schließt der Wert in diesem Feld die Anzahl der Byte in der ursprünglichen Datei ein, bevor doppelte Bereiche entfernt wurden. Wenn doppelte Bereiche bereits auf dem Zielreplikationsserver vorhanden sind, ist die Anzahl der Byte in der ursprünglichen Datei größer als die Anzahl der übertragenen Byte.

Summe der aufgrund von Fehlern nicht replizierten Byte (MB)

Die Gesamtzahl der Byte, die übersprungen wurden, da sie vom Quellenreplikationsserver nicht an den Zielreplikationsserver übertragen werden konnten.

Summe der noch nicht replizierten Byte (MB)

Die Gesamtzahl der Byte, die noch nicht an den Zielreplikationsserver übertragen wurden.

Geschätzte Fertigstellung in Prozent

- Die geschätzte Fertigstellung in Prozent auf der Basis der Anzahl der Byte.
- Geschätzte verbleibende Zeit
- Die geschätzte verbleibende Zeit bis zum Abschluss des Knotenreplikationsprozesses.
- Geschätzte Zeit der Fertigstellung
- Die geschätzte Zeit, zu der der Knotenreplikationsprozess beendet sein wird.

Tabelle 1. Zugehörige Befehle für QUERY REPLICATION

| Befehl             | Beschreibung  |
|--------------------|---|
| CANCEL REPLICATION | Bricht Knotenreplikationsprozesse ab.   |
| QUERY ACTLOG       | Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.                          |
| QUERY FILESPACE    | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.   |
| QUERY NODE         | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an. |
| QUERY PROCESS      | Zeigt Informationen über Hintergrundprozesse an.                                  |
| QUERY REPLNODE     | Zeigt Informationen zum Replikationsstatus eines Clientknotens an.                |
| QUERY REPLRULE     | Zeigt Informationen zu Knotenreplikationsregeln an.                               |
| REPLICATE NODE     | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.            |
| SET REPLRETENTION  | Gibt den Aufbewahrungszeitraum für Replikationsprotokollsätze an.                 |

## QUERY REPLNODE (Informationen zum Replikationsstatus für einen Clientknoten anzeigen)

Verwenden Sie diesen Befehl, um die Anzahl der Dateien anzuzeigen, die für jeden replizierten Dateibereich gespeichert werden. Informationen werden zu Dateibereichen für jeden Clientknoten angezeigt, der für die Replikation konfiguriert ist.

Ein Clientknoten ist für die Replikation konfiguriert, wenn er aktiviert oder inaktiviert ist.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

>>-Query REPLNode-----Knotenname-----+-----Zielservename- '<
      v                                     |
      .-----'
  
```

### Parameter

Knotenname (Erforderlich)

Gibt den Clientknoten an, der der Eigner der Dateien ist, zu denen Informationen angezeigt werden sollen. Sie können einen oder mehrere Namen angeben. Werden mehrere Namen angegeben, sind die Namen durch Kommas voneinander zu trennen. Verwenden Sie zwischen den Namen keine Leerzeichen. Es können Platzhalterzeichen verwendet werden, um mehrere Namen anzugeben.

Informationen zu Clientknoten, die den Dateikriterien entsprechen, aber nicht für die Replikation konfiguriert sind, werden nicht angezeigt.

Zielservename

Gibt den Namen des Replikationsservers an, der nach Replikationsinformationen abgefragt werden soll. Dieser Parameter ist wahlfrei. Wenn Sie keinen Wert für diesen Parameter angeben, wird der Server, der das Standardziel für replizierte Daten ist, abgefragt.



Als Wert für diesen Parameter können Sie auch einen Server angeben, der früher ein Ziel für replizierte Daten war.

Die Clientknoten, die für einen Replikationsserver definiert sind, können die Quelle oder das Ziel der replizierten Daten sein. Um zu bestimmen, ob ein bestimmter Clientknoten Daten sendet oder empfängt, geben Sie den Befehl QUERY NODE aus. Suchen Sie im Feld 'Replikationsmodus' der Ausgabe nach dem Wert *Send* oder *Receive*.

Um den Namen des aktiven Zielreplikationsservers anzuzeigen, geben Sie den Befehl QUERY STATUS aus und suchen Sie den Namen im Feld 'Zielreplikationsserver'.

## Beispiel: Clientknotendateien auf einem Quellen- und einem Zielreplikationsserver auflisten

Der Name des Clientknotens ist NODE1.

```
query replnode *
```

| Knoten-<br>name | Typ  | Dateibereich-<br>Name | FSID | Dateien<br>auf Server | Replikations-<br>server (1) | Dateien<br>auf Server (1) |
|-----------------|------|-----------------------|------|-----------------------|-----------------------------|---------------------------|
| NODE1           | SpMg | /hmsmfs               | 1    | 1                     |                             |                           |
| NODE1           | Bkup | /lspace2              | 2    | 27                    |                             |                           |
| NODE1           | Arch | /lspace2              | 2    | 22                    | TGTSRV                      | 22                        |
| NODE1           | Bkup | /lspace               | 3    | 18.096                |                             |                           |
| NODE1           | Arch | /lspace               | 3    | 61.150                | TGTSRV                      | 61.150                    |
| NODE2           |      |                       |      |                       |                             |                           |

Die Anzahl der Dateien, die für die Replikationsserver angezeigt werden, kann aus folgenden Gründen abweichen:

- Die Ausgabe des Befehls QUERY REPLNODE zeigt die Anzahl der Dateien an, die aus der Belegungstabelle abgerufen wurden. Die Belegungstabelle enthält nur Dateien, die eine Länge größer als Null haben. Dateien, die die Länge 0 haben und repliziert wurden, werden in dieser Ausgabe nicht wiedergespiegelt.
- Wenn nur aktive Daten auf den Zielserver repliziert werden, ist die Anzahl der Dateien, die für den Quellenserver angezeigt werden, größer als die Anzahl der Dateien, die auf dem Zielserver angezeigt werden. Die Ursache für die Abweichung liegt darin, dass der Quellenreplikationsserver sowohl über aktive als auch über inaktive Daten und der Zielserver nur über aktive Daten verfügt.
- Ein Clientknoten kann über Daten verfügen, die vom Quellenreplikationsserver exportiert und auf den Zielreplikationsserver importiert wurden. Wenn diese Daten synchronisiert wurden und wenn der Clientknoten auch Daten auf dem Zielreplikationsserver gespeichert hat, ist die Anzahl der Dateien auf dem Zielreplikationsserver größer als die Anzahl der Dateien, die infolge von Export- und Importoperationen und der Replikation gespeichert wurden.
- Wenn Sie Knotendaten von einem Quellenserver mit einer Version vor Version 7.1 auf einen Zielserver mit Version 7.1 oder höher replizieren, werden Dateien mit mehr als 10 GB in kleinere Dateien aufgeteilt, wenn der Parameter SPLITLARGEOBJECTS für die Knotendefinition auf *Yes* gesetzt ist. Alle diese Teildateien werden auf dem Zielserver gezählt.

## Feldbeschreibungen

### Knotenname

Der Name des Clientknotens, der der Eigner der Dateien ist.

### Typ

Der Datentyp. Ist dieses Feld leer, ist der Clientknoten für die Replikation konfiguriert, aber er verfügt über keine Daten auf dem Replikationsserver. In der Beispielausgabe ist NODE2 für die Replikation konfiguriert, aber der Knoten verfügt über keine Sicherungsdaten, Archivierungsdaten oder speicher verwaltete Daten.

Die folgenden Werte sind gültig:

#### Arch

Archivierungsdaten

#### Bkup

Sicherungsdaten

#### SpMg

Daten, die von IBM Spectrum Protect for Space Management-Clients umgelagert wurden

### Dateibereichsname

Der Name des Dateibereichs, der zu dem Knoten gehört.

Ist dieses Feld leer, ist der Clientknoten für die Replikation konfiguriert, aber er verfügt über keine Daten auf dem Replikationsserver.

Dateibereichsnamen können eine andere Zeichenumsetzungstabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten

werden normal gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetztabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetztabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

#### FSID

Die Dateibereichs-ID des Dateibereichs. Der Server ordnet eine eindeutige FSID zu, wenn ein Dateibereich zum ersten Mal auf dem Server gespeichert wird. Ist dieses Feld leer, ist der Clientknoten für die Replikation konfiguriert, aber er verfügt über keine Daten auf dem Replikationsserver.

#### Dateien auf Server

Die Anzahl der Sicherungsdateien, Archivierungsdateien und speicher verwalteten Dateien auf dem Server, auf dem dieser Befehl ausgegeben wird. Ist dieses Feld leer, ist der Clientknoten für die Replikation konfiguriert, aber er verfügt über keine Daten auf dem Replikationsserver.

#### Replikationsserver (1)

Der Name des Replikationsservers, der nach Informationen abgefragt wird. Ist dieses Feld leer, können eine oder mehrere der folgenden Bedingungen vorhanden sein:

- Der Dateibereich des Knotens auf dem Replikationsserver, auf dem der Befehl ausgegeben wurde, verfügt über keine Daten.
- Der Clientknoten ist nicht auf dem Replikationsserver (1) definiert.
- Der Clientknoten ist auf dem Replikationsserver (1) definiert, aber der Knoten ist nicht für die Replikation konfiguriert.
- Der entsprechende Dateibereich auf dem Replikationsserver (1) verfügt über keine Daten oder der Dateibereich ist nicht definiert.

#### Dateien auf Server (1)

Die Anzahl der Dateien für den Datentyp, die auf dem Zielreplikationsserver gespeichert sind. Dieses Feld kann leer sein. Ist dies der Fall, können eine oder mehrere der folgenden Bedingungen vorhanden sein:

- Der Replikationsserver (1) verfügt über keine Daten.
- Der Clientknoten ist nicht auf dem Replikationsserver (1) definiert.
- Der Clientknoten ist auf dem Replikationsserver (1) definiert, aber der Knoten ist nicht für die Replikation konfiguriert.
- Der entsprechende Dateibereich auf dem Replikationsserver (1) verfügt über keine Daten oder der Dateibereich ist nicht definiert.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY REPLNODE

| Befehl            | Beschreibung  |
|-------------------|---|
| QUERY FILESPACE   | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.   |
| QUERY NODE        | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an. |
| QUERY REPLICATION | Zeigt Informationen zu Knotenreplikationsprozessen an.                            |
| QUERY REPLRULE    | Zeigt Informationen zu Knotenreplikationsregeln an.                               |
| REPLICATE NODE    | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.            |
| UPDATE REPLRULE   | Aktiviert oder inaktiviert Replikationsregeln.                                    |

## QUERY REPLRULE (Replikationsregeln abfragen)

Verwenden Sie diesen Befehl, um Informationen zu Replikationsregeln anzuzeigen.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

## Berechtigungs-klasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

---

```
.-*----->
>>-Query REPLRule-----<
'---ALL_DATA-----'
+-ACTIVE_DATA-----+
+-ALL_DATA_HIGH_PRIORITY-----+
'-ACTIVE_DATA_HIGH_PRIORITY--'
```

## Berechtigungsklasse

---

Jeder Administrator kann diesen Befehl ausgeben.

## Parameter

---

### Regelname

Gibt den Namen der Replikationsregel an, zu der Informationen angezeigt werden sollen. Dieser Parameter ist wahlfrei. Sie können Platzhalterzeichen verwenden, um eine oder mehrere Regeln anzugeben. Wenn Sie diesen Parameter nicht angeben, werden Informationen zu allen Regeln in der Ausgabe der Abfrage angezeigt. Sie können die folgenden Werte angeben:

### ALL\_DATA

Zeigt Informationen zu der Replikationsregel ALL\_DATA an. Mit dieser Regel werden Sicherungsdaten, Archivierungsdaten oder speicher verwaltete Daten repliziert. Die Daten werden mit einer normalen Priorität repliziert.

### ACTIVE\_DATA

Zeigt Informationen zu der Replikationsregel ACTIVE\_DATA an. Mit dieser Regel werden nur aktive Sicherungsdaten repliziert. Die Daten werden mit einer normalen Priorität repliziert. Diese Regel ist für Archivierungsdaten oder speicher verwaltete Daten nicht gültig.

Achtung: Wenn Sie ACTIVE\_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

- Wenn eine frühere Serverversion als Version 7.1.1 auf dem Quellen- oder Zielreplikationsserver installiert ist.
- Wenn Sie den Befehl REPLICATE NODE mit dem Parameter `FORCERECONCILE=YES` verwenden.
- Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Serverversion vor Version 7.1.1 ausführen.

Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

### ALL\_DATA\_HIGH\_PRIORITY

Zeigt Informationen zu der Regel ALL\_DATA\_HIGH\_PRIORITY an. Mit dieser Regel werden Sicherungsdaten, Archivierungsdaten oder speicher verwaltete Daten repliziert. Die Daten werden mit einer normalen Priorität repliziert. In einem Replikationsprozess werden Daten mit hoher Priorität vor Daten mit normaler Priorität repliziert.

### ACTIVE\_DATA\_HIGH\_PRIORITY

Zeigt Informationen zu der Regel ACTIVE\_DATA\_HIGH\_PRIORITY an.

Diese Regel entspricht der Replikationsregel ACTIVE\_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden.

## Beispiel: Informationen zu einer Serverreplikationsregel anzeigen

---

Der Name der Regel lautet ALL\_DATA\_HIGH\_PRIORITY.

```
query replrule all_data_high_priority
```

```
Name der Replikationsregel: ALL_DATA_HIGH_PRIORITY
                          Zielreplikationsserver:
                          Nur aktive: No
```

```
Aktiviert: Ja
```

## Feldbeschreibungen

---

### Name der Replikationsregel

Gibt den Namen der Regel an, die abgefragt wurde.

### Zielreplikationsserver

Gibt den Namen des Zielreplikationsservers an.

#### Nur aktive

Gibt an, ob die Regel nur für aktive Sicherungsdaten gilt. Die folgenden Werte sind gültig:

Yes

Gibt an, dass nur aktive Sicherungsdaten für Dateibereiche repliziert werden, denen diese Regel zugeordnet ist.

No

Gibt an, dass alle Sicherungsdaten für Dateibereiche repliziert werden, denen diese Regel zugeordnet ist.

#### Aktiviert

Gibt an, ob die Regel aktiviert oder inaktiviert ist. Die folgenden Werte sind gültig:

Yes

Gibt an, dass die Regel für die Replikation aktiviert ist. Daten in Dateibereichen, denen die Regel zugeordnet ist, werden repliziert.

No

Gibt an, dass die Regel nicht für die Replikation aktiviert ist. Daten in Dateibereichen, denen die Regel zugeordnet ist, werden nicht repliziert.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY REPLRULE

| Befehl            | Beschreibung   |
|-------------------|--|
| QUERY REPLICATION | Zeigt Informationen zu Knotenreplikationsprozessen an.             |
| QUERY REPLNODE    | Zeigt Informationen zum Replikationsstatus eines Clientknotens an. |
| UPDATE REPLRULE   | Aktiviert oder inaktiviert Replikationsregeln.                     |

## QUERY REPLSERVER (Replikationsserver abfragen)

Verwenden Sie diesen Befehl, um Informationen zu allen Replikationsservern anzuzeigen, die dem Server bekannt sind. Die Ausgabe dieses Befehls schließt Serverinformationen für den Server ein, auf dem der Befehl ausgegeben wurde. Der Befehl gibt an, ob eine Replikationsserverdefinition als Ergebnis eines Befehls REMOVE REPLSERVER gelöscht wird.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-Query REPLServer .-*-----  
+-----+-----<<  
'-Servername-'
```

## Beispiel: Übersichtsstatistik zu allen Replikationsservern anzeigen

Informationen zum Replikationsserver anzeigen. Den Befehl entweder auf dem Quellen- oder dem Zielreplikationsserver ausgeben:

```
query replserver *
```

```
Global eindeutige Replikations-ID: 4d.83.fc.30.67.c1.11.e1.b8.  
40.f0.de.f1.5e.f1.89  
Servername: Server1  
Letzte Replikation:  
Überwachungssignal:  
Adresse höherer Ebene für Übernahme: server1.example.com  
TCP-Anschlussnummer für Übernahme: 1500  
SSL-Anschlussnummer für Übernahme: 1542  
Löschen aktiv: No  
Ungleiche Maßnahmen:  
  
Global eindeutige Replikations-ID: 91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.27.00.58.dc  
Servername: DRServer1  
Letzte Replikation: 06/30/2012 08:16:30 PM  
Überwachungssignal: 07/09/2012 22:15:22 PM
```

```

Adresse höherer Ebene für Übernahme: drserver1.example.com
TCP-Anschlussnummer für Übernahme: 1500
SSL-Anschlussnummer für Übernahme: 1542
    Löschen aktiv: No
    Ungleiche Maßnahmen: On
Global eindeutige Replikations-ID: 90.4f.53.b0.8e.cb.11.e3.a8.
    2f.00.14.5e.55.b3.67
    Servername: DRSERVER2
        Letzte Replikation: 04/01/14   12:38:28
        Überwachungssignal: 05/29/14   11:15:44
Adresse höherer Ebene für Übernahme: drserver2.example.com
TCP-Anschlussnummer für Übernahme: 1500
    SSL-Anschlussnummer für Übernahme:
        Löschen aktiv: No
        Ungleiche Maßnahmen: Off

```

## Beispiel: Übersichtsstatistik zu einem bestimmten Replikationsserver anzeigen

---

Informationen zum Replikationsserver DRServer1 anzeigen. Den Befehl entweder auf dem Quellen- oder dem Zielreplikationsserver ausgeben:

```
query replserver drserver1
```

```

Global eindeutige Replikations-ID: 91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.27.00.58.dc
    Servername: DRServer1
        Letzte Replikation: 06/30/2012 08:16:30 PM
        Überwachungssignal: 07/09/2012 22:15:22 PM
Adresse höherer Ebene für Übernahme: drserver1.example.com
TCP-Anschlussnummer für Übernahme: 1500
SSL-Anschlussnummer für Übernahme: 1542
    Löschen aktiv: No
    Ungleiche Maßnahmen: On

```

## Parameter

---

### Servername

Gibt den Namen des Replikationsservers an, der abgefragt werden soll. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Alle übereinstimmenden Server werden abgefragt. Wird kein Wert für diesen Parameter angegeben, werden alle Server abgefragt. Der Parameter ist wahlfrei.

## Feldbeschreibungen

---

### Global eindeutige Replikations-ID

Die eindeutige ID für den IBM Spectrum Protect-Server. Die Werte für die global eindeutige Replikations-ID werden erstellt, wenn ein Server zum ersten Mal in einem Replikationsprozess verwendet wird.

Tipp: Die im Feld 'Global eindeutige Replikations-ID' aufgelistete ID ist nicht mit dem Wert für die ID im Feld 'Maschinen-GUID' identisch, das im Befehl QUERY STATUS angezeigt wird.

### Servername

Der Name des Replikationsservers.

### Letzte Replikation

Das Datum des letzten Replikationsprozesses, in dem der Server verwendet wurde.

### Überwachungssignal

Das letzte Mal, dass der Server eine erfolgreiche Testkommunikationssitzung beendet hat.

### TCP-Anschlussnummer für Übernahme

Der aktive TCP-Clientanschluss (TCP = Transmission Control Protocol) auf dem Replikationsserver, der für Clientverbindungen verwendet wird. Wenn der Client für TCP konfiguriert ist, wird der Anschluss verwendet, um die Verbindung zum Übernahmeserver herzustellen.

### SSL-Anschlussnummer für Übernahme

Der aktive SSL-Anschluss (SSL = Secure Sockets Layer) auf dem Replikationsserver, der für Clientverbindungen verwendet wird. Wenn der Client für SSL konfiguriert ist, wird der Anschluss verwendet, um die Verbindung zum Übernahmeserver herzustellen.

### Adresse höherer Ebene für Übernahme

Die Adresse der höheren Ebene, die der Client verwendet, um während einer Übernahme die Verbindung zum Replikationsserver herzustellen.

### Löschen aktiv

Gibt an, ob ein Befehl REMOVE REPLSERVER für diesen Replikationsserver ausgegeben wurde und der Befehl noch ausgeführt wird. Die folgenden Werte sind gültig:

#### Yes

Das Löschen des Replikationsservers ist aktiv.

No

Das Löschen des Replikationsservers ist nicht aktiv.

Ungleiche Maßnahmen

Gibt an, ob die Maßnahmen, die auf dem Zielreplikationsserver definiert sind, aktiviert sind. Die folgenden Werte sind gültig:

On

Die Maßnahmen auf dem Zielreplikationsserver verwalten replizierte Clientknotendaten.

Off

Die Maßnahmen auf dem Quellenreplikationsserver verwalten replizierte Clientknotendaten.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY REPLSERVER

| Befehl   | Beschreibung                               |
|--|--|
| REMOVE REPLNODE (Clientknoten aus Replikation entfernen) | Entfernt einen Knoten aus der Replikation. |
| REMOVE REPLSERVER (Replikationsserver entfernen)         | Entfernt einen Server aus der Replikation. |

## QUERY REQUEST (Anstehende Ladeanforderungen abfragen)

Verwenden Sie den Befehl QUERY REQUEST, um Informationen über eine oder mehrere anstehende Ladeanforderungen anzuzeigen. Der Server gibt Anforderungen an den Administrator zum Ausführen einer Aktion aus, wie beispielsweise zum Einlegen eines Banddatenträgers in ein Kassettenarchiv, nachdem ein Befehl CHECKIN LIBVOL ausgegeben wurde.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-Query REQuest-----+-----><
                        '-Anforderungsnummer-'
```

## Parameter

Anforderungsnummer

Gibt die Identifikationsnummer der anstehenden Ladeanforderung an. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle anstehenden Ladeanforderungen.

## Beispiel: Alle anstehenden Ladeanforderungen auflisten

Informationen zu allen anstehenden Ladeanforderungen anzeigen, nachdem ein Befehl CHECKIN LIBVOL ausgegeben wurde.

```
query request
```

## Ausgabe für ein manuelles Kassettenarchiv

### AIX-Betriebssysteme

```
ANR8352I Ausstehende Anforderungen:
ANR8326I 001: 8MM Datenträger EXP001 R/W
in Laufwerk 8MM.1 (/dev/mt0) des Kassettenarchivs
MANUALLIB innerhalb von 60 Minuten laden.
```

### Linux-Betriebssysteme

```
ANR8352I Ausstehende Anforderungen:
ANR8326I 001: 8MM Datenträger EXP001 R/W
in Laufwerk 8MM.1 (/dev/mt0) des Kassettenarchivs
MANUALLIB innerhalb von 60 Minuten laden.
```

### Windows-Betriebssysteme

ANR8352I Ausstehende Anforderungen:  
 ANR8326I 001: GENERICTAPE Datenträger EXP001 R/W  
 in Laufwerk 8MM.1 (mt3.0.0.0) des Kassettenarchivs  
 MANUALLIB innerhalb von 60 Minuten laden.

## Ausgabe für ein automatisiertes Kassettenarchiv

ANR8352I Ausstehende Anforderungen:  
 ANR8306I 001: LTO-Datenträger 133540L5 R/W in den Schacht mit Elementnummer  
 31 des Kassettenarchivs LTOLIB innerhalb von 60 Minuten einlegen; wenn bereit, 'REPLY'  
 mit der Anforderungs-ID ausgeben.

ANR8352I Ausstehende Anforderungen:  
 ANR8306I 001: 3590 Datenträger 133540 R/W in den Schacht mit Elementnummer  
 31 des Kassettenarchivs 3590LIB innerhalb von 60 Minuten einlegen; wenn bereit, 'REPLY'  
 mit der Anforderungs-ID ausgeben.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY REQUEST

| Befehl         | Beschreibung  |
|----------------|---|
| CANCEL REQUEST | Bricht anstehende Datenträgerladeanforderungen ab.        |
| REPLY          | Erlaubt einer Anforderung, die Verarbeitung fortzusetzen. |

## QUERY RESTORE (Wiederanlauffähige Zurückschreibungssitzungen abfragen)

Mit diesem Befehl können Informationen über die wiederanlauffähigen Zurückschreibungssitzungen angezeigt werden.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-Query--REStore-+-----+-----+-----+-----+----->
                    '-Knotenname-'  '-Dateibereichsname-'

.-Format----Standard-----.-NAMEType----SERVER-----
>-+-----+-----+-----+-----+-----<
'-Format----+Standard-+-'  '-NAMEType----+SERVER-+-'
                    '-Detailed-'          +-UNICode-+
                                         '-FSID----'
```

## Parameter

### Knotenname

Gibt den Clientknoten an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Wird kein Wert angegeben, werden alle Clientknoten mit wiederanlauffähigen Zurückschreibungssitzungen angezeigt. Für diesen Parameter muss ein Wert angegeben werden, wenn ein Dateibereichsname angegeben wird.

### Dateibereichsname

Gibt den Dateibereich an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Wird kein Wert angegeben, werden alle Dateibereiche für den angegebenen Knoten abgefragt.

Ein Server, der über Clients mit Unterstützung für Unicode verfügt, muss möglicherweise den Dateibereichsnamen, den Sie eingeben, konvertieren. Beispielsweise muss der Server gegebenenfalls den Namen, den Sie eingeben, aus der Zeichenumsetztabelle des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich unter dem Parameter NAME TYPE.

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

Standard

Gibt an, dass Teilinformationen angezeigt werden.

Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

NAMETYPE

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unterstützung für Unicode verfügt. Sie können diesen Parameter für IBM Spectrum Protect-Clients mit Unicode-Unterstützung angeben, die die Betriebssysteme Windows, Macintosh OS 9, Macintosh OS X und NetWare verwenden.

Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen eingeben. Der Standardwert lautet SERVER. Gültige Werte:

SERVER

Der Server verwendet die Zeichenumsetzungstabelle des Servers, um die Dateibereichsnamen zu interpretieren.

UNICODE

Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetzungstabelle in die Zeichenumsetzungstabelle UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetzungstabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetzungstabelle nicht verfügbar sind oder wenn der Server Probleme beim Zugriff auf die Systemkonvertierungsroutinen hat.

FSID

Der Server interpretiert die Dateibereichsnamen als ihre Dateibereichs-IDs (FSIDs).

## Beispiel: Eine wiederanlauffähige Zurückschreibungssitzung für einen bestimmten Clientknoten anzeigen

---

Zeigen Sie ausführliche Informationen zum Clientknoten JAMES an, der dem Dateibereich DRIVE\_F\_R zugeordnet ist. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query restore james drive_f_r format=detailed

Sitzungsnummer: -1
Zurückschreibungsstatus: Wiederanlauffähig
  Abgelaufene Minuten: 2
    Knotenname: JAMES
      FSID: 1
        Dateibereichsname: DRIVE_F_R:
          Dateispezifikation: /RESTORE/TESTDIR\
```

## Feldbeschreibungen

---

Sitzungsnummer

Gibt die Sitzungsnummer für die wiederanlauffähige Zurückschreibungssitzung an. Die Nummer für aktive Zurückschreibungssitzungen entspricht der im Befehl QUERY SESSION angezeigten Nummer. Bei Zurückschreibungssitzungen im wiederanlauffähigen Status wird eine negative Zahl als Sitzungsnummer angezeigt. Alle in der Ausgabe des Befehls QUERY RESTORE angezeigten Sitzungsnummern können von der Ausgabe des Befehls QUERY RESTORE angegeben werden.

Zurückschreibungsstatus

- Aktiv: Gibt an, dass die Zurückschreibungssitzung Dateien aktiv in den Client zurückschreibt.
- Wiederanlauffähig: Gibt an, dass die Zurückschreibungssitzung fehlgeschlagen ist und an dem Unterbrechungspunkt erneut gestartet werden kann.

Abgelaufene Minuten

Gibt die Anzahl Minuten seit dem Start der Zurückschreibungssitzung an. Alle wiederanlauffähigen Zurückschreibungssitzungen, deren abgelaufene Zeit größer als die Serveroption RESTOREINTERVAL ist, können bei Bedarf oder während der Verfallsverarbeitung automatisch aus der Datenbank gelöscht werden. Ist die abgelaufene Zeit kürzer als RESTOREINTERVAL, kann dieser Eintrag nur gelöscht werden (und der Dateibereich freigegeben werden), indem der Befehl CANCEL RESTORE ausgegeben und der Wert für RESTOREINTERVAL herabgesetzt wird.

Knotenname

Gibt den Knoten an, der der wiederanlauffähigen Zurückschreibungssitzung zugeordnet ist.

FSID

Gibt die Dateibereichs-ID des Dateibereichs an.

Dateibereichsname

Gibt den Dateibereich an, der der wiederanlauffähigen Zurückschreibungssitzung zugeordnet ist.



Dateibereichsnamen können eine andere Zeichenumsetztabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetztabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetztabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

#### Dateispezifikation

Gibt die Dateispezifikation an, die in der Operation zum Zurückschreiben verwendet wird. Dieselbe Dateispezifikation muss angegeben werden, wenn eine fehlgeschlagene Operation zum Zurückschreiben an ihrem Unterbrechungspunkt erneut gestartet werden soll.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY RESTORE

| Befehl         | Beschreibung  |
|----------------|---|
| CANCEL RESTORE | Bricht eine wiederanlauffähige Zurückschreibungssitzung ab. |

## QUERY RPFCONTENT (Inhalt der auf Zielsever gespeicherten Plandatei abfragen)

Verwenden Sie diesen Befehl, um den Inhalt einer Wiederherstellungsplandatei anzuzeigen, die auf einem Zielsever gespeichert ist (d. h., wenn der Parameter DEVCLASS im Befehl PREPARE angegeben wurde). Dieser Befehl kann entweder von dem Server, der die Datei erstellt hat (Quellen-Server), oder von dem Server, auf dem die Wiederherstellungsplandatei gespeichert ist (Ziel-Server), ausgegeben werden. Dieser Befehl kann nicht über die Server-Konsole ausgegeben werden.

Die Ausgabe kann sich verzögern, wenn sich die Datei auf Band befindet.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Query RPFContent--Plandateiname----->
>--+DEVclass----Einheitenklassenname+-----<
'-NODENAME----Knotennamenname-----'
```

## Parameter

#### Plandateiname (Erforderlich)

Gibt den Namen der Wiederherstellungsplandatei an, die abgefragt werden soll. Das Format des Dateinamens lautet servername.yyyymmdd.hhmmss. Sollen die Namen von vorhandenen Dateien angezeigt werden, den Befehl QUERY RPFFILE ausgeben.

#### DEVclass

Gibt den Namen der Einheitenklasse an, die zum Erstellen der Wiederherstellungsplandatei verwendet wurde. Platzhalterzeichen sind nicht zulässig.

Diesen Parameter angeben, wenn

- der Inhalt der Wiederherstellungsplandatei angezeigt werden soll, die für diesen Server erstellt wurde.
- Dieser Befehl wird für denselben Server ausgegeben, auf dem der Befehl PREPARE ausgegeben wurde (Quellenserver).
- Der angegebene Einheitenklassenname wurde in dem Befehl PREPARE verwendet, mit dem die Wiederherstellungsplandatei erstellt wurde.

#### NODENAME

Gibt den auf dem Ziel-Server registrierten Knotennamen des Quellen-Servers an, der die Wiederherstellungsplandatei erstellt hat. Platzhalterzeichen sind nicht zulässig.

Diesen Parameter angeben, wenn

- der Inhalt der Wiederherstellungsplandatei angezeigt werden soll, die auf diesem Server gespeichert war.
- dieser Befehl für den Server ausgegeben wird, der das Ziel des Befehls PREPARE war, der die Wiederherstellungsplandatei erstellt hat.
- der angegebene Knotenname auf diesem Server mit der Knotenart SERVER registriert ist.
- der IBM Spectrum Protect-Server, der die Wiederherstellungsplandatei erstellt hat, nicht verfügbar ist.

## Beispiel: Den Wiederherstellungsplan für den Quellenserver anzeigen

Auf dem Quellenserver den Inhalt einer Wiederherstellungsplandatei anzeigen, die für diesen Server am 19. März 1998 um 6:10 Uhr erstellt wurde. Der Befehl PREPARE gibt die Einheitenklasse REMOTE an. Die Ausgabe dieses Befehls ist der gesamte Inhalt der Wiederherstellungsplandatei.

```
query rpfcontent branch1.19980319.061000 devclass=remote
```

## Beispiel: Den Wiederherstellungsplan für den Zielservers anzeigen

Auf dem Zielservers den Inhalt einer Wiederherstellungsplandatei anzeigen, die auf diesem Server am 19. März 1998 um 6:10 Uhr gespeichert wurde. Der Server, der die Datei erstellt hat, ist auf dem Zielservers als Knoten POLARIS mit der Knotenart SERVER registriert. Die Ausgabe dieses Befehls ist der gesamte Inhalt der Wiederherstellungsplandatei.

```
query rpfcontent branch1.19980319.061000 nodename=polaris
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY RPFCONTENT

| Befehl           | Beschreibung   |
|------------------|--|
| PREPARE          | Erstellt eine Wiederherstellungsplandatei.   |
| QUERY RPFFILE    | Zeigt Informationen über Wiederherstellungsplandateien an.                         |
| QUERY VOLHISTORY | Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden. |

### Zugehörige Informationen:

 Wiederherstellungsplandatei

## QUERY RPFFILE (Auf Zielservers gespeicherte Infos über Plandateien abfragen)

Mit diesem Befehl können Informationen über Wiederherstellungsplandateien angezeigt werden, die auf einem Ziel-Servers gespeichert sind. Dieser Befehl kann entweder von dem Server, der die Datei erstellt hat (Quellen-Servers), oder von dem Server, auf dem die Wiederherstellungsplandatei gespeichert ist (Ziel-Servers), ausgegeben werden.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-Query RPFfile---+DEVclass----+Einheitenklassenname+----->
      '-NODENAME----+Knotenname-----'

  .-Source-----+DBBackup-----+ .-Format----+Standard-----+
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+
  '-Source-----+DBBackup-----+' '-Format----+Standard+++'
      '-DBSnapshot-'                '-Detailed-'
```

## Parameter

### DEVclass

Gibt den Namen der Einheitenklasse an, die zum Erstellen der Wiederherstellungsplandateien verwendet wurde. Diesen Parameter verwenden, wenn die Anmeldung an dem Server erfolgte, der die Wiederherstellungsplandatei erstellt hat. Es können

Platzhalterzeichen in dem Namen der Einheitenklasse verwendet werden. Alle Wiederherstellungsplandateien, die mit der angegebenen Einheitenklasse erstellt werden, werden in der Abfrage berücksichtigt.

#### NODENAME

Gibt den auf dem Ziel-Server registrierten Knotennamen des Quellen-Servers an, der die Wiederherstellungsplandateien erstellt hat. Diesen Parameter verwenden, wenn die Anmeldung an dem Ziel-Server erfolgte. Dieser Parameter kann verwendet werden, wenn der Quellen-Server nicht verfügbar ist. Es können Platzhalterzeichen verwendet werden, um den Knotennamen anzugeben. Alle Dateiobjekte, die mit dem angegebenen Knotennamen gespeichert sind, werden in dieser Abfrage berücksichtigt.

#### SOURCE

Gibt die Art der Datenbanksicherung an, die bei der Vorbereitung der Wiederherstellungsplandatei angegeben wurde. Dieser Parameter ist wahlfrei. Der Standardwert ist DBBACKUP. Gültige Werte:

##### DBBackup

Die Wiederherstellungsplandatei wurde mit angegebenen Gesamtsicherungen und Teilsicherungen der Datenbank vorbereitet.

##### DBSnapshot

Die Wiederherstellungsplandatei wurde mit angegebenen Datenbankmomentaufnahmesicherungen vorbereitet.

#### FORMAT

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

##### Standard

Zeigt Teilinformationen für die Wiederherstellungsplandatei an.

##### Detailed

Zeigt alle Informationen für die Wiederherstellungsplandatei an.

## Beispiel: Ausführliche Informationen zu den Wiederherstellungsplänen anzeigen

---

Wiederherstellungsplandateien anzeigen, die für diesen Server unter Verwendung der angegebenen Einheitenklasse erstellt wurden. Für Felddesreibungen siehe Felddesreibungen.

```
query rpf file devclass=* format=detailed
```

```
Name der Wiederherstellungsplandatei: ALASKA.20000406.170423
      Knotenname: BRANCH1
      Einheitenklassenname: REMOTE
Art der Wiederherstellungsplandatei: RPF FILE
      Verwaltungsklassenname: STANDARD
Größe der Wiederherstellungsplandatei: 16,255 Bytes
      Zum Löschen markiert: Yes
      Löschdatum: 06/12/2000 13:05:31

Name der Wiederherstellungsplandatei: ALASKA.20000407.170845
      Knotenname: BRANCH1
      Einheitenklassenname: REMOTE
Art der Wiederherstellungsplandatei: RPF SNAPSHOT
      Verwaltungsklassenname: STANDARD
Größe der Wiederherstellungsplandatei: 16,425 Byte
      Zum Löschen markiert: No
      Löschdatum:
```

## Beispiel: Eine Liste der Wiederherstellungspläne für einen bestimmten Knotennamen anzeigen

---

Eine Liste aller Wiederherstellungsplandateiobjekte anzeigen, die mit dem angegebenen Knotennamen (TYPE=SERVER) gespeichert sind. Für Felddesreibungen siehe Felddesreibungen.

```
query rpf file nodename=branch1
```

| Wiederherstellungsplandatei | Knotenname | Einheitenklassenname |
|-----------------------------|------------|----------------------|
| -----                       | -----      | -----                |
| ALASKA.19980406.170423      | BRANCH1    | REMOTE               |
| ALASKA.19980407.170845      | BRANCH1    | REMOTE               |

## Felddesreibungen

---

#### Name der Wiederherstellungsplandatei

Der Name der Wiederherstellungsplandatei.

#### Knotenname

Der Knotenname, der mit dem Zielsystem registriert ist und zum Speichern der Wiederherstellungsplandateiobjekte verwendet wird.

#### Einheitenklassenname

Der Einheitenklassenname, der im Quellenserver definiert ist und zum Erstellen der Wiederherstellungsplandateien verwendet wird.

#### Art der Wiederherstellungsplandatei

Die Art der Wiederherstellungsplandatei:

##### RPFFILE

Der Plan nimmt Gesamt- und Teilsicherungen der Datenbank an.

##### RPFsnapshot

Der Plan nimmt Datenbankmomentaufnahmesicherungen an.

#### Verwaltungsklassenname

Der Name der Verwaltungsklasse, der die Wiederherstellungsplandatei auf dem Ziel-Server zugeordnet ist.

#### Größe der Wiederherstellungsplandatei

Die geschätzte Größe des Wiederherstellungsplandateiobjekts auf dem Ziel-Server.

#### Zum Löschen markiert

Die Angabe, ob das Objekt, das die Wiederherstellungsplandatei enthält, auf dem Quellen-Server gelöscht und auf dem Ziel-Server zum Löschen markiert wurde, wenn der Aufbewahrungszeitraum noch nicht abgelaufen ist. Gültige Werte:

Yes

Das Objekt ist zum Löschen markiert.

No

Das Objekt ist nicht zum Löschen markiert.

#### Löschdatum

Das Datum, an dem das Objekt auf dem Quellen-Server gelöscht und auf dem Ziel-Server zum Löschen markiert wurde. Dieses Feld bleibt leer, wenn das Objekt nicht zum Löschen markiert wurde.


## Zugehörige Befehle


Tabelle 1. Zugehörige Befehle für QUERY RPFFILE


| Befehl           | Beschreibung   |
|------------------|--|
| PREPARE          | Erstellt eine Wiederherstellungsplandatei.   |
| QUERY VOLHISTORY | Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden. |
| QUERY RPFCONTENT | Zeigt den Inhalt einer Wiederherstellungsplandatei an.                             |

## QUERY SAN (Einheiten in dem SAN abfragen)

Verwenden Sie diesen Befehl, um Informationen zu Einheiten abzurufen, die in einem SAN (Storage Area Network - Speicherbereichsnetz) erkannt werden können, so dass Sie IBM Spectrum Protect für die LAN-unabhängige Datenversetzung konfigurieren können.

 **AIX-Betriebssysteme** Der Befehl QUERY SAN erfordert die libhbaapi.a, die die allgemeine SNIA Host Bus Adapter (HBA) API unterstützt. Mit diesem Bibliotheksobjekt kann IBM Spectrum Protect die hbaapi-Funktionen aufrufen, die im allgemeinen SNIA HBA-API-Standard angegeben sind.

 **Windows-Betriebssysteme** Der Befehl QUERY SAN erfordert die hbaapi.dll, die die allgemeine SNIA Host Bus Adapter (HBA) API unterstützt. Mit diesem Bibliotheksobjekt kann IBM Spectrum Protect die hbaapi-Funktionen aufrufen, die im allgemeinen SNIA HBA-API-Standard angegeben sind.

 **Linux-Betriebssysteme** Der Befehl QUERY SAN erfordert die libhbaapi.so, die die allgemeine SNIA Host Bus Adapter (HBA) API unterstützt. Mit diesem Bibliotheksobjekt kann IBM Spectrum Protect die hbaapi-Funktionen aufrufen, die im allgemeinen SNIA HBA-API-Standard angegeben sind.

Mit dem Befehl QUERY SAN werden möglicherweise nicht alle Einheiten angezeigt, wenn die Serveroption SANDISCOVERY nicht auf ON gesetzt ist.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

. -Type----Any----- .

```
>>-Query SAN-----+----->
      '-Type-----+Any-----+'
              +-DRive----+
              '-LIBRARY-'

.-Format-----Standard-----
>-----+-----+-----<
      '-Format-----+Standard-+-'
              '-Detailed-'
```

## Parameter

### Type

Gibt den Typ der Einheit an, die angezeigt wird. Dieser Parameter ist wahlfrei. Der Standardwert ist Any. Gültige Werte:

#### Any

Gibt an, dass alle in dem SAN erkannten Einheiten angezeigt werden.

#### DRive

Gibt an, dass nur Laufwerkeinheiten angezeigt werden.

#### LIBRARY

Gibt an, dass nur Kassettenarchivseinheiten angezeigt werden.

### Format

Gibt die Art der Informationen an, die angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist Standard. Gültige Werte:

#### Standard

Gibt an, dass die angezeigten Informationen zusammengefasst werden.

#### Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

Tipp: Die Ausgabe zeigt möglicherweise nicht die Seriennummer der Einheit an. Ist dies der Fall, suchen Sie die Seriennummer auf der Rückseite der Einheit oder fragen Sie den Hersteller der Einheit.

## Beispiel: Laufwerkeinheiten auflisten

Übersichtsdaten für Laufwerkeinheiten in einem SAN anzeigen. Für Felddesreibungen siehe Felddesreibungen.

```
query san type=drive
```

| Einheitentyp | Lieferant | Produkt | Seriennummer | Einheit   |
|--------------|-----------|---------|--------------|-----------|
| LIBRARY      | STK       | L180    | MPC01000128  | /dev/smc1 |
| DRIVE        | STK       | 9840D   | 331001017229 | /dev/rmt3 |
| DRIVE        | Quantum   | DLT4000 | JF62806275   | /dev/rmt4 |
| DRIVE        | Quantum   | DLT4000 | JP73213185   | /dev/rmt5 |
| DRIVE        | STK       | 9840D   | 331000028779 | /dev/rmt6 |

## Beispiel: Informationen zu Laufwerkeinheiten anzeigen

Ausführliche Informationen zu allen Laufwerkeinheiten in einem SAN anzeigen. Für Felddesreibungen siehe Felddesreibungen.

```
query san type=drive format=detailed
```

```
Einheitentyp:  DRIVE
                Lieferant:  IBM
                Produkt:    03570B02
                Seriennummer:
                Einheit:    mt10.2.0.3
Einheit zum Versetzen von Daten:  No
                Knoten-WWN:  5005076206039E05
                Anschluss-WWN: 5005076206439E05
                LUN:         0
                SCSI-Anschluss: 3
                SCSI-Bus:    0
                SCSI-Ziel:   10
```

## Felddesreibungen

Einheitentyp

|  |
|--|
| Der Typ der Einheit, die angezeigt wird.   |
| Lieferant  |
| Der Name des Lieferanten der Einheit.  |
| Produkt  |
| Der Name des Produkts, der vom Lieferanten zugeordnet wird.  |
| Seriennummer   |
| Die Seriennummer der Einheit.  |
| Einheit  |
| Der Gerätedateiname der Einheit.   |
| Einheit zum Versetzen von Daten  |
| Gibt an, ob die Einheit eine Einheit zum Versetzen von Daten ist.  |
| Knoten-WWN   |
| Der weltweit verwendete Name (World Wide Name) der Einheit.  |
| Anschluss-WWN  |
| Der weltweit verwendete Name (World Wide Name) der Einheit, der für den Anschluss spezifisch ist, mit dem die Einheit verbunden ist. |
| LUN  |
| Die Nummer der logischen Einheit (Logical Unit Number) der Einheit.  |
| SCSI-Anschluss   |
| Der Anschluss des Fibre Channel (oder SCSI) Host Bus Adapter.  |
| SCSI-Bus   |
| Der Bus der Host Bus Adapter-Karte.  |
| SCSI-Ziel  |
| Die Zielnummer der Einheit.  |

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SAN

| Befehl           | Beschreibung  |
|------------------|---|
| DEFINE DATAMOVER | Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server. |
| DEFINE DRIVE     | Ordnet ein Laufwerk einem Kassettenarchiv zu.                                       |
| DEFINE LIBRARY   | Definiert ein automatisiertes oder manuelles Kassettenarchiv.                       |

## QUERY SCHEDULE (Zeitpläne abfragen)

Mit diesem Befehl können Informationen über einen oder mehrere Zeitpläne angezeigt werden.

Für den Befehl QUERY SCHEDULE sind zwei Formate möglich, abhängig davon, ob der Zeitplan für Clientoperationen oder für Verwaltungsbefehle gilt. Syntax und Parameter für jede Operation werden separat definiert. Abhängig davon, ob der Zeitplan eine klassische oder erweiterte Darstellung verwendet, können einige Optionen in der Abfrageanzeige leer sein.

Tabelle 1. Zugehörige Befehle für QUERY SCHEDULE

| Befehl          | Beschreibung  |
|-----------------|---|
| COPY SCHEDULE   | Erstellt eine Kopie eines Zeitplans.  |
| DEFINE SCHEDULE | Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl. |
| UPDATE SCHEDULE | Ändert die Attribute eines Zeitplans.   |

- QUERY SCHEDULE (Clientzeitpläne abfragen)  
Mit diesem Befehl können Informationen über einen oder mehrere Clientzeitpläne angezeigt werden.
- QUERY SCHEDULE (Verwaltungszeitplan abfragen)  
Mit diesem Befehl können Informationen über einen oder mehrere Verwaltungszeitpläne angezeigt werden.

## QUERY SCHEDULE (Clientzeitpläne abfragen)

Mit diesem Befehl können Informationen über einen oder mehrere Clientzeitpläne angezeigt werden.

## Berechtigungsklasse



## Feldbeschreibungen: Zeitpläne für eine bestimmte Maßnahmendomäne

---

### Domäne

Gibt den Namen der Maßnahmendomäne an, zu der der angegebene Zeitplan gehört.

### \* (Stern)

Gibt an, ob ein Zeitplan abgelaufen ist. Steht in dieser Spalte ein Stern, ist der betreffende Zeitplan abgelaufen.

### Zeitplanname

Gibt den Namen des Zeitplans an.

### Aktion

Gibt die Aktion an, die bei der Verarbeitung dieses Zeitplans ausgeführt wird.

### Startdatum/-zeit

Gibt das/die anfängliche Startdatum/Uhrzeit für diesen Zeitplan an.

### Dauer

Gibt die Länge des Startfensters für diesen Zeitplan an.

### Intervall

Gibt die Zeit zwischen den Startfenstern an (bei DAYOFWEEK=ANY). Für erweiterte Zeitpläne ist die Spalte leer.

### Tag

Gibt den Wochentag an, an dem die Startfenster für den Zeitplan beginnen. Für erweiterte Zeitpläne enthält die Spalte einen Stern.

## Beispiel: Ausführliche Clientzeitpläne anzeigen

---

Von einem verwalteten Server ausführliche Informationen über Clientzeitpläne anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen: Ausführliche Clientzeitpläne.

```
query schedule * type=client format=detailed
```

```

      Name der Maßnahmendomäne: ADMIN_RECORDS
      Zeitplanname: ADMIN_BACKUP
      Beschreibung:
      Aktion: Backup
      Subaktion: vApp
      Optionen:
      Objekte:
      Priorität: 5
      Startdatum/-zeit: 04/06/2013 17.04.20
      Dauer: 1 Stunde
Maximale Ausführungszeit (Minuten): 0
      Zeitplandarstellung: Klassisch
      Intervall: 1 Tag(e)
      Wochentag: Any
      Monat:
      Tag des Monats:
      Woche des Monats:
      Verfall:
      Letzte Aktualisierung durch
      (Administrator): $$CONFIG_MANAGER$$
      Datum/Zeit der letzten Aktualisierung: 04/06/2013 17.51.49
      Verwaltendes Profil: ADMIN_INFO

      Name der Maßnahmendomäne: EMPLOYEE_RECORDS
      Zeitplanname: EMPLOYEE_BACKUP
      Beschreibung:
      Aktion: Incremental
      Subaktion:
      Optionen:
      Objekte:
      Priorität: 5
      Startdatum/-zeit: 2004.06.04 17.04.33
      Dauer: 1 Stunde
Maximale Ausführungszeit (Minuten): 0
      Zeitplandarstellung: Erweitert
      Intervall:
      Wochentag: Any
      Monat: Mär,Jun,Nov
      Tag des Monats: -14,14,22
      Woche des Monats: Last
      Verfall:
      Letzte Aktualisierung durch
      (Administrator): $$CONFIG_MANAGER$$
      Datum/Zeit der letzten Aktualisierung: 2004.06.04 17.18.30
      Verwaltendes Profil: EMPLOYEE
```



## Feldbeschreibungen: Ausführliche Clientzeitpläne

---

|   |   |
|---|---|
| Name der Maßnahmendomäne                    | Gibt den Namen der Maßnahmendomäne an.  |
| Zeitplanname                                | Gibt den Namen des Zeitplans an.  |
| Beschreibung                                | Beschreibung des Zeitplans.   |
| Aktion                                      | Gibt die Art der Aktion an, die bei der Verarbeitung dieses Zeitplans ausgeführt wird. Eine Liste der Aktionen befindet sich unter dem Befehl DEFINE SCHEDULE.  |
| Subaktion                                   | Gibt an, dass der Typ der Operation, der mit dem Parameter ACTION angegeben wird, geplant werden soll. Eine Liste der Subaktionen befindet sich unter dem Befehl DEFINE SCHEDULE.   |
| Optionen                                    | Gibt die Optionen an, die dem Befehl DSMC geliefert werden, wenn der Zeitplan ausgeführt wird.  |
| Objekte                                     | Gibt die Objekte an, für die die angegebene Aktion ausgeführt wird.   |
| Priorität                                   | Gibt den Prioritätswert für den Zeitplan an.  |
| Startdatum/-zeit                            | Gibt das/die anfängliche Startdatum/Uhrzeit für den Zeitplan an.  |
| Dauer                                       | Gibt die Länge des Startfensters für den Zeitplan an.   |
| Maximale Ausführungszeit (Minuten)          | Gibt die Anzahl Minuten an, in denen alle Clientsitzungen, die von der geplanten Operation gestartet werden, abgeschlossen werden sollten. Sind Sitzungen nach Ablauf der maximalen Ausführungszeit noch aktiv, gibt der Server eine Warnung aus, aber die Ausführung der Sitzungen wird fortgesetzt. |
| Zeitplandarstellung                         | Gibt an, ob klassische oder erweiterte Zeitplanregeln verwendet werden.   |
| Intervall                                   | Gibt die Zeit zwischen den Startfenstern an (bei DAYOFWEEK=ANY). Diese Angabe wird für Zeitpläne mit erweiterter Syntax nicht angezeigt.  |
| Wochentag                                   | Gibt den Wochentag an, an dem die Startfenster für den Zeitplan beginnen. Bei Verwendung eines Standardformats wird für erweiterte Zeitpläne im Feld 'Wochentag' ein Stern angezeigt.   |
| Monat                                       | Gibt die Monate an, in denen der Zeitplan ausgeführt wird. Diese Angabe wird für Zeitpläne mit klassischer Syntax nicht angezeigt.  |
| Tag des Monats                              | Gibt die Tage des Monats an, an denen der Zeitplan ausgeführt wird. Diese Angabe wird für Zeitpläne mit klassischer Syntax nicht angezeigt.   |
| Woche des Monats                            | Gibt die Wochen (erste, zweite, dritte, vierte oder letzte) des Monats an, in denen der Zeitplan ausgeführt wird. Diese Angabe wird für Zeitpläne mit klassischer Syntax nicht angezeigt.   |
| Verfall                                     | Gibt das Datum und die Uhrzeit an, an dem bzw. zu der dieser Zeitplan abläuft. Ist diese Spalte leer, läuft der Zeitplan nicht ab.  |
| Letzte Aktualisierung durch (Administrator) | Gibt den Namen des Administrators an, der den Zeitplan zuletzt aktualisiert hat. Enthält dieses Feld \$\$CONFIG_MANAGER\$\$, ist der Zeitplan einer Domäne zugeordnet, die von dem Konfigurationsmanager verwaltet wird.  |
| Datum/Zeit der letzten Aktualisierung       | Gibt das Datum und die Uhrzeit an, an dem bzw. zu der der Zeitplan zuletzt aktualisiert wurde.  |
| Verwaltendes Profil                         | Das Profil oder die Profile, für die der verwaltete Server subskribiert hat, um die Definition dieses Zeitplans zu erhalten.  |

## QUERY SCHEDULE (Verwaltungszeitplan abfragen)

---

Mit diesem Befehl können Informationen über einen oder mehrere Verwaltungszeitpläne angezeigt werden.

### Berechtigungsklasse

---

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

---

```

      .-*-----
>>-Query SCHEDULE-----+-----Type-----Administrative----->
      '-Zeitplanname-'

      .-Format-----Standard-----
>-----+-----Standard-----<
      '-Format-----+Standard-+-'
      '-Detailed-'

```

## Parameter

### Zeitplanname

Gibt den Namen des Zeitplans an, der abgefragt werden soll. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.

### Type=Administrative (Erforderlich)

Gibt an, daß die Abfrage Verwaltungszeitpläne anzeigt.

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

#### Standard

Gibt an, daß Teilinformationen für die Zeitpläne angezeigt werden.

#### Detailed

Gibt an, daß ausführliche Informationen für die Zeitpläne angezeigt werden.

Für erweiterte Zeitpläne zeigt das Standardformat ein Leerzeichen in der Spalte "Intervall" und einen Stern in der Spalte "Tag" an. Geben Sie FORMAT=DETAILED aus, um vollständige Informationen zu einem erweiterten Zeitplan anzuzeigen.

## Beispiel: Ausführliche Informationen zu Zeitplänen für Verwaltungsbefehle anzeigen

Von einem verwalteten Server ausführliche Informationen über Verwaltungszeitpläne anzeigen. Für Felddescriptions siehe Felddescriptions.

```

query schedule * type=administrative
format=detailed

```

```

          Zeitplanname: BACKUP_ARCHIVEPOOL
          Beschreibung:
            Befehl: backup db
            Priorität: 5
          Startdatum/-zeit: 2004.06.04 16.57.15
            Dauer: 1 Stunde
          Maximale Ausführungszeit (Minuten): 0
          Zeitplandarstellung: Klassisch
            Intervall: 1 Tag(e)
            Wochentag: Any
            Monat:
          Tag des Monats:
          Woche des Monats:
          Verfall:
            Aktiv: No
          Letzte Aktualisierung durch Administrator: $$CONFIG MANAGER$$
          Datum/Zeit der letzten Aktualisierung: 2004.06.04 17.51.49
          Verwaltendes Profil: ADMIN_INFO

          Zeitplanname: MONTHLY_BACKUP
          Beschreibung:
            Befehl: q status
            Priorität: 5
          Startdatum/-zeit: 2004.06.04 16.57.14
            Dauer: 1 Stunde
          Maximale Ausführungszeit (Minuten): 0
          Zeitplandarstellung: Erweitert
            Intervall:
            Wochentag: Die,Do,Fre
            Monat: Aug,Nov
          Tag des Monats:
          Woche des Monats: Second,Third
          Verfall:
            Aktiv: No
          Letzte Aktualisierung durch Administrator: $$CONFIG MANAGER$$
          Datum/Zeit der letzten Aktualisierung: 2004.06.04 17.51.49

```

## Feldbeschreibungen

---

|   |  |
|---|--|
| Zeitplanname                                | Gibt den Namen des Zeitplans an.   |
| Beschreibung                                | Beschreibung des Zeitplans.  |
| Befehl                                      | Gibt den geplanten Befehl an.  |
| Priorität                                   | Gibt den Prioritätswert für diesen Zeitplan an.  |
| Startdatum/-zeit                            | Gibt das/die anfängliche Startdatum/Uhrzeit für diesen Zeitplan an.  |
| Dauer                                       | Gibt die Länge des Startfensters an.   |
| Maximale Ausführungszeit (Minuten)          | Gibt die Anzahl Minuten an, in denen Serverprozesse, die von geplanten Befehlen gestartet werden, abgeschlossen werden müssen. Sind Prozesse nach Ablauf der maximalen Ausführungszeit noch aktiv, werden die Prozesse von der zentralen Zeitplanung abgebrochen.<br>Tipps: <ul style="list-style-type: none"> <li>Dieser Parameter gilt nicht für einige Prozesse, wie z. B. Prozesse zum Identifizieren doppelter Daten, deren Ausführung nach Ablauf der maximalen Ausführungszeit fortgesetzt werden kann.</li> <li>Einigen Befehlen kann eine andere Abbruchzeit zugeordnet werden. Beispielsweise kann der Befehl MIGRATE STGPOOL einen Parameter einschließen, der die Länge der Zeit angibt, die die Speicherpoolumlagerung ausgeführt wird, bevor die Umlagerung automatisch abgebrochen wird. Wenn Sie einen Befehl planen, für den eine Abbruchzeit definiert ist, und Sie außerdem eine maximale Ausführungszeit für den Zeitplan definieren, werden die Prozesse zu der Abbruchzeit abgebrochen, die zuerst erreicht wird.</li> </ul> |
| Zeitplandarstellung                         | Gibt an, ob klassische oder erweiterte Zeitplanregeln verwendet werden.  |
| Intervall                                   | Gibt die Zeit zwischen den Startfenstern an (bei DAYOFWEEK=ANY). Diese Angabe wird für Zeitpläne mit erweiterter Syntax nicht angezeigt.   |
| Wochentag                                   | Gibt den Wochentag an, an dem die Startfenster beginnen.   |
| Monat                                       | Gibt die Monate an, in denen der Zeitplan ausgeführt wird. Diese Angabe wird für Zeitpläne mit klassischer Syntax nicht angezeigt.   |
| Tag des Monats                              | Gibt die Tage des Monats an, an denen der Zeitplan ausgeführt wird. Diese Angabe wird für Zeitpläne mit klassischer Syntax nicht angezeigt.  |
| Woche des Monats                            | Gibt die Wochen (erste, zweite, dritte, vierte oder letzte) des Monats an, in denen der Zeitplan ausgeführt wird. Diese Angabe wird für Zeitpläne mit klassischer Syntax nicht angezeigt.  |
| Verfall                                     | Gibt das Datum an, nach dem dieser Zeitplan nicht mehr verwendet wird. Ist diese Spalte leer, läuft der Zeitplan nicht ab.   |
| Aktiv?                                      | Gibt an, ob der Zeitplan termingerecht ausgeführt wurde.   |
| Letzte Aktualisierung durch (Administrator) | Gibt den Namen des Administrators an, der den Zeitplan zuletzt aktualisiert hat. Enthält dieses Feld \$\$CONFIG_MANAGER\$\$, ist der Zeitplan einer Domäne zugeordnet, die von dem Konfigurationsmanager verwaltet wird.   |
| Datum/Zeit der letzten Aktualisierung       | Gibt an, wann der Zeitplan zuletzt geändert wurde (Datum und Uhrzeit).   |
| Verwaltendes Profil                         | Das Profil oder die Profile, für die der verwaltete Server subskribiert hat, um die Definition dieses Zeitplans zu erhalten.   |

## QUERY SCRATCHPADENTRY (Scratchpadeintrag abfragen)

---

Mit diesem Befehl können Sie Daten anzeigen, die im Scratchpad enthalten sind.

### Berechtigungsklasse

---

Jeder Administrator kann diesen Befehl ausgeben.



## Feldbeschreibungen

### Scratchpaddaten

Die Daten, die in dem Scratchpadeintrag gespeichert sind.

### Datum/Zeit der Erstellung

Das Datum und die Uhrzeit, an dem bzw. zu der der Scratchpadeintrag erstellt wurde.

### Datum/Zeit der letzten Aktualisierung

Das Datum und die Uhrzeit, an dem bzw. zu der der Scratchpadeintrag zuletzt aktualisiert wurde.

### Letzte Aktualisierung durch (Administrator)

Der Administrator, der den Scratchpadeintrag zuletzt aktualisiert hat.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SCRATCHPADENTRY

| Befehl                  | Beschreibung  |
|-------------------------|---|
| DEFINE SCRATCHPADENTRY  | Erstellt eine Zeile mit Daten im Scratchpad.                    |
| DELETE SCRATCHPADENTRY  | Löscht eine Zeile mit Daten aus dem Scratchpad.                 |
| SET SCRATCHPADRETENTION | Gibt den Zeitraum an, den Scratchpadeinträge aufbewahrt werden. |
| UPDATE SCRATCHPADENTRY  | Aktualisiert Daten in einer Zeile im Scratchpad.                |

## QUERY SCRIPT (IBM Spectrum Protect-Prozeduren abfragen)

Mit diesem Befehl können Informationen über Prozeduren angezeigt werden.

Dieser Befehl kann mit dem Befehl DEFINE SCRIPT verwendet werden, um eine neue Prozedur unter Verwendung des Inhalts aus einer anderen Prozedur zu erstellen.

## Berechtigungsklasse

Die für diesen Befehl erforderliche Berechtigungsklasse hängt davon ab, ob der Parameter Outputfile im Befehl angegeben ist.

- Ist der Parameter Outputfile nicht angegeben, kann jeder Administrator diesen Befehl ausgeben.
- Ist der Parameter Outputfile angegeben und ist die Serveroption REQSYSAUTHOUTFILE auf YES gesetzt, muss der Administrator die Systemberechtigung haben.
- Ist der Parameter Outputfile angegeben und ist die Serveroption REQSYSAUTHOUTFILE auf NO gesetzt, muss der Administrator die Bedienerberechtigung, die Maßnahmenberechtigung, die Speicherberechtigung oder die Systemberechtigung haben.

## Syntax

```
..*-----.  
>>-Query SCript----->  
    '-Prozedurname-'  
  
.-FORMAT----Standard-----.  
>----->  
    '-FORMAT----+Standard-----+'  
        +-Detailed-----+  
        +-Lines-----+  
    '-Raw-----+'  
        '-Outputfile----Dateiname-'
```

## Parameter

### Prozedurname

Gibt den Namen der Prozedur an, für die Informationen angezeigt werden sollen. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.

Wichtig: Wird keine Prozedur angegeben, zeigt die Abfrage Informationen über alle Prozeduren an. Die zur Verarbeitung dieses Befehls erforderliche Zeit und der Umfang der angezeigten Informationen kann sehr umfangreich sein.

## Format

Gibt das Ausgabeformat für die Anzeige der Prozedurinformationen an. Der Standardwert ist STANDARD. Gültige Werte:

### Standard

Gibt an, daß nur der Prozedurname und die Beschreibung in einer Prozedur angezeigt werden.

### Detailed

Gibt an, daß ausführliche Informationen über die Prozedur angezeigt werden. Diese Informationen enthalten die Befehle in der Prozedur und ihre Zeilennummern, das Datum der letzten Aktualisierung und den Administrator, der die Aktualisierungen ausgeführt hat.

### Lines

Gibt an, daß der Prozedurname, die Zeilennummer der Befehle, die Kommentarzeilen und die Befehle in der Prozedur angezeigt werden.

### Raw

Gibt an, dass die in der Prozedur enthaltenen Befehle in eine Datei geschrieben werden, die mit dem Parameter Outputfile angegeben wird. Dieses Format bietet die Möglichkeit, die Ausgabe aus einer Prozedur in eine Datei umzuleiten, die dann mithilfe des Befehls DEFINE SCRIPT in eine andere Prozedur kopiert werden kann.

Wird keine Ausgabedatei angegeben, gibt der IBM Spectrum Protect-Server "query script" mit "format=raw" an der Konsole aus.

## Outputfile

Gibt den Namen der Datei an, in die die Ausgabe umgeleitet wird, wenn FORMAT=Raw angegeben wird. Die angegebene Datei muss sich auf dem Server befinden, der diesen Befehl ausführt. Ist die Datei vorhanden, wird die Abfrageausgabe an das Ende der Datei angehängt.

## Beispiel: Die Prozedurbeschreibungen auflisten

Die Standardinformationen über Prozeduren anzeigen.

```
query script *
```

| Name    | Beschreibung  |
|---------|---|
| QCOLS   | Spalten für angegebene SQL-Tabelle anzeigen               |
| QSAMPLE | Beispiel-SQL-Abfrage                                      |
| EXAMPLE | Speicherpools und Datenbank sichern, wenn keine Sitzungen |

## Beispiel: Den Inhalt einer Prozedur mit Zeilennummern anzeigen

Die Zeilen mit Informationen für die Prozedur Q\_AUTHORITY anzeigen.

```
query script q_authority format=lines
```

| Name        | Zeilen-<br>Anzahl | Befehl  |
|-------------|-------------------|---|
| Q_AUTHORITY | 1                 | /* -----*/                                      |
|             | 5                 | /* Prozedurname: Q_AUTHORITY */                 |
|             | 10                | /* Beschreibung: Administratoren mit der */     |
|             | 15                | /* Berechtigung für Befehle, */                 |
|             | 20                | /* die eine bestimmte Berech- */                |
|             | 25                | /* tigung erfordern, anzeigen. */               |
|             | 30                | /* Parameter 1: Berechtigungsname in der Form*/ |
|             | 35                | /* x_priv - EX. policy_priv */                  |
|             | 40                | /* Beispiel: run q_authority storage_priv */    |
|             | 45                | /* -----*/                                      |
|             | 50                | select admin_name from admins where -           |
|             | 55                | upper(system_priv) <> 'NO' or -                 |
|             | 60                | upper(\$1) <> 'NO'                              |

## Beispiel: Eine Prozedur aus einer vorhandenen Prozedur erstellen

Die Prozedur ENGDEV abfragen und die Ausgabe in die Datei MY.SCRIPT umleiten.

```
query script engdev format=raw outputfile=my.script
```

## Beispiel: Ausführliche Informationen zur Prozedur anzeigen

Ausführliche Informationen zu Prozeduren anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query script * format=detailed
```

Name: QCOLS  
 Zeilennummer: DESCRIPTION  
 Befehl: Spalten für eine angegebene  
 SQL-Tabelle anzeigen  
 Letzte Aktualisierung durch (Administrator): SERVER\_CONSOLE  
 Datum/Zeit der letzten Aktualisierung: 12/02/1997 16:05:29

Name: QCOLS  
 Zeilennummer: 1  
 Befehl: Spaltenname aus Spalten auswählen;  
 dabei ist tabname='\$1'  
 Letzte Aktualisierung durch (Administrator): SERVER\_CONSOLE  
 Datum/Zeit der letzten Aktualisierung: 12/02/1997 16:05:29

## Feldbeschreibungen

**Name**  
 Der Name der Prozedur.

**Zeilennummer**  
 Die Zeilennummer der Prozedur oder die Zeichenfolge DESCRIPTION.

**Befehl**  
 Der Befehl in der Zeile, die im vorherigen Feld angezeigt wurde.

**Letzte Aktualisierung durch (Administrator)**  
 Der Name des Administrators, der die Prozedur definiert oder zuletzt aktualisiert hat.

**Datum/Zeit der letzten Aktualisierung**  
 Das Datum und die Uhrzeit, an dem bzw. zu der der Administrator die Prozedur definiert oder aktualisiert hat.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SCRIPT

| Befehl        | Beschreibung  |
|---------------|---|
| COPY SCRIPT   | Erstellt eine Kopie einer Prozedur.                           |
| DEFINE SCRIPT | Definiert eine Prozedur für den IBM Spectrum Protect-Server.  |
| DELETE SCRIPT | Löscht eine Prozedur oder einzelne Zeilen aus einer Prozedur. |
| RENAME SCRIPT | Vergibt einen neuen Namen für eine Prozedur.                  |
| RUN           | Führt ein Script aus.   |
| UPDATE SCRIPT | Ändert Zeilen oder fügt Zeilen in einer Prozedur hinzu.       |

**Zugehörige Konzepte:**  
 Server-Scripts

## QUERY SERVER (Server abfragen)

Mit diesem Befehl können Informationen über eine Server-Definition angezeigt werden.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```

.*----- .-Format----Standard----.
>>-Query SERver---+-----+-----+-----<
                '-Servername-' '-Format----+Standard+'
                                '-Detailed-'
  
```

## Parameter

**Servername**  
 Gibt den Namen des Servers an, der abgefragt werden soll. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Server-Namen.

**Format**

Gibt an, wie die Informationen angezeigt werden. Der Parameter ist wahlfrei. Der Standardwert ist STANDARD.

Standard

Gibt an, dass Teilinformationen angezeigt werden.

Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

## Beispiel: Alle Server auflisten

---

Informationen im Standardformat über alle Server anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query server *
```

| Server-<br>Name | Übertr.<br>Methode | Adresse d.<br>höheren Ebene | Adresse d.<br>unteren Ebene | Tage<br>seit<br>ltzt.<br>Zugr. | Server-<br>kenn-<br>wort-<br>vergabe | Kennwort-<br>vergabe<br>virtueller<br>Bereich | Ersetzen<br>möglich |
|-----------------|--------------------|-----------------------------|-----------------------------|--------------------------------|--------------------------------------|---|---------------------|
| SERVER_A        | TCPIP              | 9.115.35.6                  | 1501                        | 11                             | Yes                                  | No  | No                  |
| SERVER_B        | TCPIP              | 9.115.45.24                 | 1500                        | <1                             | Yes                                  | No  | No                  |
| ASTRO           | TCPIP              | 9.115.32.21                 | 1500                        | 24                             | Yes                                  | No  | No                  |

## Beispiel: Ausführliche Informationen zu einem bestimmten Server anzeigen

---

Von einem verwalteten Server ausführliche Informationen zu SERVER\_A anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query server server_a format=detailed
```

```
Servername: SERVER_A
```

```
Übertragungsmethode: TCPIP
Übertragungsmethode: TCPIP
Adresse der höheren Ebene: 9.115.4.15
Adresse der unteren Ebene: 1500
Beschreibung:
Ersetzen möglich: No
Knotenname:
Datum/Zeit des letzten Zugriffs: 07/09/2013 09:00:00
Tage seit letztem Zugriff: <1
Komprimierung: Vom Client definiert
Archivierung löschen?: No
URL:
Registrierung (Datum/Uhrzeit): 07/08/2013 09:15:09
Registriert durch: $$CONFIG_MANAGER$$
Byte empfangen (letzte Sitzung): 362
Byte gesendet (letzte Sitzung): 507
Dauer der letzten Sitzung: 0,00
Inaktiver Wartestatus in % (letzte Sitzung): 0,00
Auf Übertragung warten in % (letzte Sitzung): 0,00
Auf Datenträger warten in % (letzte Sitzung): 0,00
Verweildauer vor Löschen: 5
Verwaltendes Profil:
Serverkennwort definiert: Yes
Serverkennwort definiert (Datum/Uhrzeit): 07/08/2013 09:15:09
Tage seit Kennwortvergabe: 1
Ungültige Anmeldeversuche für Server: 0
Kennwortvergabe für virtuellen Bereich: No
Datum/Zeit der Kennwortvergabe für virtuellen Bereich:(?)
Tage seit Kennwortvergabe für virtuellen Bereich:(?)
Ungültige Anmeldeversuche für virtuellen Bereichsknoten: 0
Protokoll auswerten: No
Version: 7
Release: 1
Stufe: 0.0
Rolle(n): Replikation
SSL: No

Sitzungssicherheit: Strict

Transportmethode: TLS 1.2
```

## Feldbeschreibungen

---

Servername

Der Name des Servers.



Übertragungsmethode  
Die Übertragungsmethode, mit der die Verbindung zum Server hergestellt wird.

Übertragungsmethode  
Die Methode, die für die Datenübertragung zwischen Servern verwendet wird.

Adresse der höheren Ebene  
Die IP-Adresse des Servers (in Schreibweise mit Trennzeichen).

Adresse der unteren Ebene  
Die Anschlußnummer des Servers.

Beschreibung  
Die Server-Beschreibung.

Ersetzen möglich  
Gibt an, ob eine Serverdefinition auf einem verwalteten Server durch eine Definition von einem Konfigurationsmanager ersetzt werden kann.

Knotenname  
Der Name des Clientknotens.

Datum/Zeit des letzten Zugriffs  
Das Datum und die Uhrzeit, an dem bzw. zu der der Clientknoten zuletzt auf den Server zugegriffen hat.

Tage seit letztem Zugriff  
Die Anzahl der Tage seit dem Zugriff des Client-Knotens auf den Server.

Komprimierung  
Die Art der Komprimierung, die von IBM Spectrum Protect für Clientdateien ausgeführt wird.

Archivierung löschen?  
Gibt an, ob der Clientknoten seine eigenen Archivierungsdateien löschen kann. Der Wert (?) gibt an, dass dieses Feld nicht definiert ist und für diese Definition nicht gilt.

URL  
Der URL für den Zugriff auf diesen Server von einer browserbasierten Schnittstelle aus.

Registrierung (Datum/Uhrzeit)  
Das Datum und die Uhrzeit, an dem bzw. zu der der Clientknoten registriert wurde.

Registriert durch  
Der Name des Administrators, der den Clientknoten registriert hat.

Byte empfangen (letzte Sitzung)  
Die Anzahl der Byte, die während der letzten Sitzung des Clientknotens vom Server empfangen wurden.

Byte gesendet (letzte Sitzung)  
Die Anzahl Byte, die an den Clientknoten gesendet wurden.

Dauer der letzten Sitzung  
Die Dauer der letzten Sitzung des Client-Knotens in Sekunden.

Inaktiver Wartestatus in % (letzte Sitzung)  
Der Prozentsatz der gesamten Sitzungszeit, zu dem der Client keine Funktionen ausgeführt hat.

Auf Übertragung warten in % (letzte Sitzung)  
Der Prozentsatz der gesamten Sitzungszeit, zu dem der Client auf eine Antwort von dem Server gewartet hat.

Auf Datenträger warten in % (letzte Sitzung)  
Der Prozentsatz der gesamten Sitzungszeit, zu dem der Client auf das Laden eines austauschbaren Datenträgers gewartet hat.

Verweildauer vor Löschen  
Die Anzahl der Tage, die ein Objekt auf dem Zielsever verbleibt, nachdem es zum Löschen markiert wurde.

Verwaltendes Profil  
Das Profil, aus dem der verwaltete Server die Definition dieses Servers erhalten hat.

Serverkennwort definiert  
Gibt an, ob das Kennwort für den Server definiert wird.

Serverkennwort definiert (Datum/Uhrzeit)  
Gibt an, wann das Kennwort für den Server definiert wurde.

Tage seit Kennwortvergabe  
Die Anzahl der Tage seit der Definition des Server-Kennworts.

Ungültige Anmeldeversuche für Server  
Die maximale Anzahl ungültiger Anmeldeversuche, die der Server akzeptieren kann.

Kennwortvergabe für virtuellen Bereich  
Gibt an, ob das Kennwort für die Anmeldung beim Zielsever definiert wird.

Datum/Zeit der Kennwortvergabe für virtuellen Bereich  
Gibt an, wann das Kennwort für die Unterstützung virtueller Bereiche definiert wurde.

Tage seit Kennwortvergabe für virtuellen Bereich  
Die Anzahl der Tage seit der Definition des Kennworts für die Unterstützung virtueller Bereiche.

Ungültige Anmeldeversuche für virtuellen Bereichsknoten  
Die maximale Anzahl ungültiger Anmeldeversuche, die auf dem Ziel-Server akzeptiert werden.

Protokoll auswerten (veraltet)  
Gibt an, ob für den Speicheragenten die Funktion für die Datenprüfung aktiviert ist. Dieses Feld wird nicht mehr verwendet.

**Version**

Die Softwareversion des IBM Spectrum Protect-Servers.

**Release**

Das Software-Release des IBM Spectrum Protect-Servers.

**Stufe**

Die Softwarestufe des IBM Spectrum Protect-Servers.

**Rolle(n)**

Die Rolle des Servers. Eine der Rollen, für die der Server verwendet wird, ist z. B. die Replikation.

**SSL**

Gibt an, ob die SSL-Kommunikation (SSL = Secure Sockets Layer) verwendet wird.

**Sitzungssicherheit**

Gibt die Stufe der Sitzungssicherheit an, die für den Server durchgesetzt wird. Die gültigen Werte sind STRICT und TRANSITIONAL.




**Transportmethode**

Gibt die Transportmethode an, die zuletzt für den angegebenen Server verwendet wurde. Die gültigen Werte sind TLS 1.2, TLS 1.1 und NONE. Ein Fragezeichen (?) wird angezeigt, bis eine erfolgreiche Authentifizierung ausgeführt wird.

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für QUERY SERVER

| Befehl   | Beschreibung   |
|--|--|
| DEFINE DEVCLASS  | Definiert eine Einheitenklasse.  |
| DEFINE SERVER  | Definiert einen Server für die Übertragung zwischen Servern.   |
| DELETE DEVCLASS  | Löscht eine Einheitenklasse.   |
| DELETE FILESPACE   | Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.   |
| DELETE SERVER  | Löscht die Definition eines Servers.   |
|  <br> PROTECT STGPOOL |  <br> Schützt einen Verzeichniscontainerspeicherpool. |
| QUERY NODE   | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.  |
| RECONCILE VOLUMES  | Stimmt Definitionen von virtuellen Datenträgern auf dem Quellenserver mit Archivierungsobjekten des Zielservers ab.  |
| REGISTER NODE  | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.  |
| REMOVE NODE  | Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.   |
| REPLICATE NODE   | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |
| SET REPLSERVER   | Gibt einen Zielreplikationsserver an.  |
| UPDATE DEVCLASS  | Ändert die Attribute einer Einheitenklasse.  |
| UPDATE NODE  | Ändert die Attribute, die einem Clientknoten zugeordnet sind.  |
| UPDATE SERVER  | Aktualisiert Informationen über einen Server.  |

## QUERY SERVERGROUP (Servergruppe abfragen)

---

Mit diesem Befehl können Informationen über Server-Gruppen und Gruppenteile angezeigt werden.

### Berechtigungsklasse

---

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

---

```
>>-QUERY SERVERGroup--*-----+-----><
                        '-Gruppenname-'
```

## Parameter

---

### Gruppenname

Gibt die Server-Gruppe an, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden.

## Beispiel: Servergruppen auflisten

---

Von einem verwalteten Server alle Servergruppen abfragen. Für Felddesreibungen siehe Felddesreibungen.

```
query servergroup *
```

| Servergruppe | Mitglieder | Beschreibung                                     | Verwaltendes Profil |
|--------------|------------|--|---------------------|
| ADMIN_GROUP  | SERVER_A   | Headquarters<br>SERVER_B<br>SERVER_C<br>SERVER_D | ADMIN_INFO          |

## Felddesreibungen

---

### Servergruppe

Der Name der Server-Gruppe.

### Mitglieder

Die Gruppenteile.

### Beschreibung

Die Beschreibung der Server-Gruppe.

### Verwaltendes Profil

Das Profil oder die Profile, für die der verwaltete Server subskribiert hat, um die Definition der Servergruppen zu erhalten.

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für QUERY SERVERGROUP

| Befehl             | Beschreibung                            |
|--------------------|---|
| COPY SERVERGROUP   | Erstellt eine Kopie einer Servergruppe. |
| DEFINE SERVERGROUP | Definiert eine neue Servergruppe.       |
| DELETE SERVERGROUP | Löscht eine Servergruppe.               |
| QUERY SERVER       | Zeigt Informationen über Server an.     |
| RENAME SERVERGROUP | Benennt eine Servergruppe um.           |
| UPDATE SERVERGROUP | Aktualisiert eine Servergruppe.         |

## QUERY SESSION (Clientsitzungen abfragen)

---

Mit diesem Befehl können Informationen zu Verwaltungs-, Knoten- und Serversitzungen angezeigt werden.

## Berechtigungsklasse

---

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

---

```
>>-Query SEssion--*-----+----->
                        '-Sitzungsnummer-'
```

```

>----->
'-MINTIMethreshold----Minuten-'

>----->
'-MAXTHRoughput----Kilobyte_pro_Sekunde-'

.-Format----Standard----.  .-Type----*-----
>----->
'-Format----+Standard+-'  '-Type----+Admin--+'
          '-Detailed-'          +-Node---+
                                '-Server-'

.-CLIENTName----*-----
>-----<
'-CLIENTName-----Clientname--'

```

## Parameter

### Sitzungsnummer

Gibt die Nummer der Verwaltungssitzung oder Client-Knotensitzung an, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Wird kein Wert für diesen Parameter angegeben, werden alle Sitzungen angezeigt.

### MINTIMethreshold

Gibt an, dass Sitzungen angezeigt werden sollen, für die mindestens diese Anzahl Minuten ab dem Zeitpunkt verstrichen sind, zu dem der Client Daten zum Speichern an den Server gesendet hat. Dieser Parameter ist wahlfrei. Die Mindestanzahl Minuten ist 1. Die maximale Anzahl Minuten beträgt 99999999.

### MAXTHRoughput

Gibt an, daß Sitzungen angezeigt werden sollen, in denen Daten mit einer geringeren Übertragungsgeschwindigkeit als dieser Anzahl Kilobyte pro Sekunde übertragen werden. Dieser Parameter ist wahlfrei. Die Mindestanzahl Kilobyte pro Sekunde beträgt 0. Die maximale Anzahl Kilobyte pro Sekunde beträgt 99999999.

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Die folgenden Werte sind gültig:

#### Standard

Gibt an, daß Teilinformationen für die Sitzung angezeigt werden.

#### Detailed

Gibt an, daß die gesamten Informationen für die Sitzung angezeigt werden.

### Type

Gibt den Typ der Sitzungen an, der in den Abfrageergebnissen berücksichtigt werden soll. Wird kein Wert für diesen Parameter angegeben, werden alle Typen von Sitzungen abgefragt. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

#### Admin

Gibt an, dass Verwaltungssitzungen angezeigt werden.

#### Node

Gibt an, dass Knotensitzungen angezeigt werden.

#### Server

Gibt an, dass Serversitzungen angezeigt werden.

### CLIENTName

Gibt den Namen eines Administrators, Clientknotens oder Servers an, der abgefragt werden soll. Sie können einen oder mehrere Namen angeben. Sie können auch Knotengruppen und Proxy-Knoten angeben. Werden mehrere Namen angegeben, sind die Namen durch Kommas voneinander zu trennen; verwenden Sie zwischen den Namen keine Leerzeichen. Sie können Platzhalterzeichen für Knotennamen, aber nicht für Knotengruppenamen verwenden. Der Parameter ist wahlfrei.

Während der Knotenreplikation wird der Clientname auf dem Zielservers als *Knotenname (Servername)* angezeigt. Dabei ist *Knotenname* der Knoten, dessen Daten repliziert werden, und *Servername* der Name des Quellenservers. Sie können entweder den Knotennamen oder den Servernamen im Parameter CLIENTName angeben, um die Replikationssitzungen anzuzeigen.

## Beispiel: Aktive Clientknotensitzungen auflisten

Informationen zu allen Verwaltungs- und Clientknotensitzungen, die mit dem Server kommunizieren, anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query session
```

| Sitz.<br>nummer | Über.<br>meth. | Sitz.<br>status | Warte-<br>zeit | Byte<br>gesend. | Byte<br>empf. | Sitz.<br>typ | Platt-<br>form | Client-<br>Name |
|-----------------|----------------|-----------------|----------------|-----------------|---------------|--------------|----------------|-----------------|
| 4               | TCP/IP         | Run             | 0 S            | 1.4 K           | 162           | Admin        | WinNT          | ADMIN           |

## Beispiel: Ausführliche Informationen zu aktiven Clientknotensitzungen anzeigen

Ausführliche Informationen zu allen Verwaltungs- und Clientknotensitzungen, die mit dem Server kommunizieren, anzeigen. Für Felddesreibungen siehe Felddesreibungen.

```
query session format=detailed
```

```

Sitzungsnummer: 4
Übertragungsmethode: Tcp/Ip
Sitzungsstatus: Run
Wartezeit: 0 S
Byte gesendet: 1,4 K
Byte empfangen: 162
Sitzungstyp: Admin
Plattform: WinNT
Clientname: ADMIN
Datenträgerzugriffstatus:
Benutzername:
Ersten Daten gesendet am/um:
Proxy durch Speicheragent:
Aktionen:
Übernahmemodus: No

```

## Felddesreibungen

### Sitzungsnummer

Gibt eine eindeutige Sitzungsidentifikationsnummer an, die vom Server zugeordnet wird.

### Übertragungsmethode

Gibt die Methode an, die vom Client für die Kommunikation mit dem Server verwendet wird.

### Sitzungsstatus

Gibt den aktuellen Übertragungsstatus des Servers an. Die folgenden Status sind gültig:

#### End

Die Sitzung wird beendet (Sitzungsressourcen werden freigegeben).

#### IdleW

Es wird auf die nächste Anforderung des Clients gewartet (Sitzung ist inaktiv).

#### MediaW

Die Sitzung wartet darauf, auf einen Datenträger mit sequenziellem Zugriff zugreifen zu können.

#### RecvW

Der Server wartet darauf, eine unerwartete Nachricht vom Client zu empfangen.

#### Run

Der Server führt gerade eine Clientanforderung aus (und wartet nicht auf das Senden von Daten).

#### SendW

Der Server wartet darauf, Daten an den Client zu senden (wartet auf bereits gesendete Daten, die an den Clientknoten weitergegeben werden sollen).

#### SSLiW

Die Sitzung wartet auf die Beendigung der SSL-Initialisierung (SSL = Secure Sockets Layer).

#### Start

Die Sitzung wird gestartet (Identifikationsüberprüfung läuft).

### Wartezeit

Gibt die Zeit an (Sekunden, Minuten oder Stunden), die sich der Server im angezeigten aktuellen Status befindet.

### Byte gesendet

Gibt die Anzahl der Datenbyte an, die an den Clientknoten gesendet wurden, seit die Sitzung eingeleitet wurde.

### Byte empfangen

Gibt die Anzahl der Datenbyte an, die vom Clientknoten empfangen wurden, seit die Sitzung eingeleitet wurde.

### Sitzungstyp

Gibt die Art der Sitzung an, die gerade läuft: ADMIN bei einer Verwaltungssitzung, NODE bei einer Clientknotensitzung oder SERVER. SERVER gibt an, dass der Server eine Sitzung startet und serverübergreifende Operationen einleitet, wie beispielsweise Sitzungen für zentrale Konfiguration, gemeinsame Nutzung von Speicherarchiven und Speicheragenten.

### Plattform

Gibt den Typ des Betriebssystems an, das dem Client zugeordnet ist.

### Clientname

Gibt den Namen des Client-Knoten bzw. Administrators an.

Für Knotenreplikationssitzungen wird der Clientname nach dem Start der Datenübertragung auf dem Zielsystem in *Knotenname* (*Servername*) aktualisiert.

#### Datenträgerzugriffsstatus

Gibt den Statustyp "Auf Datenträger warten" an. Befindet sich eine Sitzung in einem Datenträgerwartestatus, zeigt dieses Feld eine Liste aller Mountpunkte und aller sequenziellen Datenträger für die Sitzung an. Die Liste der Mountpunkte gibt die Einheitensklasse und den zugeordneten Speicherpool an. Die Liste der Datenträger gibt die Datenträger des primären Speicherpools sowie die Datenträger aller Kopierspeicherpools und Pools für aktive Daten zusammen mit den zugeordneten Speicherpools an.

Der Server erlaubt es mehreren Sitzungen, einen Datenträger in einem Speicherpool, dem der Einheitentyp FILE oder CENTERA zugeordnet ist, gleichzeitig zu lesen, und einer Sitzung, auf den Datenträger zu schreiben. Daher kann ein Datenträger in einem Speicherpool mit einem Einheitentyp FILE oder CENTERA für mehrere Sitzungen als aktueller Datenträger erscheinen.

#### Proxy durch Speicheragent

Gibt den Speicheragenten an, der der Proxy für die LAN-unabhängige Datenversetzung für den Knoten ist.

#### Benutzername

Gibt die Benutzer-ID des Knotens auf einem Mehrbenutzersystem an, mit der die Verbindung zum Server hergestellt wird, wenn es sich nicht um denselben Systembenutzer handelt, der ursprünglich mit dem Server verbunden war.

#### Ersten Daten gesendet am/um

Gibt das Datum und die Uhrzeit an, an dem bzw. zu der der Client zum ersten Mal Daten zum Speichern an den Server gesendet hat.

#### Aktionen

Zeigt eine Liste der Aktionen an, die während der Sitzung ausgeführt wurden. Eine Aktion wird nur ein Mal aufgelistet, auch wenn die Aktion während einer Sitzung mehrmals ausgeführt wurde. Die folgenden Aktionen sind gültig:

#### BkIns

Ein oder mehrere Sicherungsobjekte wurden auf dem Server gespeichert. Die Operation kann eine Teilsicherung oder eine selektive Sicherung gewesen sein.

#### BkUpd

Ein oder mehrere Attribute wurden für ein Sicherungsobjekt aktualisiert, das auf dem Server gespeichert ist.

#### BkDel

Ein oder mehrere Sicherungsobjekte, die auf dem Server gespeichert waren, wurden gelöscht.

#### BkRebind

Ein oder mehrere Sicherungsobjekte, die auf dem Server gespeichert sind, wurden an eine andere Verwaltungsklasse gebunden.

#### NoQueryRestore

Eine Zurückschreibungsoperation ohne Abfrage wurde von dem Client eingeleitet, um gesicherte Dateien vom Server in das Clientsystem zurückzuschreiben.

#### ArIns

Ein oder mehrere Archivierungsobjekte wurden auf dem Server gespeichert.

#### ObjRtrv

Ein oder mehrere Dateien wurden von dem Server abgerufen. Möglicherweise sollten Archivierungsdateien abgerufen oder Sicherungsdaten (außer Sicherungsdaten aus einer Zurückschreibungsoperation ohne Abfrage) zurückgeschrieben werden.

#### MigIns

Ein oder mehrere Dateien wurden von IBM Spectrum Protect for Space Management (HSM-Client) umgelagert und auf dem Server gespeichert.

#### MigDel

Ein oder mehrere speicher verwaltete Dateien, die auf dem Server gespeichert waren, wurden gelöscht.

#### MigRebind

Ein oder mehrere speicher verwaltete Dateien, die auf dem Server gespeichert sind, wurden an eine andere Verwaltungsklasse gebunden.

#### MigRecall

Ein oder mehrere speicher verwaltete Dateien, die auf dem Server gespeichert sind, wurden zurückgerufen.

#### MigUpd

Die Attribute für eine oder mehrere speicher verwaltete Dateien, die auf dem Server gespeichert sind, wurden aktualisiert.

#### FSAdd

Der Clientknoten hat einen oder mehrere neue Dateibereiche zum Serverspeicher hinzugefügt.

#### FSUpd

Der Clientknoten hat Attribute für einen oder mehrere Dateibereiche aktualisiert, die für den Server definiert sind.

#### DefAuth

Ein Befehl SET ACCESS wurde von dem Clientknoten verarbeitet, der zur Folge hatte, dass eine Berechtigungsregel für den Zugriff auf die Daten des Clientknotens hinzugefügt wurde.

## Übernahmemodus

Gibt an, ob die Clientsitzung im Übernahmemodus gestartet wurde. Die folgenden Werte sind gültig:

### Force

Das Flag FORCEFAILOVER ist auf dem Client angegeben und der Übernahmemodus wird für die Sitzung erzwungen.

### Yes

Die Clientsitzung wurde im Übernahmemodus gestartet.

### No

Die Clientsitzung wurde nicht im Übernahmemodus gestartet.

## Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für QUERY SESSION

| Befehl         | Beschreibung                               |
|----------------|--|
| CANCEL SESSION | Bricht aktive Sitzungen mit dem Server ab. |

## QUERY SHREDSTATUS (Status für Schreddern abfragen)

Verwenden Sie diesen Befehl, um Informationen zu Daten anzuzeigen, die geschreddert werden sollen.

## Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie über die Administratorberechtigung verfügen.

## Syntax

```
>>-QUERY SHREDstatus-+-Format-----Standard-----><
                        '-Format-----+Standard-+-'
                        '-Detailed-'
```

## Parameter

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

#### Standard

Gibt an, dass Teilinformationen angezeigt werden. Dies ist der Standardwert.

#### Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

## Beispiel: Übersichtsdaten zum Schreddern anzeigen

Teilinformationen zum Schreddern von Daten auf dem Server anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query shredstatus
```

```
Schreddern  Objekte, die auf
aktiv      Schreddern
           warten
-----
NO         4
```

## Beispiel: Ausführliche Informationen zum Schreddern anzeigen

Ausführliche Informationen zum Schreddern von Daten auf dem Server anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query shredstatus format=detailed
```

```
Schreddern Objekte, die   Belegter   Noch zu
aktiv      auf Schreddern Speicherber. schreddernde
           warten         (MB)         Daten (MB)
-----
NO         4             182           364
```

## Feldbeschreibungen

### Schreddern aktiv

Gibt an, ob der Server zu diesem Zeitpunkt aktiv Daten schreddert.

### Objekte, die auf Schreddern warten

Die Anzahl der Objekte, die gegenwärtig auf das Schreddern warten.

### Belegter Speicherbereich (MB)

Der Serverspeicherbereich (in MB), der durch die Objekte belegt ist, die gegenwärtig auf das Schreddern warten. Dies ist der Speicherbereich, der verfügbar wird, wenn die Objekte geschreddert wurden.

### Noch zu schreddernde Daten (MB)

Das Datenvolumen, das noch geschreddert werden muss.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SHREDSTATUS

| Befehl                | Beschreibung   |
|-----------------------|--|
| BACKUP STGPOOL        | Sichert einen primären Speicherpool in einem Kopierspeicherpool.                                       |
| DEFINE STGPOOL        | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.                     |
| EXPORT NODE           | Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.        |
| GENERATE BACKUPSET    | Generiert eine Sicherungsgruppe mit den Daten eines Clients.   |
| GENERATE BACKUPSETTOC | Generiert ein Inhaltsverzeichnis für eine Sicherungsgruppe.  |
| MOVE DATA             | Versetzt Daten aus einem angegebenen Speicherpooldatenträger in einen anderen Speicherpooldatenträger. |
| QUERY STGPOOL         | Zeigt Informationen zu Speicherpools an.   |
| SETOPT                | Aktualisiert eine Serveroption, ohne den Server zu stoppen und erneut zu starten.                      |
| SHRED DATA            | Startet manuell den Prozess zum Schreddern gelöschter Daten.   |
| UPDATE STGPOOL        | Ändert die Attribute eines Speicherpools.  |

## QUERY SPACETRIGGER (Speicherbereichsauslöser abfragen)

Verwenden Sie diesen Befehl, um die Einstellungen der Speicherbereichsauslöser für den Speicherpool anzuzeigen.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query SPACETrigger--STG--+-----+----->
                                     '-STGPOOL---Speicherpool-'
.-Format----Standard----.
>+-----+-----<
  '-Format---+Standard+-'
                                     '-Detailed-'
```

### Parameter

#### STG

Gibt einen Speicherbereichsauslöser für den Speicherpool an.

#### STGPOOL

Gibt einen oder mehrere Speicherpools an (unter Verwendung eines Platzhalterzeichens), für die Informationen zum Speicherpoolauslöser angezeigt werden. Wird STG angegeben, aber STGPOOL nicht angegeben, wird der standardmäßige



Speicherbereichsauslöser für den Speicherpool (sofern vorhanden) angezeigt.

**Format**

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

**Standard**

Gibt an, dass Teilinformationen angezeigt werden.

**Detailed**

Gibt an, dass die gesamten Informationen angezeigt werden.

## Beispiel: Die ausführlichen Einstellungen des Speicherbereichsauslöser für einen Speicherpool anzeigen

Diesen Befehl ausgeben:

```
query spacetrigger stg stgpool=archivepool format=detailed
```

 **AIX-Betriebssysteme**

```
Speicherpool Prozent belegt: 50
Prozentsatz für Speicherpoolerweiterung: 20
  Präfix für Speicherpoolerweiterung: /usr/tivoli/tsm/server/filevol/
  SPEICHERPOOL: ARCHIVEPOOL
Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
Datum/Zeit der letzten Aktualisierung: 05/10/2004 11:59:59
```

 **Linux-Betriebssysteme**

```
Speicherpool Prozent belegt: 50
Prozentsatz für Speicherpoolerweiterung: 20
  Präfix für Speicherpoolerweiterung: /opt/tivoli/tsm/server/filevol/
  SPEICHERPOOL: ARCHIVEPOOL
Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
Datum/Zeit der letzten Aktualisierung: 05/10/2004 11:59:59
```

 **Windows-Betriebssysteme**

```
Speicherpool Prozent belegt: 50
Prozentsatz für Speicherpoolerweiterung: 20
  Präfix für Speicherpoolerweiterung: c:\Programdateien\tivoli\filevol\
  SPEICHERPOOL: ARCHIVEPOOL
Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
Datum/Zeit der letzten Aktualisierung: 05/10/2004 11:59:59
```

## Feldbeschreibungen

**Speicherpool Prozent belegt**

Der Auslöserauslastungsprozentsatz, bei dem IBM Spectrum Protect mehr Speicherbereich für den Speicherpool zuordnet.

**Prozentsatz für Speicherpoolerweiterung**

Der Prozentsatz des Speicherbereichs, um den der Speicherpool erweitert werden soll.

**Präfix für Speicherpoolerweiterung**

Das Präfix, das dem Speicherbereichsauslöser zugeordnet ist.

**STGPOOL**

Der in der Abfrage verwendete Speicherpoolname.

**Letzte Aktualisierung durch (Administrator)**

Der Administrator, der den Speicherbereichsauslöser für den Speicherpool zuletzt aktualisiert hat.

**Datum/Zeit der letzten Aktualisierung**

Das Datum und die Uhrzeit, an dem bzw. zu der der Administrator den Speicherbereichsauslöser für den Speicherpool zuletzt aktualisiert hat.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SPACETRIGGER

| Befehl              | Beschreibung  |
|---------------------|---|
| DEFINE SPACETRIGGER | Definiert einen Speicherbereichsauslöser zum Erweitern des Speicherbereichs für einen Speicherpool. |
| DELETE SPACETRIGGER | Löscht den Speicherbereichsauslöser für den Speicherpool.   |

| Befehl              | Beschreibung   |
|---------------------|--|
| UPDATE SPACETRIGGER | Ändert Attribute des Speicherbereichsauslösers für den Speicherpool. |

## QUERY STATUS (Systemparameter abfragen)

Mit dem Befehl QUERY STATUS können Informationen zu Systemparametern angezeigt werden.

Diesen Befehl verwenden, um

- die Servicestufe für den Server anzuzeigen.
- Informationen zu allgemeinen Serverparametern anzuzeigen, zum Beispiel zu den mit den SET-Befehlen definierten Parametern.
- Informationen zu Clientsitzungen anzufordern, beispielsweise die Verfügbarkeit des Servers, Kennwortauthentifizierung, Einstellungen für die Abrechnung oder die Aufbewahrungsdauer der Informationen, die im Aktivitätenprotokoll aufbewahrt werden.
- Informationen über den zentralen Scheduler anzuzeigen, beispielsweise den zentralen Planungsmodus des Servers.
- die maximale Anzahl der Wiederholungen anzuzeigen, die nach der fehlgeschlagenen Ausführung eines geplanten Befehls zulässig sind.
- anzuzeigen, ob Subdateien auf diesem Server gesichert werden können, wie durch den Befehl SET SUBFILE angegeben ist.
- Informationen zu einem Zielreplikationsserver anzuzeigen.
- Lizenzinformationen anzuzeigen.

Tipp: Um Informationen zu einem Zielreplikationsserver anzuzeigen, müssen Sie den Befehl auf dem Zielreplikationsserver ausgeben.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-Query STatus-----<<
```

## Parameter

Keine.

## Beispiel: Den Status eines Konfigurationsmanagers abfragen

Allgemeine Informationen zu Serverparametern anzeigen. Der Befehl wird von einem Konfigurationsmanager ausgeführt. Beschreibungen der angezeigten Felder befinden sich in Feldbeschreibungen.

```
query status
```

 AIX-Betriebssysteme

```

Servername: SETSHOT
Server-Host-Name oder IP-Adresse: setshot
Server-TCP/IP-Anschlussnummer: 1500
Überkreuzdefinition: On
Serverkennwort definiert: Yes
Datum/Zeit der Serverinstallation: 2016-07-08, 09:45:53
Datum/Zeit des Serverneustarts: 2016-10-10, 05:38:49
Authentifizierung: Off
Kennwortablaufdauer: 9.999 Tag(e)
Grenzwert für ungültige Anmeldeversuche: 0
Mindestlänge für Kennwort: 0
Registrierung: Geschlossen
Subdateisicherung: Client
Verfügbarkeit: Aktiviert
Inaktivierte eingehende Sitzungen:
Inaktivierte abgehende Sitzungen:
Abrechnung: Off
Aufbewahrungsdauer für Aktivitätenprotokoll: 30 Tag(e)
Anzahl Sätze im Aktivitätenprotokoll: 222919
Größe des Aktivitätenprotokolls: 6 M
Aufbewahrungszeitraum für Aktivitätsübers.: 30 Tag(e)

```

```

Intervall für Lizenzprüfung: 30 Tag(e)
  Letzte Lizenzprüfung: 2016-10-21, 07:40:20
  Server-Lizenzbestimmungen: Gültig
    Zentraler Scheduler: Aktiv
  Maximale Anzahl Sitzungen: 300
  Maximale Anzahl geplanter Sitzungen: 75
  Aufbewahrungszeitraum für Ereignissätze: 14 Tag(e)
    Dauer von Clientaktionen: 5 Tage(e)
  Zeitplanzufallsgenerierung (Prozent): 25
    Intervall für Zeitplanabfragen: Client
  Maximale Anzahl Befehlswiederholungen: Client
    Wiederholungszeitlimit: Client
  Prüfstufe für clientseitige Deduplizierung: 0%
    Planungsmodi: Beliebig
      Aktive Empfänger: CONSOLE ACTLOG
    Konfigurationsmanager?: Off
    Aktualisierungsintervall: 60
  Datum/Zeit der letzten Aktualisierung:
  Anzeigen von Nachrichtenkontext: On
  Aufbewahrungszeitraum für Laden für Inhaltsverzeichnis: 120 Minute(n)
  Maschinen-GUID:
d4.cg.f6.ae.04.6e.11.e3.80.1f.00.21.5e.18.df.01
  Aufbewahrungsschutz für Archivierung: Off
    Datenbankverzeichnisse: /TSMserver/DB1,/TSMserver/DB2
  Gesamtspeicherbereich des Dateisystems (MB): 222.720,00
  Verwendeter Speicherbereich im Dateisystem (MB): 47.780,74
  Freier verfügbarer Speicherbereich (MB): 174.939,26
  Verschlüsselungsstufe: AES
  Aktualisierungsintervall für Client-CPU-Informationen: 180
    Abgehende Replikation: Enabled
    Zielreplikationsserver: POWER
  Standardreplikationsregel für Archivierungsdaten: ALL_DATA
  Standardreplikationsregel für Sicherungsdaten: ALL_DATA
  Standardreplikationsregel für speicher verwaltete Daten: ALL_DATA
  Aufbewahrungszeitraum für Replikationsdatensätze: 30 Tag(e)
    LDAP-Benutzer:
      LDAP-Kennwort definiert: No
    Standardauthentifizierung: Local
  Adresse höherer Ebene für Übernahme:
  Aufbewahrungszeit für Scratchpad: 365 Tag(e)
  Replikationswiederherstellung beschädigter Dateien: On
    SUR-Belegung (TB): 5,66
    SUR-Belegung (Datum/Zeit): 2016-10-10, 05:39:33
    Front-End-Kapazität (MB): 226.331
    Anzahl Front-End-Clients: 6
    Datum für Front-End-Kapazität: 2016-10-13, 09:20:02
    Produktangebot: IBM Spectrum Protect

```

## Linux-Betriebssysteme

```

  Servername: GOBI
  Server-Host-Name oder IP-Adresse:
  Server-TCP/IP-Anschlussnummer: 1500
  Überkreuzdefinition: On
  Serverkennwort definiert: Yes
  Datum/Zeit der Serverinstallation: 2016-07-08, 11:29:03
  Datum/Zeit des Serverneustarts: 2016-11-10, 14:25:03
  Authentifizierung: On
  Kennwortablaufdauer: 90 Tag(e)
  Grenzwert für ungültige Anmeldeversuche: 0
  Mindestlänge für Kennwort: 0
  Registrierung: Geschlossen
  Subdateisicherung: No
  Verfügbarkeit: Aktiviert
  Inaktivierte eingehende Sitzungen:
  Inaktivierte abgehende Sitzungen:
    Abrechnung: Off
  Aufbewahrungsdauer für Aktivitätenprotokoll: 30 Tag(e)
  Anzahl Sätze im Aktivitätenprotokoll: 21346
  Größe des Aktivitätenprotokolls: <1 M
  Aufbewahrungszeitraum für Aktivitätsübers.: 30 Tag(e)
  Intervall für Lizenzprüfung: 30 Tag(e)
    Letzte Lizenzprüfung: 2016-10-21, 23:27:23
  Server-Lizenzbestimmungen: Gültig
    Zentraler Scheduler: Aktiv
  Maximale Anzahl Sitzungen: 500
  Maximale Anzahl geplanter Sitzungen: 250
  Aufbewahrungszeitraum für Ereignissätze: 14 Tag(e)

```

```

Dauer von Clientaktionen: 5 Tage(e)
Zeitplanzufallsgenerierung (Prozent): 25
Intervall für Zeitplanabfragen: Client
Maximale Anzahl Befehlswiederholungen: Client
Wiederholungszeitlimit: Client
Prüfstufe für clientseitige Deduplizierung: 0%
Planungsmodi: Beliebig
Aktive Empfänger: CONSOLE ACTLOG
Konfigurationsmanager?: Off
Aktualisierungsintervall: 60
Datum/Zeit der letzten Aktualisierung:
Anzeigen von Nachrichtenkontext: Off
Aufbewahrungszeitraum für Laden für Inhaltsverzeichnis: 120 Minute(n)
Maschinen-GUID:
fc.e7.be.58.4a.a7.11.e0.8a.c8.e4.1f.13.34.11.e0
Aufbewahrungsschutz für Archivierung: Off
Datenbankverzeichnisse:
/TSMdbspace1/gpcinst1,/TSMdbspace2/gpcinst1,/TSMdbspace3/gpcinst1
GesamtSpeicherbereich des Dateisystems (MB): 302.379,84
Verwendeter Speicherbereich im Dateisystem (MB): 106.793,65
Freier verfügbarer Speicherbereich (MB): 195.586,20
Verschlüsselungsstufe: AES
Aktualisierungsintervall für Client-CPU-Informationen: 180
Abgehende Replikation: Enabled
Zielreplikationsserver:
Standardreplikationsregel für Archivierungsdaten: ALL_DATA
Standardreplikationsregel für Sicherungsdaten: ALL_DATA
Standardreplikationsregel für speicher verwaltete Daten: ALL_DATA
Aufbewahrungszeitraum für Replikationsdatensätze: 30 Tag(e)
LDAP-Benutzer:
LDAP-Kennwort definiert: No
Standardauthentifizierung: Local
Adresse höherer Ebene für Übernahme:
Aufbewahrungszeit für Scratchpad: 365 Tag(e)
Replikationswiederherstellung beschädigter Dateien: Off
SUR-Belegung (TB): 0,00
SUR-Belegung (Datum/Zeit): 2016-10-10, 14:25:35
Front-End-Kapazität (MB): 226.331
Anzahl Front-End-Clients: 6
Datum für Front-End-Kapazität: 2016-10-13, 09:20:02
Produktangebot: IBM Spectrum Protect

```

#### Windows-Betriebssysteme

```


Servername: EXCELSIOR
Server-Host-Name oder IP-Adresse: excelsior.storage.
newyork.example.com
Server-TCP/IP-Anschlussnummer: 1500
Überkreuzdefinition: On
Serverkennwort definiert: Yes
Datum/Zeit der Serverinstallation: 2016-07-08, 18:02:50
Datum/Zeit des Serverneustarts: 2016-11-10, 11:48:32
Authentifizierung: On
Kennwortablaufdauer: 90 Tag(e)
Grenzwert für ungültige Anmeldeversuche: 0
Mindestlänge für Kennwort: 0
Registrierung: Geschlossen
Subdateisicherung: No
Verfügbarkeit: Aktiviert
Inaktivierte eingehende Sitzungen:
Inaktivierte abgehende Sitzungen:
Abrechnung: On
Aufbewahrungsdauer für Aktivitätenprotokoll: 30 Tag(e)
Anzahl Sätze im Aktivitätenprotokoll: 1346376
Größe des Aktivitätenprotokolls: 37 M
Aufbewahrungszeitraum für Aktivitätsübers.: 30 Tag(e)
Intervall für Lizenzprüfung: 30 Tag(e)
Letzte Lizenzprüfung: 2016-10-21, 17:05:16
Server-Lizenzbestimmungen: Gültig
Zentraler Scheduler: Aktiv
Maximale Anzahl Sitzungen: 25
Maximale Anzahl geplanter Sitzungen: 12
Aufbewahrungszeitraum für Ereignissätze: 14 Tag(e)
Dauer von Clientaktionen: 5 Tage(e)
Zeitplanzufallsgenerierung (Prozent): 25
Intervall für Zeitplanabfragen: Client
Maximale Anzahl Befehlswiederholungen: Client

```

```

Wiederholungszeitlimit: Client
Prüfstufe für clientseitige Deduplizierung: 0%
Planungsmodi: Beliebig
Aktive Empfänger: CONSOLE ACTLOG
NTEVENTLOG
Konfigurationsmanager?: Off
Aktualisierungsintervall: 60
Datum/Zeit der letzten Aktualisierung:
Anzeigen von Nachrichtenkontext: Off
Aufbewahrungszeitraum für Laden für Inhaltsverzeichnis: 120 Minute(n)
Maschinen-GUID:
e9.3e.f1.70.ff.c5.11.e2.a5.67.5c.f3.fc.0c.5e.60
Aufbewahrungsschutz für Archivierung: Off
Datenbankverzeichnisse: e:\Server1\TSMDBdir
Gesamtspeicherbereich des Dateisystems (MB): 102.270,00
Verwendeter Speicherbereich im Dateisystem (MB): 22.032,79
Freier verfügbarer Speicherbereich (MB): 80.237,20
Verschlüsselungsstufe: AES
Aktualisierungsintervall für Client-CPU-Informationen: 180
Abgehende Replikation: Enabled
Zielreplikationsserver: EXPLORER
Standardreplikationsregel für Archivierungsdaten: ALL_DATA
Standardreplikationsregel für Sicherungsdaten: ALL_DATA
Standardreplikationsregel für speicher verwaltete Daten: ALL_DATA
Aufbewahrungszeitraum für Replikationsdatensätze: 30 Tag(e)
LDAP-Benutzer: cn=excelsior_ldapadmin,ou=excelsior,
ou=John Doe,dc=tsmadldap,dc=storage,
dc=newyork, dc=example,dc=com
LDAP-Kennwort definiert: Yes
Standardauthentifizierung: LDAP
Adresse höherer Ebene für Übernahme:
Aufbewahrungszeit für Scratchpad: 365 Tag(e)
Replikationswiederherstellung beschädigter Dateien: On
SUR-Belegung (TB): 8,98
SUR-Belegung (Datum/Zeit): 2016-10-10, 11:49:27
Front-End-Kapazität (MB): 226.331
Anzahl Front-End-Clients: 6

```

 Windows-Betriebssysteme

Datum für Front-End-Kapazität: 2016-10-13, 09:20:02  
Produktangebot: IBM Spectrum Protect

## Feldbeschreibungen

---

### Servername

Gibt den Namen des Servers an.

### Server-Host-Name oder IP-Adresse

Gibt die Server-TCP/IP-Adresse an.

### Server-TCP/IP-Anschlussnummer

Gibt die Serveranschlussadresse an.

### Überkreuzdefinition

Gibt an, ob ein anderer Server, der den Befehl DEFINE SERVER ausführt, sich automatisch selbst für diesen Server definiert. Siehe Befehl SET CROSSDEFINE.

### Server-Kennwort definiert

Gibt an, ob das Kennwort für den Server definiert wurde.

### Datum/Zeit der Serverinstallation

Gibt das Datum und die Uhrzeit an, an dem bzw. zu der der Server installiert wurde.

### Datum/Zeit des Serverneustarts

Gibt das Datum und die Uhrzeit an, an dem bzw. zu der der Server zuletzt gestartet wurde.

### Authentifizierung

Gibt an, ob die Kennwortauthentifizierung aktiviert oder inaktiviert ist.

### Kennwortablaufdauer

Gibt die Anzahl Tage an, nach deren Ablauf das Kennwort für den Administrator oder den Clientknoten seine Gültigkeit verliert.

### Grenzwert für ungültige Anmeldeversuche

Gibt die Anzahl der ungültigen Anmeldeversuche an, die zulässig sind, bevor der Knoten gesperrt wird.

### Mindestlänge für Kennwort

Gibt die Mindestanzahl Zeichen für das Kennwort an.

### Registrierung

Gibt an, ob die Registrierung für den Clientknoten geöffnet oder geschlossen ist.

### Subdateisicherung

Gibt an, ob Subdateien auf diesem Server gesichert werden können, wie durch den Befehl SET SUBFILE angegeben ist.

Verfügbarkeit  
Gibt an, ob der Server aktiviert oder inaktiviert ist.

Inaktivierte eingehende Sitzungen  
Gibt die Namen der Server an, von denen eine Übertragung zwischen Servern nicht zulässig ist. Um eingehende Serversitzungen zu aktivieren, verwenden Sie den Befehl ENABLE SESSIONS.

Inaktivierte abgehende Sitzungen  
Gibt die Namen der Server an, zu denen eine Übertragung zwischen Servern nicht zulässig ist. Um abgehende Serversitzungen zu aktivieren, verwenden Sie den Befehl ENABLE SESSIONS.

Abrechnung  
Gibt an, ob am Ende jeder Sitzung des Clientknotens ein Abrechnungssatz generiert wird.

Aufbewahrungsdauer für Aktivitätenprotokoll  
Gibt die Anzahl der Tage, die Informationen im Aktivitätenprotokoll aufbewahrt werden, oder die Größe des Protokolls an.

Anzahl Sätze im Aktivitätenprotokoll  
Gibt die Anzahl der Sätze im Aktivitätenprotokoll an.

Größe des Aktivitätenprotokolls  
Gibt die Größe des Aktivitätenprotokolls an.

Aufbewahrungszeitraum für Aktivitätsübersicht  
Gibt die Anzahl der Tage an, die Informationen in der SQL-Aktivitätsübersichtstabelle aufbewahrt werden sollen.

Intervall für Lizenzprüfung  
Gibt den Zeitraum an (in Tagen), nach dessen Ablauf der Lizenzmanager automatisch die IBM Spectrum Protect-Lizenz prüft. Zusätzliche Lizenzinformationen sind verfügbar, wenn der Befehl QUERY LICENSE verwendet wird.

Letzte Lizenzprüfung  
Gibt an, wann die Lizenzprüfung zuletzt durchgeführt wurde (Datum und Uhrzeit). Zusätzliche Lizenzinformationen sind verfügbar, wenn der Befehl QUERY LICENSE verwendet wird.

Server-Lizenzbestimmungen  
Gibt an, ob sich der Server an die Lizenzbedingungen hält (Gültig) oder nicht (Fehlgeschlagen). Mit dem Befehl QUERY LICENSE kann abgefragt werden, aufgrund welcher Faktoren der Server nicht die Lizenzbedingungen einhält.

Zentraler Scheduler  
Gibt an, ob die zentrale Zeitplanung aktiv oder inaktiv ist.

Maximale Anzahl Sitzungen  
Gibt die maximale Anzahl Client-/Serversitzungen an.

Maximale Anzahl geplante Sitzungen  
Gibt die maximale Anzahl Client-/Serversitzungen an, die bei der Arbeit mit einem Verarbeitungszeitplan verfügbar sind.

Aufbewahrungszeitraum für Ereignissätze  
Gibt an, wie lange Scheduler-Ereignissätze beibehalten werden (Anzahl Tage).

Dauer von Clientaktionen  
Gibt den Zeitraum an, in dem der Client den mit dem Befehl DEFINE CLIENTACTION definierten Zeitplan verarbeitet.

Zeitplanzufallsgenerierung (Prozent)  
Gibt an, welcher Anteil des Startfensters für die Ausführung von geplanten Ereignissen im Clientabfragemodus verwendet wird.

Intervall für Zeitplanabfragen  
Gibt die Häufigkeit an, mit der Clients den Server nach geplanter Arbeit abfragen, und zwar im Clientabfragemodus. Lautet der Wert in diesem Feld 'Client', wird die Abfragehäufigkeit vom Clientknoten bestimmt.

Maximale Anzahl Befehlswiederholungen  
Gibt an, wie oft ein Client-Scheduler maximal versucht, einen geplanten Befehl auszuführen, nachdem ein Versuch fehlgeschlagen ist. Lautet der Wert in diesem Feld 'Client', wird die maximale Anzahl vom Clientknoten bestimmt.

Wiederholungszeitlimit  
Gibt die Anzahl Minuten zwischen fehlgeschlagenen Versuchen des Client-Schedulers an, den Server anzusprechen oder einen geplanten Befehl auszuführen. Lautet der Wert in diesem Feld 'Client', bestimmt der Clientknoten die Anzahl der Minuten.

Prüfstufe für clientseitige Deduplizierung  
Gibt einen Prozentsatz der Bereiche an, die vom IBM Spectrum Protect-Server geprüft werden sollen. Die Bereiche werden während der clientseitigen Dateneduplizierung erstellt.

Planungsmodi  
Gibt die vom Server unterstützten Modi für die zentrale Zeitplanung an.

Aktive Empfänger  
Gibt die Empfänger an, für die das Protokollieren von Ereignissen begonnen hat.

Konfigurationsmanager?  
Gibt an, ob der Server ein Konfigurationsmanager ist.

Aktualisierungsintervall  
Gibt das Intervall an, nach dem der verwaltete Server eine Aktualisierung aller Änderungen von einem Konfigurationsmanager anfordert.

Datum/Zeit der letzten Aktualisierung  
Wenn der Server ein verwalteter Server ist, werden das Datum und die Uhrzeit der letzten erfolgreichen Aktualisierung der Konfigurationsdaten vom Konfigurationsmanager angegeben.

Anzeigen von Nachrichtenkontext  
Gibt an, ob das Anzeigen von Nachrichtenkontext aktiviert oder inaktiviert ist.

#### Aufbewahrungszeitraum für Laden für Inhaltsverzeichnis

Gibt die ungefähre Anzahl der Minuten an, die Inhaltsverzeichnisdaten, auf die nicht verwiesen wird, in der Datenbank aufbewahrt werden.

#### Maschinen-GUID

Die global eindeutige ID (Globally Unique Identifier = GUID) zu dem Zeitpunkt, als der Server das letzte Mal gestartet wurde. Diese GUID identifiziert das Hostsystem, zu dem der aktuelle Server gehört.

#### Aufbewahrungsschutz für Archivierung

Gibt an, ob der Aufbewahrungsschutz für Archivierungsdaten aktiviert oder inaktiviert ist.

#### Datenbankverzeichnisse

Gibt die Positionen der Datenbankverzeichnisse an.

#### GesamtSpeicherbereich des Dateisystems (MB)

Gibt die Gesamtgröße des Dateisystems an.

#### Verwendeter Speicherbereich im Dateisystem (MB)

Gibt den Speicherbereich an, der in dem Dateisystem verwendet wird.

#### Freier verfügbarer Speicherbereich (MB)

Gibt den Speicherbereich an, der verfügbar ist.

#### Verschlüsselungsstufe

Gibt die Datenverschlüsselungsstufe an: AES oder DES.

#### Aktualisierungsintervall für Client-CPU-Informationen

Gibt die Anzahl der Tage an, die zwischen Clientsuchläufen nach CPU-Informationen vergehen, die für PVU-Schätzungen verwendet werden.

#### Abgehende Replikation

Gibt an, ob die Replikationsverarbeitung aktiviert oder inaktiviert ist. Ist die abgehende Replikation inaktiviert, können keine neuen Replikationsprozesse auf dem Server gestartet werden.

#### Zielreplikationsserver

Gibt den Namen des Servers an, der das Ziel für Knotenreplikationsoperationen ist. Ist kein Zielreplikationsserver vorhanden, ist dieses Feld leer.

#### Standardreplikationsregel für Archivierungsdaten

Gibt die Serverreplikationsregel an, die für Archivierungsdaten gilt. Die folgenden Werte sind gültig:

##### ALL\_DATA

Repliziert Archivierungsdaten. Die Daten werden mit einer normalen Priorität repliziert.

##### ALL\_DATA\_HIGH\_PRIORITY

Repliziert Archivierungsdaten. Die Daten werden mit einer hohen Priorität repliziert.

##### NONE

Die Archivierungsdaten werden nicht repliziert.

#### Standardreplikationsregel für Sicherungsdaten

Gibt die Serverreplikationsregel an, die für Sicherungsdaten gilt. Die folgenden Werte sind gültig:

##### ALL\_DATA

Repliziert aktive und inaktive Sicherungsdaten. Die Daten werden mit einer normalen Priorität repliziert.

##### ACTIVE\_DATA

Repliziert nur aktive Sicherungsdaten. Die Daten werden mit einer normalen Priorität repliziert.

Achtung: Wenn Sie ACTIVE\_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

- Wenn eine frühere Serverversion als Version 7.1.1 auf dem Quellen- oder Zielreplikationsserver installiert ist.
- Wenn Sie den Befehl REPLICATE NODE mit dem Parameter `FORCERECONCILE=YES` verwenden.
- Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Serverversion vor Version 7.1.1 ausführen.

Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

##### ALL\_DATA\_HIGH\_PRIORITY

Repliziert aktive und inaktive Sicherungsdaten. Die Daten werden mit einer hohen Priorität repliziert.

##### ACTIVE\_DATA\_HIGH\_PRIORITY

Diese Regel entspricht der Replikationsregel ACTIVE\_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden.

##### NONE

Die Sicherungsdaten werden nicht repliziert.

#### Standardreplikationsregel für speicherverwaltete Daten

Gibt die Serverreplikationsregel an, die für speicherverwaltete Daten gilt. Die folgenden Werte sind gültig:

ALL\_DATA

Repliziert speicherverwaltete Daten. Die Daten werden mit einer normalen Priorität repliziert.

ALL\_DATA\_HIGH\_PRIORITY

Repliziert speicherverwaltete Daten. Die Daten werden mit einer hohen Priorität repliziert.

NONE

Speicherverwaltete Daten werden nicht repliziert.

**Aufbewahrungszeitraum für Replikationsdatensätze**

Gibt die Anzahl der Tage an, die Replikationsprotokolldatensätze in der Datenbank des Quellenreplikationsservers aufbewahrt werden.

**LDAP-Benutzer**

Gibt die Benutzer-ID an, die im Befehl SET LDAPUSER angegeben wurde. Diese Benutzer-ID kann Verwaltungsbefehle für den Namensbereich ausgeben, der für IBM Spectrum Protect auf dem LDAP-Verzeichnisserver reserviert ist.

**LDAP-Kennwort definiert**

Dieses Ausgabefeld zeigt an, ob ein Kennwort für die Benutzer-ID definiert ist, die im Befehl SET LDAPUSER angegeben wurde. Die Werte lauten YES und NO. Lautet der Wert YES, kann die im Befehl SET LDAPUSER angegebene Benutzer-ID Verwaltungsbefehle für den LDAP-Namensbereich ausgeben, der für IBM Spectrum Protect reserviert ist. Lautet der Wert NO, geben Sie den Befehl SET LDAPPASSWORD aus, um das Kennwort für die Benutzer-ID festzulegen, die im Befehl SET LDAPUSER angegeben wurde.

**Standardauthentifizierung**

Gibt die Standardkennwortauthentifizierungsmethode an: LOCAL oder LDAP.

| Authentifizierungsziel      | Authentifizierungsmethode |
|-----------------------------|---------------------------|
| IBM Spectrum Protect-Server | LOCAL                     |
| LDAP-Verzeichnisserver      | LDAP                      |

Wenn Sie den Befehl SET DEFAULTAUTHENTICATION ausgeben, definieren Sie die resultierende Authentifizierungsmethode für alle Befehle REGISTER ADMIN und REGISTER NODE. Der Standardwert ist LOCAL.

**Adresse höherer Ebene für Übernahme**

Gibt die Adresse höherer Ebene für den Übernahmeserver an, der vom Client verwendet wird.

Clientzurückschreibungsoperationen werden durch Übernahme an diese Adresse der höheren Ebene übertragen, wenn die vom Client verwendete Schnittstelle von der Schnittstelle abweicht, die von der Replikation verwendet wird.

**Aufbewahrungszeit für Scratchpad**

Gibt die Anzahl Tage an, die Scratchpadeinträge nach ihrer letzten Aktualisierung aufbewahrt werden.

**Replikationswiederherstellung beschädigter Dateien**

Gibt an, ob die Knotenreplikation aktiviert ist, um beschädigte Dateien durch einen Zielreplikationsserver wiederherzustellen. Dies ist eine systemseitige Einstellung. Ist ON angegeben, kann der Knotenreplikationsprozess so konfiguriert werden, dass beschädigte Dateien auf einem Quellenreplikationsserver erkannt und durch unbeschädigte Dateien von einem Zielreplikationsserver ersetzt werden. Ist OFF angegeben, werden beschädigte Dateien nicht durch einen Zielreplikationsserver wiederhergestellt.

**SUR-Belegung (TB)**

Wenn Sie über eine Lizenz für IBM Spectrum Protect Suite (SUR) verfügen, gibt dieses Feld die SUR-Belegung auf dem Server an. Die *SUR-Belegung* ist die Größe des Speicherbereichs, die zum Speichern der Daten verwendet wird, die von den IBM Spectrum Protect-Produkten im SUR-Produktpaket verwaltet werden.

**SUR-Belegung (Datum/Zeit)**

Gibt das Datum und die Uhrzeit an, an dem bzw. zu der die SUR-Belegung zuletzt erfasst wurde.

**Front-End-Kapazität (MB)**

Gibt den Umfang der primären Daten an, die von Clients gesichert werden. Clients umfassen Anwendungen, virtuelle Maschinen und Systeme. Dieser Wert wird für das Front-End-Lizenzierungsmodell verwendet.

**Anzahl Front-End-Clients**

Gibt die Anzahl der Clients an, die eine Kapazitätsnutzung auf der Basis des Front-End-Lizenzierungsmodells zurückgemeldet haben.

**Datum für Front-End-Kapazität**

Gibt das Datum und die Uhrzeit an, an dem bzw. zu der Front-End-Kapazitätsdaten zuletzt erfasst wurden.

**Produktangebot**

Gibt ein Produktangebot an.

| Mit dem Befehl SET PRODUCTOFFERING angegebener Wert | In der Befehlsausgabe für QUERY STATUS angezeigter Wert |
|---|---|
| ENTry   | IBM Spectrum Protect Entry                              |
| DATARet   | IBM Spectrum Protect for Data Retention                 |
| BASIC   | IBM Spectrum Protect                                    |
| EE  | IBM Spectrum Protect Extended Edition                   |



| Mit dem Befehl SET PRODUCTOFFERING angegebener Wert | In der Befehlsausgabe für QUERY STATUS angezeigter Wert |
|---|---|
| SUIte   | IBM Spectrum Protect Suite                              |
| SUITEEntry  | IBM Spectrum Protect Suite Entry                        |
| SUITEArchive  | IBM Spectrum Protect Suite - Archive                    |
| SUITEProtectier                                     | IBM Spectrum Protect Suite - ProtecTier                 |
| SUITEFrontend                                       | IBM Spectrum Protect Suite - FrontEnd                   |
| SUITEENTRYFrontend                                  | IBM Spectrum Protect Suite Entry - FrontEnd             |
| CLEAR   | NULL  |

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY STATUS

| Befehl                     | Beschreibung   |
|----------------------------|--|
| BEGIN EVENTLOGGING         | Startet das Ereignisprotokoll für einen bestimmten Empfänger.  |
| DISABLE REPLICATION        | Verhindert die Verarbeitung abgehender Replikation auf einem Server.   |
| DISABLE SESSIONS           | Verhindert, dass neue Sitzungen auf IBM Spectrum Protect zugreifen, lässt jedoch zu, dass bestehende Sitzungen fortgesetzt werden. |
| ENABLE REPLICATION         | Ermöglicht die Verarbeitung abgehender Replikation auf einem Server.   |
| ENABLE SESSIONS            | Nimmt die Serveraktivität nach einem Befehl DISABLE oder ACCEPT DATE wieder auf.   |
| END EVENTLOGGING           | Beendet das Ereignisprotokoll für einen bestimmten Empfänger.  |
| QUERY LICENSE              | Zeigt Informationen über Lizenzen und Prüfvorgänge an.   |
| SET ACCOUNTING             | Gibt an, ob am Ende jeder Clientsitzung Abrechnungssätze erstellt werden.  |
| SET ACTLOGRETENTION        | Gibt die Anzahl Tage an, die Protokollsätze im Aktivitätenprotokoll aufbewahrt werden sollen.                                      |
| SET CONTEXTMESSAGING       | Gibt an, dass das Anzeigen von Nachrichtenkontext für eine Nachricht ANR9999D aktiviert werden soll.                               |
| SET CPUINFOREFRESH         | Gibt die Anzahl der Tage zwischen Clientsuchläufen nach Workstationinformationen an, die für PVU-Schätzungen verwendet werden.     |
| SET CROSSDEFINE            | Gibt an, ob Server überkreuz definiert werden sollen.  |
| SET DEDUPVERIFICATIONLEVEL | Gibt den Prozentsatz der Bereiche an, die vom Server während der clientseitigen Deduplizierung geprüft werden sollen.              |
| SET DEFAULTAUTHENTICATION  | Gibt die Standardkennwortauthentifizierungsmethode für alle Befehle REGISTER NODE oder REGISTER ADMIN an.                          |
| SET EVENTRETENTION         | Gibt die Anzahl Tage für die Aufbewahrung von Sätzen geplanter Operationen an.   |
| SET LDAPPASSWORD           | Legt das Kennwort für den LDAPUSER fest.   |
| SET LDAPUSER               | Definiert den Benutzer, der die Kennwörter und Administratoren auf dem LDAP-Verzeichnisserver überwacht.                           |
| SET MAXCMDRETRIES          | Gibt die maximale Anzahl Wiederholungen nach der fehlgeschlagenen Ausführung eines geplanten Befehls an.                           |
| SET MAXSCHEDESESSIONS      | Gibt die maximale Anzahl Client-/Serversitzungen an, die bei der Arbeit mit einem Verarbeitungszeitplan verfügbar sind.            |
| SET PASSEXP                | Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.   |

| Befehl                 | Beschreibung   |
|------------------------|--|
| SET PRODUCTOFFERING    | Definiert das für Ihr Unternehmen lizenzierte Produktangebot.  |
| SET QUERYSCHEDPERIOD   | Gibt die Häufigkeit an, mit der Clients geplante Arbeit im Clientsendeaufrufmodus abrufen.   |
| SET RANDOMIZE          | Gibt die Zufallsgenerierung von Startzeiten innerhalb eines Fensters für Zeitpläne im Clientsendeaufrufmodus an.                     |
| SET REPLRECOVERDAMAGED | Gibt an, ob die Knotenreplikation aktiviert ist, um beschädigte Dateien durch einen Zielreplikationsserver wiederherzustellen.       |
| SET RETRYPERIOD        | Gibt die Zeitspanne zwischen Wiederholungsversuchen des Client-Schedulers an.  |
| SET SCHEDMODES         | Gibt den zentralen Planungsmodus für den Server an.  |
| SET SERVERHLADDRESS    | Gibt die Adresse der höheren Ebene eines Servers an.   |
| SET SERVERLLADDRESS    | Gibt die Adresse der unteren Ebene eines Servers an.   |
| SET SERVERNAME         | Gibt den Namen an, unter dem der Server registriert ist.   |
| SET SERVERPASSWORD     | Gibt das Serverkennwort an.  |
| SET SUMMARYRETENTION   | Gibt die Anzahl Tage an, die Informationen in der Aktivitätsübersichtstabelle aufbewahrt werden sollen.                              |
| SET TOCLOADRETENTION   | Gibt die Anzahl Minuten an, die Informationen für Inhaltsverzeichnisgruppen, auf die nicht verwiesen wird, aufbewahrt werden sollen. |

## QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)

Mit diesem Befehl können Sie Informationen zu Schwellenwerten für die Statusüberwachung anzeigen.

Mit Statusüberwachungsschwellenwerten werden die definierten Bedingungen mit den Serverabfragen für die Statusüberwachung verglichen und die Ergebnisse in die Statusüberwachungstabelle eingefügt.

Es können mehrere Schwellenwerte für eine Aktivität definiert werden. Sie können beispielsweise einen Schwellenwert erstellen, der einen Warnstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 80 % ist. Sie können dann einen anderen Schwellenwert erstellen, der einen Fehlerstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 90 % ist.

Anmerkung: Wenn bereits ein Schwellenwert für eine Bedingung EXISTS definiert ist, können Sie keinen anderen Schwellenwert mit einem der anderen Bedingungstypen definieren.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

.<!--*----->
>>-Query STATusthreshold-->+-----+----->
    '-Schwellenwertname-'

.-Format-----Standard-----
>+-----+-----+----->
    '-Format-----+Standard-+'    '-Activity-----Aktivität-'
    '-Detailed-'

>+-----+-----+----->
    '-Condition-----+EXists-+'    '-Value-----Wertname-'
        +-GT-----+
        +-GE-----+
        +-LT-----+
        +-LE-----+
        '-Equal--'
```

```
>-----<
'-Status-----+Normal--+-'
  +-Warning-+-
    '-Error---'
```

## Parameter

### Schwellenwertname

Gibt den Schwellenwertnamen an. Der Name darf 48 Zeichen nicht überschreiten.

### Format

Gibt an, wie die Informationen angezeigt werden. Der Standardwert ist STANDARD. Gültige Werte:

#### Standard

Gibt an, dass Teilinformationen für die angegebenen Statusschwellenwerte angezeigt werden.

#### Detailed

Gibt an, dass die gesamten Informationen für die angegebenen Statusschwellenwerte angezeigt werden.

### Activity

Gibt die Aktivität an, für die Statusanzeiger angezeigt werden sollen. Wird kein Wert angegeben, werden Informationen für alle Aktivitäten angezeigt. Eine Liste der Aktivitäten befindet sich in der Beschreibung des Befehls DEFINE STATUSTHRESHOLD.

### Condition

Begrenzt die Ausgabe auf die Schwellenwerte, die mit dem angegebenen Wert übereinstimmen. Gültige Werte:

#### EXists

Zeigt Statusschwellenwerte an, bei denen die Bedingung gleich EXISTS ist.

#### GT

Zeigt Statusschwellenwerte an, bei denen die Bedingung gleich GT ist.

#### GE

Zeigt Statusschwellenwerte an, bei denen die Bedingung gleich GE ist.

#### LT

Zeigt Statusschwellenwerte an, bei denen die Bedingung gleich LT ist.

#### LE

Zeigt Statusschwellenwerte an, bei denen die Bedingung gleich LE ist.

#### EQual

Zeigt Statusschwellenwerte an, bei denen die Bedingung gleich EQUAL ist.

### Value

Zeigt Schwellenwerte an, die den angegebenen Wert haben. Wird kein Wert angegeben, werden Informationen für alle Werte angezeigt. Sie können eine ganze Zahl von 0 bis 9223372036854775807 angeben.

### Status

Zeigt Statusschwellenwerte an, die den angegebenen Statuswert haben. Wird kein Wert angegeben, werden Informationen für alle Werte angezeigt. Gültige Werte:

#### Normal

Zeigt die Statusschwellenwerte an, die einen normalen Statuswert haben.

#### Warnung

Zeigt die Statusschwellenwerte an, die einen Warnstatuswert haben.

#### Fehler

Zeigt die Statusschwellenwerte an, die einen Fehlerstatuswert haben.

## Statusschwellenwert abfragen

Mit dem folgenden Befehl alle Statusschwellenwerte abfragen:

```
query statusthreshold
```

| Schwellenwert-<br>name | Name der<br>Aktivität                                | Bedingungs-<br>name | Wert | Berichts-<br>status |
|------------------------|--|---------------------|------|---------------------|
| ACTIVELOGCHECK         | AUSLASTUNG DER<br>AKTIVEN<br>PROTOKOLLDATEN<br>(%)   | >                   | 90   | ERROR               |
| AVGSTGPLW              | DURCHSCHNITTL.<br>SPEICHERPOOL-<br>AUSLASTUNG<br>(%) | >                   | 85   | WARNING             |
| AVGSTGPLE              | DURCHSCHNITTL.                                       | >                   | 90   | ERROR               |

## Statusschwellenwerte abfragen und Detailformat anzeigen

Mit dem folgenden Befehl Statusschwellenwerte abfragen und die Ausgabe im Detailformat anzeigen:

```
query statusthreshold f=d
```

```
Schwellenwertname: ACTIVELOGCHECK
Name der Aktivität: AUSLASTUNG DER AKTIVEN PROTOKOLLDATTEI (%)
Bedingungsname: >
    Wert: 90
    Berichtsstatus: ERROR
    Servername: TSMAMP24

Schwellenwertname: AVGSTGPLW
Name der Aktivität: DURCHSCHNITTLICHE SPEICHERPOOLAUSLASTUNG (%)
Bedingungsname: >
    Wert: 85
    Berichtsstatus: WARNING
    Servername: TSMAMP24

Schwellenwertname: AVGSTGPLE
Name der Aktivität: DURCHSCHNITTLICHE SPEICHERPOOLAUSLASTUNG (%)
Bedingungsname: >
    Wert: 95
    Berichtsstatus: ERROR
    Servername: TSMAMP24
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY STATUSTHRESHOLD

| Befehl  | Beschreibung   |
|---|--|
| DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)   | Definiert einen Schwellenwert für die Statusüberwachung.   |
| DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)  | Löscht einen Schwellenwert für die Statusüberwachung.  |
| QUERY MONITORSTATUS (Überwachungsstatus abfragen)   | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                             |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)                                      | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                             |
| SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)        | Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.         |
| SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)   | Gibt an, ob die Statusüberwachung aktiviert werden soll.   |
| SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)   | Gibt das Aktualisierungsintervall für die Statusüberwachung an.  |
| SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll) | Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll. |
| UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)  | Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.   |

## QUERY STGPOOL (Speicherpools abfragen)

Mit diesem Befehl können Informationen über einen oder mehrere Speicherpools angezeigt werden. Mit diesem Befehl können auch Umlagerungsprozesse für Speicherpools überwacht werden.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
.*----- .-Format----Standard-----
>>-Query STGpool--+-+-----+----->
      '-Poolname-' '-Format----+Standard-+-'
                          '-Detailed-'

.-Pooltype----ANY-----
>--+-+-----+-----<
      '-Pooltype----+ANY-----+'
          +-Primary-----+
          +-Copy-----+
          +-COPYCONTainer-+
          '-ACTIVEdata----'
```

## Parameter

### Poolname

Gibt den Speicherpool an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Speicherpools angezeigt.

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Geben Sie einen der folgenden Werte an:

#### Standard

Gibt an, dass Teilinformationen angezeigt werden.

#### Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

### Pooltype

Gibt den Typ des Speicherpools an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Geben Sie einen der folgenden Werte an:

#### ANY

Primäre Speicherpools, Kopierspeicherpools und Pools für aktive Daten abfragen.

#### Primary

Nur primäre Speicherpools abfragen.

#### Copy

Nur Kopierspeicherpools abfragen.

#### COPYCONTainer

Nur Containerkopierspeicherpools abfragen.

#### ACTIVEdata

Nur Speicherpools für aktive Daten abfragen.

## Beispiel: Ausführliche Informationen zu Plattenspeicherpools mit wahlfreiem Zugriff anzeigen

Tipp: In den Beispielen für die detaillierte Ausgabe sind einige Felder leer, da sie für die angegebene Umgebung nicht gelten. Ausführliche Informationen zu einem Speicherpool mit dem Namen DISKPOOL anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query stgpool diskpool format=detailed
```

```
Speicherpoolname: DISKPOOL
    Speicherpooltyp: Primary
    Einheitenklassenname: DISK
    Speichertyp: DEVCLASS
    Cloudtyp:
    Cloud-URL:
    Cloud-ID:
    Cloudposition:
    Geschätzte Kapazität: 66 G
    Speicherbereichsauslöser Ausl.: 0.0
    Auslastung in %: 0,0
    Umlagerung in %: 3.1
    Prozent logische Belegung: 100.0
    Obere Umlagerungsschwelle in %: 90
    Untere Umlagerungsschwelle in %: 70
```

```

Umlagerungsverzögerung: 0
Umlagerung fortsetzen: Yes
Umlagerungsprozesse: 1
Wiederherstellungsprozesse: 1
Nächster Speicherpool:
Speicherpool wiederherstellen:
Schwelle für maximale Größe: No Limit
Zugriff: Read/Write
Beschreibung:
Überlaufstandort:
Umgelagerte Dateien zwischenspeichern?:
Zusammenfassen?: Group
Wiederherstellungsschwelle: 60
Grenzwert für Wiederh. ausgelag. Datenträger:
Maximale Anzahl Arbeitsdatenträger: 32
Anzahl verwendeter Arbeitsdatenträger: 1
Verzögerungszeitraum für Containerwiederverwendung: 1 Tag(e)
Wird Umlagerung ausgeführt?: No
Umgelagerte Datenmenge (MB): 0.00
Abgelaufene Umlagerungszeit (Sek): 0
Wird Wiederherstellung ausgeführt?: No

Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
Datum/Zeit der letzten Aktualisierung: 01/03/2014 13:57:16
Speicherpooldatenformat: Native
Kopierspeicherpool(s):
Pool(s) für aktive Daten:
Kopieren bei Fehler fortsetzen?: No
CRC-Daten: Yes
Wiederherstellungstyp: Threshold
Daten nach Löschen überschreiben: 2 Mal
Daten deduplizieren?: No
Prozesse zum Identifizieren doppelter Daten:
Komprimiert:
Deduplizierungseinsparungen:
Komprimierungseinsparungen:
Eingesparter Gesamtspeicherbereich:
Modus für automatisches Kopieren: Client
Enthält vom Client deduplizierte Daten?: No
Maximale Anzahl simultaner Writer:

```

Schutzprozesse:

```

Schutzspeicherpool: Lokale
Speicherpools schützen: Grenzwert für Datenträgerwiederherstellung:

```

```

Datum des letzten Schutzes in fernem Pool:
Datum des letzten Schutzes in lokalem Pool:
Deduplizierung erfordert Sicherung?:
Verschlüsselt:
Prozent verschlüsselt:
Zugeordneter Cloudspeicherbereich (MB):
Belegter Cloudspeicherbereich (MB):
Bucketname:
Lokale geschätzte Kapazität:
Lokale proz. Auslastung:
Lokale logische Belegung in Prozent:

```

## Beispiel: Ausführliche Informationen zu Plattenspeicherpools mit sequenziellem Zugriff anzeigen

Ausführliche Informationen zu einem Speicherpool mit dem Namen FILEPOOL anzeigen. Für Felddescriptions siehe Felddescriptions.

```
query stgpool filepool format=detailed
```

```

Speicherpoolname: FILEPOOL
Speicherpooltyp: Primary
Einheitenklassenname: FILEC
Speichertyp: DEVCLASS
Cloudtyp:
Cloud-URL:
Cloud-ID:
Cloudposition:
Geschätzte Kapazität: 66 G
Speicherbereichsauslöser Ausl.: 0.0
Auslastung in %: 0,0
Umlagerung in %: 3.1
Prozent logische Belegung: 100.0
Obere Umlagerungsschwelle in %: 90

```

```

Untere Umlagerungsschwelle in %: 70
  Umlagerungsverzögerung: 0
    Umlagerung fortsetzen: Yes
      Umlagerungsprozesse: 1
        Wiederherstellungsprozesse: 1
          Nächster Speicherpool:
            Speicherpool wiederherstellen:
              Schwelle für maximale Größe: No Limit
                Zugriff: Read/Write
                  Beschreibung:
                    Überlaufstandort:
                      Umgelagerte Dateien zwischenspeichern?:
                        Zusammenfassen?: Group
                          Wiederherstellungsschwelle: 60
                            Grenzwert für Wiederh. ausgelag. Datenträger:
                              Maximale Anzahl Arbeitsdatenträger: 32
                                Anzahl verwendeter Arbeitsdatenträger: 1
                                  Verzögerungszeitraum für Containerwiederverwendung: 1 Tag(e)
                                    Wird Umlagerung ausgeführt?: No
                                      Umgelagerte Datenmenge (MB): 0.00

Abgelaufene Umlagerungszeit (Sek): 0
  Wird Wiederherstellung ausgeführt?: No
    Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
      Datum/Zeit der letzten Aktualisierung: 01/02/2014 13:57:16
        Speicherpooldatenformat: Native
          Kopierspeicherpool(s):
            Pool(s) für aktive Daten:
              Kopieren bei Fehler fortsetzen?: No
                CRC-Daten: Yes
                  Wiederherstellungstyp: Threshold
                    Daten nach Löschen überschreiben:
                      Daten deduplizieren?: Yes
                        Prozesse zum Identifizieren doppelter Daten: 1
                          Komprimiert:
                            Deduplizierungseinsparungen: 65.396 K (49,99 %)
                              Komprimierungseinsparungen:
                                Eingesparter Gesamtspeicherbereich: 65.396 K (49,99 %)
                                  Modus für automatisches Kopieren: Client
                                    Enthält vom Client deduplizierte Daten?: Yes
                                      Maximale Anzahl simultaner Writer:

```

Schutzprozesse:

```

  Schutzspeicherpool: Lokale
Speicherpools schützen: Grenzwert für Datenträgerwiederherstellung:
  Datum des letzten Schutzes in fernem Pool:
    Datum des letzten Schutzes in lokalem Pool:
      Deduplizierung erfordert Sicherung?:
        Verschlüsselt:
          Prozent verschlüsselt:
            Zugeordneter Cloudspeicherbereich (MB):
              Belegter Cloudspeicherbereich (MB):
                Bucketname:
                  Lokale geschätzte Kapazität:
                    Lokale proz. Auslastung:
                      Lokale logische Belegung in Prozent:

```

## Beispiel: Ausführliche Informationen zu sequenziellen Speicherpools anzeigen

Ausführliche Informationen zu einem sequenziellen Speicherpool für aktive Daten mit dem Namen FILEPOOL anzeigen, der eine Einheitenklasse FILE verwendet. Für Felddescriptions siehe Felddescriptions.

```
query stgpool filepool format=detailed
```

```

Speicherpoolname: FILEPOOL
  Speicherpooltyp: Active-data
Einheitenklassenname: FILEC
  Speichertyp: DEVCLASS
    Cloudtyp:
      Cloud-URL:
        Cloud-ID:
          Cloudposition:
            Geschätzte Kapazität: 0.0 M
Speicherbereichsauslöser Ausl.: 0.0
  Auslastung in %: 0,0
    Umlagerung in %: 0.0
      Prozent logische Belegung: 0.0
        Obere Umlagerungsschwelle in %: 90

```

```

Untere Umlagerungsschwelle in %: 70
Umlagerungsverzögerung: 0
Umlagerung fortsetzen: Yes
Umlagerungsprozesse: 1
Wiederherstellungsprozesse: 1
Nächster Speicherpool:
Speicherpool wiederherstellen:
Schwelle für maximale Größe: No Limit
Zugriff: Read/Write
Beschreibung:
Überlaufstandort:
Umgelagerte Dateien zwischenspeichern?:
Zusammenfassen?: Group
Wiederherstellungsschwelle: 60
Grenzwert für Wiederh. ausgelag. Datenträger:
Maximale Anzahl Arbeitsdatenträger: 99
Anzahl verwendeter Arbeitsdatenträger: 0
Verzögerungszeitraum für Containerwiederverwendung: 1 Tag(e)
Wird Umlagerung ausgeführt?: No
Umgelagerte Datenmenge (MB): 0.00

Abgelaufene Umlagerungszeit (Sek): 0
Wird Wiederherstellung ausgeführt?: No
Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
Datum/Zeit der letzten Aktualisierung: 01/02/2014 11:37:57
Speicherpooldatenformat: Native
Kopienspeicherpool(s):
Pool(s) für aktive Daten:
Kopieren bei Fehler fortsetzen?:
CRC-Daten: Yes
Wiederherstellungstyp: Threshold
Daten nach Löschen überschreiben:
Daten deduplizieren?: Yes
Prozesse zum Identifizieren doppelter Daten: 1
Komprimiert:
Deduplizierungseinsparungen: 65.396 K (49,99 %)
Komprimierungseinsparungen:
Eingesparter Gesamtspeicherbereich: 65.396 K (49,99 %)
Modus für automatisches Kopieren:
Enthält vom Client deduplizierte Daten?: No
Maximale Anzahl simultaner Writer:

```

Schutzprozesse:

Schutzspeicherpool: Lokale

Speicherpools schützen: Grenzwert für Datenträgerwiederherstellung:

```

Datum des letzten Schutzes in fernem Pool:
Datum des letzten Schutzes in lokalem Pool:
Deduplizierung erfordert Sicherung?:
Verschlüsselt:
Prozent verschlüsselt:
Zugeordneter Cloudspeicherbereich (MB):
Belegter Cloudspeicherbereich (MB):
Bucketname:
Lokale geschätzte Kapazität:
Lokale proz. Auslastung:
Lokale logische Belegung in Prozent:

```

## Beispiel: Übersichtsdaten zu einem bestimmten Speicherpool anzeigen

Informationen zu einem Speicherpool mit dem Namen POOL1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query stgpool pool1
```

| Speicher-<br>poolname | Einheiten-<br>klassenname | Geschätzte<br>Kapazität | %<br>Ausl | %<br>Uml. | Ob.<br>Uml. | Unt.<br>Uml. | Nächster<br>Speicher-<br>pool |
|-----------------------|---------------------------|-------------------------|-----------|-----------|-------------|--------------|-------------------------------|
| POOL1                 | DISK                      | 58.5 M                  | 0.8       | 0.7       | 90          | 70           | POOL2                         |

## Beispiel: Ausführliche Informationen zu einem 8-mm-Bandspeicherpool anzeigen

Ausführliche Informationen über den Speicherpool 8MMPool anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query stgpool 8mmpool format=detailed
```

```

Speicherpoolname: 8MMPool
Speicherpooltyp: Primary

```



```

Einheitenklassenname: 8MMTAPE
Speichertyp: DEVCLASS
  Cloudtyp:
  Cloud-URL:
  Cloud-ID:
  Cloudposition:
  Geschätzte Kapazität: 0.0 M
Speicherbereichsauslöser Ausl.: 0.0
  Auslastung in %: 0,0
  Umlagerung in %:
  Prozent logische Belegung: 0.0
  Obere Umlagerungsschwelle in %: 90
  Untere Umlagerungsschwelle in %: 70
  Umlagerungsverzögerung: 0
  Umlagerung fortsetzen: Yes
  Umlagerungsprozesse: 1
  Wiederherstellungsprozesse: 1
  Nächster Speicherpool:
  Speicherpool wiederherstellen:
  Schwelle für maximale Größe: 5 M
  Zugriff: Read/Write
  Beschreibung: Hauptspeicherpool
  Überlaufstandort: Room1234/Bldg31
Umgelagerte Dateien zwischenspeichern?:
  Zusammenfassen?: No
  Wiederherstellungsschwelle: 60
Grenzwert für Wiederh. ausgelag. Datenträger:
  Maximale Anzahl Arbeitsdatenträger: 5
  Anzahl verwendeter Arbeitsdatenträger: 3
Verzögerungszeitraum für Containerwiederverwendung: 1 Tag(e)
  Wird Umlagerung ausgeführt?: No
  Umgelagerte Datenmenge (MB): 0.00

  Abgelaufene Umlagerungszeit (Sek): 0
  Wird Wiederherstellung ausgeführt?: No
  Letzte Aktualisierung durch (Administrator): ADMIN
  Datum/Zeit der letzten Aktualisierung: 01/08/2014 06:55:45
  Speicherpooldatenformat: Native
  Kopierspeicherpool(s): COPYPOOL1
  Pool(s) für aktive Daten: ACTIVEPOOL1 ACTIVEPOOL2
  Kopieren bei Fehler fortsetzen?: Yes
  CRC-Daten: Yes
  Wiederherstellungstyp: Threshold
  Daten nach Löschen überschreiben:
  Daten deduplizieren?: No
  Prozesse zum Identifizieren doppelter Daten:
  Komprimiert:
  Deduplizierungseinsparungen:
  Komprimierungseinsparungen:
  Eingesparter Gesamtspeicherbereich:
  Komprimiert: No
  Deduplizierungseinsparungen:
  Komprimierungseinsparungen:
  Eingesparter Gesamtspeicherbereich:
  Modus für automatisches Kopieren: Client
  Enthält vom Client deduplizierte Daten?: No
  Maximale Anzahl simultaner Writer:

```

Schutzprozesse:

```

Schutzspeicherpool: Lokale
Speicherpools schützen: Grenzwert für Datenträgerwiederherstellung:

```

```

Datum des letzten Schutzes in fernem Pool:
Datum des letzten Schutzes in lokalem Pool:
Deduplizierung erfordert Sicherung?:
Verschlüsselt:
  Prozent verschlüsselt:
Zugeordneter Cloudspeicherbereich (MB):
  Belegter Cloudspeicherbereich (MB):
  Bucketname:
  Lokale geschätzte Kapazität:
  Lokale proz. Auslastung:
  Lokale logische Belegung in Prozent:

```

## Beispiel: Ausführliche Informationen zum Speicherpool NAS2CLASS anzeigen

Ausführliche Informationen zum Speicherpool NAS2LIBPOOL anzeigen. Bei der Definition dieses Speicherpools wird das Datenformat auf NETAPPDUMP gesetzt. Für Felddesreibungen siehe Felddesreibungen.

query stgpool nas2libpool format=detailed

```
Speicherpoolname: NAS2
    Speicherpoolname: NAS2LIBPOOL
    Speicherpooltyp: Primary
    Einheitenklassenname: NAS2CLASS
    Speichertyp: DEVCLASS
    Cloudtyp:
    Cloud-URL:
    Cloud-ID:
    Cloudposition:
    Geschätzte Kapazität: 0.0 M
    Speicherbereichsauslöser Ausl.:
    Auslastung in %: 0,0
    Umlagerung in %:
    Prozent logische Belegung: 0.0
    Obere Umlagerungsschwelle in %:
    Untere Umlagerungsschwelle in %:
    Umlagerungsverzögerung:
    Umlagerung fortsetzen:
    Umlagerungsprozesse:
    Wiederherstellungsprozesse:
    Nächster Speicherpool:
    Speicherpool wiederherstellen:
    Schwelle für maximale Größe:
    Zugriff: Read/Write
    Beschreibung:
    Überlaufstandort:
    Umgelagerte Dateien zwischenspeichern?:
    Zusammenfassen?: Group
    Wiederherstellungsschwelle:
    Grenzwert für Wiederh. ausgelag. Datenträger:
    Maximale Anzahl Arbeitsdatenträger: 50
    Anzahl verwendeter Arbeitsdatenträger: 0
    Verzögerungszeitraum für Containerwiederverwendung: 1 Tag(e)
    Wird Umlagerung ausgeführt?:
    Umgelagerte Datenmenge (MB):
    Abgelaufene Umlagerungszeit (Sek):
    Wird Wiederherstellung ausgeführt?:
    Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
    Datum/Zeit der letzten Aktualisierung: 01/02/2014 16:24:43
    Speicherpooldatenformat: NetApp Dump
    Kopienspeicherpool(s):
    Pool(s) für aktive Daten:
    Kopieren bei Fehler fortsetzen?: No
    CRC-Daten: No
    Wiederherstellungstyp:
    Daten nach Löschen überschreiben:
    Daten deduplizieren?: No
    Prozesse zum Identifizieren doppelter Daten:
    Komprimiert:
    Deduplizierungseinsparungen:
    Komprimierungseinsparungen:
    Eingesparter Gesamtspeicherbereich:
    Modus für automatisches Kopieren: Client
    Enthält vom Client deduplizierte Daten?: No
    Maximale Anzahl simultaner Writer:
Schutzprozesse:
    Schutzspeicherpool: Lokale
Speicherpools schützen:
    Grenzwert für Datenträgerwiederherstellung:
Datum des letzten Schutzes in fernem Pool:
    Datum des letzten Schutzes in lokalem Pool:
    Deduplizierung erfordert Sicherung?:
    Verschlüsselt:
    Prozent verschlüsselt:
    Zugeordneter Cloudspeicherbereich (MB):
    Belegter Cloudspeicherbereich (MB):
    Bucketname:
    Lokale geschätzte Kapazität:
    Lokale proz. Auslastung:
    Lokale logische Belegung in Prozent:
```

## Beispiel: Ausführliche Informationen zu einem Verzeichniscontainerspeicherpool anzeigen, der für die Dateneduplizierung verwendet wird

Zeigen Sie ausführliche Informationen zum Verzeichniscontainerspeicherpool DPOOL1 an. Für Felddesreibungen siehe Felddesreibungen.

query stgpool dpool1 format=detailed

```
Speicherpoolname: DPOOL1
  Speicherpooltyp: Primary
  Einheitenklassenname:
    Speichertyp: Verzeichnis
    Cloudtyp:
    Cloud-URL:
    Cloud-ID:
    Cloudposition:
  Geschätzte Kapazität: 798 G
  Speicherbereichsauslöser Ausl.:
    Auslastung in %: 3,4
    Umlagerung in %:
  Prozent logische Belegung: 100.0
  Obere Umlagerungsschwelle in %:
  Untere Umlagerungsschwelle in %:
  Umlagerungsverzögerung:
  Umlagerung fortsetzen:
  Umlagerungsprozesse:
  Wiederherstellungsprozesse:
  Nächster Speicherpool:
  Speicherpool wiederherstellen:
  Schwelle für maximale Größe: No Limit
  Zugriff: Read/Write
  Beschreibung:
  Überlaufstandort:
  Umgelagerte Dateien zwischenspeichern?:
  Zusammenfassen?:
  Wiederherstellungsschwelle:
  Grenzwert für Wiederh. ausgelag. Datenträger:
  Maximale Anzahl Arbeitsdatenträger:
  Anzahl verwendeter Arbeitsdatenträger:
  Verzögerungszeitraum für Containerwiederverwendung: 1 Tag(e)
  Wird Umlagerung ausgeführt?:
  Umgelagerte Datenmenge (MB):

  Abgelaufene Umlagerungszeit (Sek):
  Wird Wiederherstellung ausgeführt?:
  Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
  Datum/Zeit der letzten Aktualisierung: 01/02/2014 16:24:43
  Speicherpooldatenformat: Native
  Kopierspeicherpool(s):
  Pool(s) für aktive Daten:
  Kopieren bei Fehler fortsetzen?:
  CRC-Daten: No
  Wiederherstellungstyp:
  Daten nach Löschen überschreiben:
  Daten deduplizieren?: Yes
  Prozesse zum Identifizieren doppelter Daten:
  Komprimiert: Yes
  Belegter Speicherbereich für geschützte Daten: 1.599 M
  Anstehender Speicherbereich insgesamt: 100 M
  Deduplizierungseinsparungen: 1.331 M (67,56 %)
  Komprimierungseinsparungen: 194.805 K (29,82 %)
  Eingesparter Gesamt Speicherbereich: 1.521 M (77,22 %)
  Modus für automatisches Kopieren:
  Enthält vom Client deduplizierte Daten?:
  Maximale Anzahl simultaner Writer: No Limit

Schutzprozesse:
  Schutzspeicherpool: DPOOL2
  Speicherpools schützen:
  Grenzwert für Datenträgerwiederherstellung: Lokale

Datum des letzten Schutzes in fernem Pool:
  Datum des letzten Schutzes in lokalem Pool:
  Deduplizierung erfordert Sicherung?:
  Verschlüsselt:
  Prozent verschlüsselt: 34,56 %
  Zugeordneter Cloudspeicherbereich (MB):
  Belegter Cloudspeicherbereich (MB):
  Bucketname:
  Lokale geschätzte Kapazität:
  Lokale proz. Auslastung:
  Lokale logische Belegung in Prozent:
```

## Beispiel: Ausführliche Informationen zu einem Cloud-Containerspeicherpool anzeigen, der für die Datendeduplizierung verwendet wird

---

Zeigen Sie ausführliche Informationen zum Cloud-Containerspeicherpool CPOOL1 an. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query stgpool cpool1 format=detailed
```

```
Speicherpoolname: CPOOL1
  Speicherpooltyp: Primary
  Einheitenklassenname:
    Speichertyp: CLOUD
    Cloudtyp: SWIFT
    Cloud-URL: http://localhost.local
    Cloud-ID: Bailey
    Cloudposition: ONPREMISE
  Geschätzte Kapazität:
  Speicherbereichsauslöser Ausl.:
    Auslastung in %:
    Umlagerung in %:
      Prozent logische Belegung: 0.0
    Obere Umlagerungsschwelle in %:
    Untere Umlagerungsschwelle in %:
    Umlagerungsverzögerung:
    Umlagerung fortsetzen:
    Umlagerungsprozesse:
    Wiederherstellungsprozesse:
    Nächster Speicherpool:
  Speicherpool wiederherstellen:
    Schwelle für maximale Größe: No Limit
    Zugriff: Read/Write
    Beschreibung:
    Überlaufstandort:
  Umgelagerte Dateien zwischenspeichern?:
    Zusammenfassen?:
    Wiederherstellungsschwelle:
  Grenzwert für Wiederh. ausgelag. Datenträger:
    Maximale Anzahl Arbeitsdatenträger:
    Anzahl verwendeter Arbeitsdatenträger:
  Verzögerungszeitraum für die Wiederverwendung des Datenträgers: 1
    Wird Umlagerung ausgeführt?:
    Umgelagerte Datenmenge (MB):

  Abgelaufene Umlagerungszeit (Sek):
  Wird Wiederherstellung ausgeführt?:
  Letzte Aktualisierung durch (Administrator): CODY
  Datum/Zeit der letzten Aktualisierung: 2015-05-28, 10:47:52
  Speicherpooldatenformat: Native
  Kopienspeicherpool(s):
  Pool(s) für aktive Daten:
  Kopieren bei Fehler fortsetzen?:
    CRC-Daten: No
  Wiederherstellungstyp:
  Daten nach Löschen überschreiben:
  Daten deduplizieren?: Yes
  Prozesse zum Identifizieren doppelter Daten:
    Komprimiert: Yes
  Deduplizierungseinsparungen: 9.241 K (89,76 %)
  Komprimierungseinsparungen: 1.033 K (98,81 %)
  Eingesparter Gesamtspeicherbereich: 10.274 K (99,79 %)
  Modus für automatisches Kopieren:
  Enthält vom Client deduplizierte Daten?:
  Maximale Anzahl simultaner Writer: No Limit

Schutzprozesse:
  Schutzspeicherpool: Lokale
Speicherpools schützen:
  Grenzwert für Datenträgerwiederherstellung:

Datum des letzten Schutzes in fernem Pool:
  Datum des letzten Schutzes in lokalem Pool:
  Deduplizierung erfordert Sicherung?:
  Verschlüsselt: Yes
  Prozent verschlüsselt: 34,56 %
  Zugeordneter Cloudspeicherbereich (MB): 4.231
  Belegter Cloudspeicherbereich (MB): 4.231
  Bucketname:
  Lokale geschätzte Kapazität: 168 G
```

## Feldbeschreibungen

---

### Speicherpoolname

Der Name des Speicherpools.

### Speicherpooltyp

Der Typ des Speicherpools.

### Einheitenklassenname

Der Name der Einheitenklasse, die dem Speicherpool zugeordnet ist.

### Speichertyp

Der Typ des Speichers, der für den Speicherpool definiert ist. Die folgenden Speichertypen können angezeigt werden:

#### DEVCLASS

Der Speicherpool gibt eine Einheitenklasse an, die den Typ der Einheit bestimmt, auf der Daten gespeichert werden.

#### DIRECTORY

Der Speicherpool erstellt logische Container für Daten in Dateisystemverzeichnissen.

#### CLOUD

Der Speicherpool erstellt logische Container für Daten in einer Cloudumgebung.

### Cloudtyp

Für Cloudspeicherpools der Typ der Cloudplattform.

### Cloud-URL

Für Cloudspeicherpools die URL für den Zugriff auf die private On-Premises-Cloud oder die öffentliche Off-Premises-Cloud.

### Cloud-ID

Für Cloudspeicherpools die Benutzer-ID für den Zugriff auf die private On-Premises-Cloud oder die öffentliche Off-Premises-Cloud.

### Cloudposition

Gibt für Cloudspeicherpools an, ob die Cloud eine private On-Premises-Cloud oder eine öffentliche Off-Premises-Cloud ist.

### Geschätzte Kapazität

Die geschätzte Kapazität des Speicherpools in Megabyte (M) oder Gigabyte (G).

Bei Platteneinheiten (DISK) ist die geschätzte Kapazität die Kapazität aller Datenträger im Speicherpool, einschließlich der Datenträger, die abgehängt sind.

Für Speicherpools mit sequenziellem Zugriff ist die geschätzte Kapazität die Summe des geschätzten Speicherbereichs aller Datenträger mit sequenziellem Zugriff in dem Speicherpool, unabhängig von ihrem Zugriffsmodus. Mindestens ein Datenträger muss in einem Speicherpool mit sequenziellem Zugriff verwendet werden (entweder ein Arbeitsdatenträger oder ein privater Datenträger), um die geschätzte Kapazität zu berechnen.

Für Bändeinheiten und FILE-Einheiten schließt die geschätzte Kapazität für den Speicherpool die folgenden Faktoren ein:

- Die Kapazität aller Arbeitsdatenträger, die der Speicherpool bereits angefordert hat oder anfordern kann. Die Anzahl der Arbeitsdatenträger wird mit dem Parameter MAXSCRATCH im Befehl DEFINE STGPOOL oder UPDATE STGPOOL definiert.
- Die Gesamtzahl der verfügbaren Arbeitsdatenträger im Bandarchiv.
- Die geschätzte Kapazität ist der Wert von MAXSCRATCH bzw. die Gesamtzahl der verfügbaren Arbeitsdatenträger im Bandarchiv, je nachdem, welcher Wert kleiner ist.

Die Berechnungen der geschätzten Kapazität hängen von dem verfügbaren Speicherbereich für die Einheit ab, die dem Speicherpool zugeordnet ist. Für FILE-Speicherpools wird die Kapazität für den Speicherpool reduziert, wenn der verfügbare Speicher kleiner als der gesamte geschätzte Speicherbereich aller FILE-Datenträger in dem Speicherpool ist. Der für die Kapazität angezeigte Wert wird schrittweise um die Größe eines FILE-Datenträgers reduziert, während der verfügbare Speicherbereich weiter zurückgeht.

Für Centera stellt der Wert die Gesamtkapazität der Centera-Speichereinheit dar, die gerade abgefragt wird.

### Speicherbereichsauslöser Ausl.

Die Auslastung des Speicherpools, die vom Speicherbereichsauslöser (sofern vorhanden) für diesen Speicherpool berechnet wurde. Speicherbereichsauslöser können nur für Speicherpools definiert werden, die dem Einheitentyp DISK oder FILE zugeordnet sind.

Bei Einheiten mit sequenziellem Zugriff wird die Auslastung des Speicherbereichsauslösers als Prozentsatz der Anzahl der verwendeten Byte auf jedem Datenträger mit sequenziellem Zugriff in Relation zur Größe des Datenträgers und der geschätzten Kapazität aller vorhandenen Datenträger im Speicherpool ausgedrückt. Sie schließt keine potenziellen Arbeitsdatenträger ein. Im Gegensatz zur Berechnung der prozentualen Auslastung legt die Berechnung der Auslastung des Speicherbereichsauslösers den

Schwerpunkt auf die Erstellung neuer privater Dateidatenträger durch den Speicherbereichsauslöser über die Verwendung weiterer Arbeitsdatenträger.

Bei Platteneinheiten wird die Auslastung des Speicherbereichsauslösers als Prozentsatz der geschätzten Kapazität einschließlich Cachedaten ausgedrückt. Daten, die sich auf abgehängten Datenträgern befinden, werden jedoch ausgeschlossen. Der Wert für die Auslastung des Speicherbereichsauslösers kann höher als der Wert für die prozentuale Umlagerung sein, wenn Sie den Befehl QUERY STGPOOL ausgeben, während eine Dateierstellung ausgeführt wird. Der Wert für die Auslastung des Speicherbereichsauslösers wird durch den Umfang des Speicherbereichs bestimmt, der zugeordnet ist, während die Transaktion ausgeführt wird. Der Wert für die prozentuale Umlagerung stellt nur den Speicherbereich dar, der von festgeschriebenen Dateien belegt ist. Am Ende der Transaktion werden diese Werte synchronisiert.

Der Wert für die Auslastung des Speicherbereichsauslösers schließt Cachedaten auf Plattendatenträgern ein. Ist Caching aktiviert und findet eine Umlagerung statt, bleibt daher der Wert unverändert, da die umgelagerten Daten als Cachedaten auf dem Datenträger verbleiben. Der Wert verringert sich nur dann, wenn die Cachedaten verfallen oder wenn der Speicherbereich, der von Cachedateien belegt ist, für Dateien ohne Cachenutzung verwendet werden muss.

#### Auslastung in %

Die geschätzte Auslastung des Speicherpools als Prozentsatz.

Bei Einheiten mit sequenziellem Zugriff ist dieser Wert ein Prozentsatz der Anzahl der aktiven Byte auf jedem Datenträger mit sequenziellem Zugriff und der geschätzten Kapazität aller Datenträger im Speicherpool. Der Prozentsatz schließt die Anzahl potenzieller Arbeitsdatenträger ein, die möglicherweise zugeordnet sind.

Bei Platteneinheiten ist dieser Wert ein Prozentsatz der geschätzten Kapazität, einschließlich Cachedaten und Daten, die sich auf abgehängten Datenträgern befinden. Der Wert für Auslastung in % kann höher sein als der Wert für Umlagerung in %, wenn dieser Befehl ausgegeben wird, während eine Dateierstellungsoperation ausgeführt wird. Der Wert für Auslastung in % wird durch den Umfang des zugeordneten Speicherbereichs bestimmt, während die Transaktion ausgeführt wird. Der Wert für Umlagerung in % stellt nur den Speicherbereich dar, der von festgeschriebenen Dateien belegt ist. Am Ende der Transaktion werden diese Werte synchronisiert.

Der Wert für Auslastung in % schließt Cachedaten auf Plattendatenträgern ein. Ist Caching aktiviert und findet eine Umlagerung statt, bleibt daher der Wert für Auslastung in % unverändert, da die umgelagerten Daten als Cachedaten auf dem Datenträger verbleiben. Der Wert für Auslastung in % verringert sich nur dann, wenn die Cachedaten verfallen oder wenn der Speicherbereich, der von Cachedateien belegt ist, für Nicht-Cachedateien verwendet werden muss.

Für Centera ist dies eine Schätzung der Auslastung der gesamten Centera-Speichereinheit, nicht des gerade abgefragten Speicherpools.

#### Umlagerung in % (nur primäre Speicherpools)

Der geschätzte Prozentsatz der Daten im Speicherpool, die umgelagert werden können. Der Server verwendet diesen Wert sowie die obere und die untere Umlagerungsschwelle, um zu bestimmen, wann die Umlagerung gestartet und gestoppt werden soll.

Bei Platteneinheiten mit wahlfreiem Zugriff wird dieser Wert als Prozentsatz des Werts für die geschätzte Kapazität angegeben, einschließlich der Daten, die sich auf abgehängten Datenträgern befinden, jedoch ohne Cachedaten.

Bei Platteneinheiten mit sequenziellem Zugriff wird dieser Wert als Prozentsatz des Werts für die geschätzte Kapazität angegeben. Der Wert schließt die Kapazität aller für den Pool angegebenen Arbeitsdatenträger ein. Für andere Typen von Einheiten mit sequenziellem Zugriff ist dieser Wert der Prozentsatz der Gesamtzahl der Datenträger in dem Pool, die mindestens ein Byte aktiver Daten enthalten. Die Gesamtzahl der Datenträger schließt die maximale Anzahl Arbeitsdatenträger ein.

Der Wert für Auslastung in % schließt Cachedaten auf einem Datenträger ein; der Wert für Umlagerung in % schließt Cachedaten aus. Ist Caching aktiviert und findet eine Umlagerung statt, verringert sich daher der Wert für Umlagerung in %, der Wert für Auslastung in % bleibt jedoch unverändert, da die umgelagerten Daten als Cachedaten auf dem Datenträger verbleiben. Der Wert für Auslastung in % verringert sich nur dann, wenn die Cachedaten verfallen oder wenn der Speicherbereich, der von Cachedateien belegt ist, für Nicht-Cachedateien verwendet werden muss.

#### Prozent logische Belegung

Die logische Belegung des Speicherpools als Prozentsatz der Gesamtbelegung. Die logische Belegung ist der Speicherbereich, der von Clientdateien belegt ist, die Teil oder kein Teil eines Aggregats sein können. Ein Wert für Prozent logische Belegung, der kleiner als 100 % ist, gibt an, dass innerhalb von Aggregaten in dem Speicherpool freier Speicherbereich verfügbar ist.

#### Obere Umlagerungsschwelle in % (nur primäre Speicherpools)

Die obere Umlagerungsschwelle, die angibt, wann der Server mit der Umlagerung für den Speicherpool beginnen kann. Der Server startet Umlagerungsprozesse, wenn die Kapazitätsnutzung diesen Schwellenwert erreicht.

#### Untere Umlagerungsschwelle in % (nur primäre Speicherpools)

Die untere Umlagerungsschwelle, die angibt, wann der Server die Umlagerung für den Speicherpool stoppen kann. Der Server stoppt Umlagerungsprozesse, wenn die Kapazitätsnutzung diesen Schwellenwert erreicht.

#### Umlagerungsverzögerung (nur primäre Speicherpools)

Die Mindestanzahl Tage, die eine Datei in einem Speicherpool verbleiben muß, bevor der Server die Datei in den nächsten Speicherpool umlagern kann. Bei einem Plattenspeicherpool werden die Tage ab dem Zeitpunkt gezählt, zu dem die Datei in dem Speicherpool gespeichert oder von einem Client zuletzt abgerufen wurde. Bei einem Speicherpool mit sequenziellem Zugriff werden die Tage ab dem Zeitpunkt gezählt, zu dem die Datei in dem Speicherpool gespeichert wurde.

Umlagerung fortsetzen (nur primäre Speicherpools)

Angabe, ob der Server die Umlagerung von Dateien in den nächsten Speicherpool auch dann fortsetzt, wenn die Dateien für die Anzahl der Tage, die durch die Umlagerungsverzögerung angegeben werden, nicht in dem Pool waren.

Umlagerungsprozesse

Die Anzahl paralleler Prozesse, die zum Umlagern von Dateien aus einem primären Speicherpool mit wahlfreiem oder sequenziellem Zugriff verwendet werden.

Wiederherstellungsprozesse

Die Anzahl paralleler Prozesse, die zum Wiederherstellen der Datenträger in einem primären Speicherpool mit sequenziellem Zugriff oder Kopierspeicherpool verwendet werden.

Nächster Speicherpool (nur primäre Speicherpools)

Der Speicherpool, der der Zielort für Daten ist, die aus diesem Speicherpool umgelagert werden.

Speicherpool wiederherstellen (nur primäre Speicherpools mit sequenziellem Zugriff)

Falls angegeben, der Speicherpool, der der Zielort für Daten ist, die von Datenträgern während der Wiederherstellungsverarbeitung versetzt werden. Wird kein Pool angegeben, werden bei der Wiederherstellungsverarbeitung standardmäßig Daten nur zwischen Datenträgern innerhalb desselben Speicherpools versetzt.

Schwelle für maximale Größe (nur primäre Speicherpools)

Die maximale Größe von Dateien, die in dem Speicherpool gespeichert werden kann.

Zugriff

Der Zugriffsmodus für Daten in dem Speicherpool. Die folgenden Zugriffsmodi sind gültig:

Lesen/Schreiben

Auf die Daten kann im Modus 'Schreib-/Lesezugriff' zugegriffen werden.

Schreibgeschützt

Auf die Daten kann im Lesezugriffsmodus zugegriffen werden.

Wird konvertiert

Der Speicherpool wird gerade in einen Verzeichniscontainerspeicherpool konvertiert.

Konvertierung gestoppt

Der Prozess der Konvertierung des Speicherpools in einen Verzeichniscontainerspeicherpool wurde gestoppt.

Bereinigung für Konvertierung erforderlich

Um den Speicherpool erfolgreich zu konvertieren, müssen Sie den Speicherpool bereinigen. Die Konvertierung wurde aufgrund von beschädigten Daten nicht abgeschlossen. Geben Sie den Befehl QUERY CLEANUP aus, um beschädigte Dateien zu identifizieren.

Konvertiert

Der Speicherpool wurde in einen Verzeichniscontainerspeicherpool konvertiert.

Beschreibung

Die Beschreibung des Speicherpools.

Überlaufstandort (nur Speicherpools mit sequenziellem Zugriff)

Der Standort, an dem Datenträger in dem Speicherpool gespeichert werden, wenn sie mit dem Befehl MOVE MEDIA aus einem automatisierten Speicherarchiv ausgegeben werden.

Umgelagerte Dateien zwischenspeichern? (nur Speicherpools mit wahlfreiem Zugriff)

Angabe, ob Caching für Dateien aktiviert ist, die in den nächsten Speicherpool umgelagert werden.

Zusammenfassen? (nur Speicherpools mit sequenziellem Zugriff)

Angabe, ob die Kollokation inaktiviert oder aktiviert ist. Ist die Kollokation inaktiviert, lautet der Wert dieses Felds No. Ist die Kollokation aktiviert, lauten die gültigen Werte Group, Node und File space.

Wiederherstellungsschwelle (nur Speicherpools mit sequenziellem Zugriff)

Die Schwelle, die bestimmt, wann Datenträger in einem Speicherpool wiederhergestellt werden. Der Server vergleicht den Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger mit diesem Wert, um festzustellen, ob eine Wiederherstellung erforderlich ist.

Grenzwert für Wiederh. ausgelag. Datenträger

Die Anzahl der ausgelagerten Datenträger, deren Speicherbereich während der Wiederherstellung für diesen Speicherpool wiederhergestellt wird. Dieses Feld gilt nur bei POOLTYPE=COPY.

Maximale Anzahl Arbeitsdatenträger (nur Speicherpools mit sequenziellem Zugriff)

Die maximale Anzahl der Arbeitsdatenträger, die der Server für den Speicherpool anfordern kann.

Anzahl verwendeter Arbeitsdatenträger (nur Speicherpools mit sequenziellem Zugriff)

Die Anzahl der Arbeitsdatenträger, die in dem Speicherpool verwendet werden.

Verzögerungszeitraum für Containerwiederverwendung (nur Containerspeicherpools)

Die Anzahl Tage, die nach dem Löschen aller Dateien aus dem Container verstreichen müssen, bevor der Container vom Server wiederverwendet wird.

Wird Umlagerung ausgeführt? (nur primäre Speicherpools)

Angabe, ob mindestens ein Umlagerungsprozess für den Speicherpool aktiv ist.

#### Umgelagerte Datenmenge (MB) (nur primäre Speicherpools)

Das Datenvolumen in Megabyte, das umgelagert wird, wenn die Umlagerung aktiv ist. Ist die Umlagerung nicht aktiv, gibt dieser Wert die bei der letzten Umlagerung umgelagerte Datenmenge an. Werden für den Speicherpool mehrere gleichzeitig stattfindende Umlagerungsprozesse verwendet, gibt dieser Wert das von allen Prozessen umgelagerte Gesamtvolumen der Daten an.

#### Abgelaufene Umlagerungszeit (Sekunden) (nur primäre Speicherpools)

Die Zeit, die seit Beginn der Umlagerung vergangen ist, wenn die Umlagerung aktiv ist. Ist die Umlagerung nicht aktiv, gibt dieser Wert die Zeit an, die für die Ausführung der letzten Umlagerung erforderlich ist. Werden für den Speicherpool mehrere gleichzeitig stattfindende Umlagerungsprozesse verwendet, gibt dieser Wert den von allen Prozessen benötigten Gesamtzeitaufwand an (vom Anfang des ersten bis zum Abschluß des letzten Prozesses).

#### Wird Wiederherstellung ausgeführt? (nur Speicherpools mit sequenziellem Zugriff)

Angabe, ob für den Speicherpool ein Wiederherstellungsprozess aktiv ist.

#### Letzte Aktualisierung durch (Administrator)

Der Name des Administrators, der den Speicherpool definiert bzw. zuletzt aktualisiert hat.

#### Datum/Zeit der letzten Aktualisierung

Das Datum und die Uhrzeit, an dem bzw. zu der ein Administrator den Speicherpool definiert oder zuletzt aktualisiert hat.

#### Speicherpooldatenformat

Der Typ des Datenformats, der zum Schreiben von Daten in diesen Speicherpool verwendet wird (beispielsweise NATIVE, NETAPPDUMP, CELERRADUMP oder NDMPDUMP).

#### Kopierspeicherpool(s)

In die aufgelisteten Kopierspeicherpools werden zu demselben Zeitpunkt Daten geschrieben, zu dem Daten in dem primären Speicherpool gesichert oder archiviert werden, der mit diesem Befehl abgefragt wird.

#### Pool(s) für aktive Daten

In die hier aufgelisteten Pools für aktive Daten werden zu demselben Zeitpunkt Daten geschrieben, zu dem Daten in dem primären Speicherpool gesichert werden, der mit diesem Befehl abgefragt wird.

#### Kopieren bei Fehler fortsetzen?

Gibt an, ob ein Server das Schreiben von Daten in andere Kopierspeicherpools in der Liste fortsetzt oder die gesamte Transaktion beendet, wenn bei einem der Kopienpools in der Liste ein Schreibfehler auftritt. Dieses Feld gilt nur für primäre Speicherpools mit wahlfreiem Zugriff und für primäre Speicherpools mit sequenziellem Zugriff.

#### CRC-Daten

Gibt an, ob Daten durch eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) ausgewertet werden, wenn Daten während des Speicherns und Abrufens auf einer Einheit übertragen werden.

#### Wiederherstellungstyp

Gibt an, ob Datenträger in diesem Speicherpool nach Schwellenwert (threshold) oder nach SnapLock-Aufbewahrungsdauer wiederhergestellt werden.

#### Daten nach Löschen überschreiben

Gibt an, wie oft Daten physisch überschrieben werden, nachdem sie aus der Datenbank gelöscht wurden.

#### Daten deduplizieren?

Angabe, ob Daten in dem Speicherpool dedupliziert werden.

#### Prozesse zum Identifizieren doppelter Daten

Die Anzahl der Prozesse zum Identifizieren doppelter Daten, die als Standardwert für den Speicherpool angegeben wurde. Die in diesem Feld angegebene Anzahl der Prozesse zum Identifizieren doppelter Daten ist möglicherweise nicht gleich der Anzahl der Prozesse zum Identifizieren doppelter Daten, die ausgeführt werden.

#### Komprimiert

Angabe, ob der Speicherpool komprimiert ist.

#### Zusätzlicher Speicherbereich für geschützte Daten

Der Umfang des Speicherbereichs in MB, der zum Schützen von Daten ferner Server verwendet wird. Dies ist der Gesamtumfang des Speicherbereichs, der für Daten verwendet wird, die von anderen Servern als Ergebnis der Ausführung des Befehls PROTECT STGPOOL empfangen werden.

Nach der Ausführung des Befehls PROTECT STGPOOL sind die Daten nicht einem Knoten zugeordnet. Wenn Sie jedoch die Knotenreplikation auf einigen oder allen Knoten ausführen, werden die Daten den Knoten zugeordnet und sind nicht mehr dem zusätzlichen Speicherbereich für geschützte Daten zugeordnet.

Wenn Sie keine Knotenreplikation ausführen, bleiben die empfangenen Daten (nach der Ausführung des Befehls PROTECT STGPOOL) dem zusätzlichen Speicherbereich für geschützte Daten zugeordnet.

#### Nicht belegter anstehender Speicherbereich insgesamt

Der Umfang des Speicherbereichs, der zu einem geplanten Zeitpunkt in einem Verzeichniscontainerspeicherpool verfügbar wird. Der Speicherbereich wird von deduplizierten Datenbereichen belegt, die aus dem Speicherpool entfernt werden, wenn der über den Parameter REUSEDELAY im Befehl DEFINE STGPOOL festgelegte Zeitraum abläuft.

#### Deduplizierungseinsparungen

Der Umfang und Prozentsatz der Daten, der im Speicherpool mithilfe der Dateneduplizierung eingespart wird.

#### Komprimierungseinsparungen

Das Datenvolumen, das im Speicherpool durch die Komprimierung eingespart wird.



#### Eingesparter Gesamtspeicherbereich

Das Gesamtdatenvolumen, das im Speicherpool eingespart wurde.

#### Modus für automatisches Kopieren

Gibt an, ob Daten während der Ausführung von Clientspeichersitzungen, Serverimportprozessen, Serverdatenumlagerungsprozessen oder aller drei Operationen gleichzeitig in Kopierspeicherpools oder Pools für aktive Daten geschrieben werden. Der Wert CLIENT gibt entweder Clientspeicheroperationen oder Serverimportoperationen an. Der Wert ALL gibt an, dass Operationen mit simultanem Schreiben immer dann ausgeführt werden, wenn dieser Pool ein Ziel für eine der auswählbaren Operationen ist.

Ist der Speicherpool ein Kopierspeicherpool oder ein Pool für aktive Daten oder ist die Funktion für simultanes Schreiben inaktiviert, ist dieses Feld leer.

#### Enthält vom Client deduplizierte Daten?

Gibt an, ob der Speicherpool Daten enthält, die von Clients dedupliziert wurden. Auf Speicherpools, die von Clients deduplizierte Daten enthalten, kann von Speicheragenten mit Version 6.1 oder einer früheren Version nicht für die LAN-unabhängige Datenversetzung zugegriffen werden.

Tipp: Dieses Feld ist für Containerspeicherpools leer. Sie können keine Containerspeicherpools für die LAN-unabhängige Datenversetzung verwenden.

#### Maximale Anzahl simultaner Writer

Die maximale Anzahl der Ein-/Ausgaben, die gleichzeitig für den Speicherpool ausgeführt werden können.

#### Schutzprozesse

Die Anzahl der Schutzprozesse.

#### Schutzspeicherpool

Der Name des Containerspeicherpools, in dem die Daten auf dem Zielreplikationsserver geschützt werden.

#### Lokale Speicherpools schützen

Gibt an, ob lokale Speicherpools geschützt werden.

#### Grenzwert für Datenträgerwiederherstellung

Gibt bei Containerkopierspeicherpools die maximale Anzahl der Datenträger an, die der Server während des Speicherpoolschutzes wiederherstellt.

#### Datum des letzten Schutzes in fernem Pool

Das Datum, an dem der Speicherpool zuletzt in einem Speicherpool auf einem fernen Server geschützt wurde.

#### Datum des letzten Schutzes in lokalem Pool

Das Datum, an dem der Speicherpool zuletzt in einem Speicherpool auf dem lokalen Server geschützt wurde.

#### Deduplizierung erfordert Sicherung?

Gibt an, ob der sequenzielle Speicherpool gesichert werden muss, wenn der Speicherpool deduplizierte Daten enthält.

#### Verschlüsselt

Gibt für Verzeichniscontainerspeicherpools oder Cloud-Containerspeicherpools an, ob Clientdaten verschlüsselt werden, bevor sie in den Speicherpool geschrieben werden.

#### Prozent verschlüsselt

Der Prozentsatz der deduplizierten Clientdaten, die im Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool verschlüsselt sind.

#### Zugeordneter Cloudspeicherbereich (MB)

Bei Cloudspeicherpools der Umfang des Speicherbereichs in Megabyte, der dem Cloudspeicher zugeordnet ist.

#### Belegter Cloudspeicherbereich (MB)

Bei Cloudspeicherpools der Speicherbereich, der vom Cloudspeicher belegt wird, angegeben in Megabyte.

#### Bucketname

Bei Cloudspeicherpools, die Simple Storage Service (S3) verwenden, der Name, den IBM Spectrum Protect dem S3-Bucket oder der IBM® Cloud Object Storage-Vault zuordnet. Dieser Wert kann auch der Name sein, den Sie dem Bucket mit dem Parameter BUCKETNAME im Befehl DEFINE STGPOOL oder UPDATE STGPOOL zugeordnet haben.

#### Lokale geschätzte Kapazität

Bei Cloudspeicherpools, die lokalen Speicher verwenden, die geschätzte Kapazität des lokalen Speichers in Megabyte (M) oder Gigabyte (G).

#### Lokale proz. Auslastung

Bei Cloudspeicherpools, die lokalen Speicher verwenden, die geschätzte Auslastung der lokalen Speicherkomponente des Cloudspeicherpools als Prozentsatz.




#### Lokale logische Belegung in Prozent

Bei Cloudspeicherpools, die lokalen Speicher verwenden, die logische Belegung des Cloudspeicherpools als Prozentsatz der Gesamtbelegung. Die logische Belegung ist der Speicherbereich, der von Clientdateien belegt ist, die Teil oder kein Teil eines Aggregats sein können. Ein Wert für Lokale logische Belegung in Prozent, der kleiner als 100 % ist, gibt an, dass innerhalb von Aggregaten in dem Cloudspeicherpool freier Speicherbereich verfügbar ist.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY STGPOOL

| Befehl                 | Beschreibung   |
|------------------------|--|
| CONVERT STGPOOL        | Konvertiert einen Speicherpool in einen Verzeichniscontainerspeicherpool.          |
| COPY ACTIVATEDATA      | Kopiert aktive Sicherungsdaten.  |
| DEFINE STGPOOL         | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern. |
| DELETE STGPOOL         | Löscht einen Speicherpool aus dem Serverspeicher.                                  |
| QUERY STGPOOLDIRECTORY | Zeigt Informationen zu Speicherpoolverzeichnissen an.                              |
| UPDATE STGPOOL         | Ändert die Attribute eines Speicherpools.  |

## QUERY STGPOOLDIRECTORY (Speicherpoolverzeichnis abfragen)

Mit diesem Befehl können Informationen zu einem oder zu mehreren Speicherpoolverzeichnissen angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

>>-Query STGPOOLDIrectory-+-----+----->
                          .-*-----
                          '-Verzeichnis-'

                          .-ACcEss---Any-----
>+-----+-----+-----+----->
  '-STGpool----Poolname-' '-ACcEss---+READWrite---+'
                               +-READOnly----+
                               +-DEStroyed---+
                               +-Any-----+
                               '-UNAVailable-'

.-Format----Standard----.
>+-----+-----+-----><
  '-Format----+Standard-+'
                    '-Detailed-'

```

### Parameter

#### Verzeichnis

Gibt das Speicherpoolverzeichnis an, das abgefragt werden soll. Dieser Parameter ist wahlfrei.

\*

Gibt an, dass ein Stern (\*) ein Platzhalterzeichen darstellt. Verwenden Sie Platzhalterzeichen, wie z. B. einen Stern, für die Übereinstimmung mit beliebigen Zeichen. Alternativ können Sie ein Fragezeichen (?) oder ein Prozentzeichen (%) verwenden, die exakt einem Zeichen entsprechen. Dies ist der Standardwert.

#### Verzeichnis

Gibt das Speicherpoolverzeichnis an. Wird kein Wert für diesen Parameter angegeben, werden alle Speicherpoolverzeichnisse angezeigt. Die maximale Länge des Speicherpoolverzeichnisses beträgt 1024 Zeichen.

#### STGpool

Gibt den Namen des Speicherpools an, der abgefragt werden soll. Wird kein Wert für diesen Parameter angegeben, werden alle Speicherpoolverzeichnisse angezeigt. Die maximale Länge des Speicherpoolnamens beträgt 30 Zeichen. Dieser Parameter ist wahlfrei.

#### Access

Gibt an, dass die Ausgabe durch den Verzeichniszugriffsmodus eingeschränkt wird. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

##### READWrite

Alle Speicherpoolverzeichnisse mit dem Zugriffsmodus `READWRITE` anzeigen.

##### READOnly

Alle Speicherpoolverzeichnisse mit dem Zugriffsmodus `READONLY` anzeigen.

##### DESTroyed

Alle Speicherpoolverzeichnisse mit dem Zugriffsmodus `DESTROYED` anzeigen. Die Verzeichnisse sind im Speicherpoolverzeichnis als dauerhaft beschädigt gekennzeichnet.

##### Any

Alle Speicherpoolverzeichnisse anzeigen. Dies ist der Standardwert.

##### UNAVailable

Verzeichnisse mit dem Zugriffsmodus `UNAVAILABLE` anzeigen.

#### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist `STANDARD`. Sie können einen der folgenden Werte angeben:

##### Standard

Gibt an, dass Teilinformationen angezeigt werden.

##### Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

## Beispiel: Übersichtsdaten zu einem bestimmten Speicherpoolverzeichnis anzeigen

---

Informationen zu dem Speicherpoolverzeichnis mit dem Namen `DPOOL` anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query stgpooldirectory C:\data
```

| Speicher-<br>poolname | Verzeichnis | Zugriff    |
|-----------------------|-------------|------------|
| -----                 | -----       | -----      |
| DPOOL                 | C:\data     | Read/Write |

## Beispiel: Ausführliche Informationen zum Speicherpoolverzeichnis anzeigen

---

Ausführliche Informationen zu dem Speicherpoolverzeichnis mit dem Namen `DPOOL` anzeigen.

```
query stgpooldirectory stgpool=dpool format=detailed
```

```
Speicherpoolname: DPOOL
                  Verzeichnis: /storage/sampleDir
                  Zugriff: Read/Write
Freier Speicherbereich (MB): 323.170
GesamtSpeicherbereich (MB): 476.938
Dateisystem: /storage
Absoluter Pfad: /storage/data
```




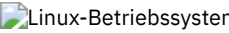
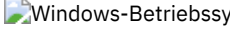



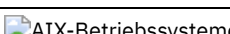
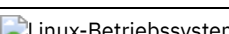
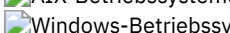
```
Speicherpoolname: DPOOL
                  Verzeichnis: /storage2/sampleDir
                  Zugriff: Read/Write
Freier Speicherbereich (MB): 323.170
GesamtSpeicherbereich (MB): 476.938
Dateisystem: /storage
Absoluter Pfad: /storage2/sampleDir
```

## Feldbeschreibungen

---

- Speicherpoolname**  
Der Name des Speicherpools.
- Verzeichnis**  
Der Name des Speicherpoolverzeichnisses.
- Zugriff**  
Der Zugriffsmodus der Daten in dem Speicherpoolverzeichnis.
- Freier Speicherbereich (MB)**  
Der Speicherbereich im Speicherpoolverzeichnis in Megabyte, der nicht verwendet wird.
- Gesamtspeicherbereich (MB)**  
Der Gesamtspeicherbereich im Speicherpoolverzeichnis in Megabyte.
- Dateisystem**  
Der Name des Dateisystems, in dem sich das Speicherpoolverzeichnis befindet.
- Absoluter Pfad**  
Der Name des absoluten Pfads, in dem sich das Speicherpoolverzeichnis befindet. Der absolute Pfadname enthält den Namen des Stammverzeichnisses und alle Unterverzeichnisse im Pfadnamen. Alle symbolischen Verbindungen werden in den absoluten Pfadnamen aufgelöst.

Tabelle 1. Zugehörige Befehle für QUERY STGPOOLDIRECTORY

| Befehl   | Beschreibung  |
|--|---|
| DEFINE STGPOOL   | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.                      |
|  <br> DEFINE STGPOOLDIRECTORY       | Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool. |
|  <br> DELETE STGPOOLDIRECTORY      | Löscht ein Speicherpoolverzeichnis aus einem Verzeichniscontainer- oder Cloud-Containerspeicherpool.    |
|  <br> UPDATE STGPOOLDIRECTORY | Ändert die Attribute eines Speicherpoolverzeichnisses.  |

## QUERY STGRULE (Speicherregelinformationen anzeigen)

Verwenden Sie diesen Befehl, um Informationen zum Typ der Speicherregel anzuzeigen, die für einen Speicherpool definiert ist.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

.*----- .-Format----Standard----.
>>-Query STGRULE-----+----->
      '-RegelName-' '-Format----+Standard-+-'
                          '-Detailed-'

.-ACTiontype----ANY----- .-ACTIVE----ANY-----.
>-----+-----+-----<
      '-ACTiontype----+ANY-+-' '-ACTIVE----+ANY-+-'
                          '-TIER-'           +-Yes-+
                                          '-No--'

```

### Parameter

- Regelname**  
Gibt den Namen der Speicherregel an. Dieser Parameter ist wahlfrei. Dieser Name kann mithilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Speicherregeln angezeigt. Die maximale Länge des Namens beträgt 30 Zeichen.
- Format**

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Die folgenden Werte sind gültig:

Standard

Gibt an, dass Teilinformationen angezeigt werden.

Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

ACTiontype

Gibt die Speicheraktion an, die von den Speicherregeln ausgeführt wird. Die folgenden Werte sind gültig:

ANY

Alle Typen von Speicherregeln werden angezeigt.

TIER

Speicherregeln für Tiering werden angezeigt.

ACTIVE

Gibt an, dass aktive Speicherregeln angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Die folgenden Werte sind gültig:

ANY

Gibt an, dass alle Speicherregeln angezeigt werden.

YES

Gibt an, dass nur aktive Speicherregeln angezeigt werden.

NO

Gibt an, dass nur inaktive Speicherregeln angezeigt werden.

## Beispiel: Alle Speicherregeln für alle Speicherpools auflisten

---

Alle Speicherregeln für alle Speicherpools abfragen. Für Feldbeschreibungen siehe QUERY STGRULE (Speicherregelinformationen anzeigen).

```
query stgrule
```

| Speicherregelname | Zielspeicherpool | Aktionstyp | Aktiv | Quellenspeicherpools |
|-------------------|------------------|------------|-------|----------------------|
| STGACTION1        | CLOUD            | Tier       | Yes   | DIRPOOL1             |

## Beispiel: Ausführliche Informationen zu einer Speicherregel anzeigen

---

Ausführliche Speicherregelinformationen für einen Speicherpool abfragen. Die Ausgabe soll im ausführlichen Format erstellt werden. Für Feldbeschreibungen siehe QUERY STGRULE (Speicherregelinformationen anzeigen).

```
query stgrule format=detailed
```

```
Speicherregelname: STGACTION1
  Zielspeicherpool: CLOUD
    Aktionstyp: Tier
      Aktiv: Yes
Maximale Anzahl Prozesse: 8
  Startzeit: 15:00:00
Tier-Verzögerung (Tage): 30
  Dauer:
    Beschreibung: Storage rule to tier data
  Quellenspeicherpools: DIRPOOL1
```

## Feldbeschreibungen

---

Speicherregelname

Der Name der Speicherregel.

Zielspeicherpool

Der Name des Cloud-Containerspeicherpools.

Aktionstyp

Der Typ der Speicherregel.

Aktiv

Angabe, ob die Speicherregel aktiv oder inaktiv ist.

Maximale Anzahl Prozesse

Die maximale Anzahl Prozesse pro Quellenspeicherpool.

#### Startzeit

Die tägliche Startzeit des Fensters, zu der die Speicherregel ausgeführt wird.

#### Tier-Verzögerung (Tage)

Die Mindestanzahl Tage, die das Objekt in einem Quellenspeicherpool verbleiben muss, bevor die Speicherregel das Objekt in den Zielspeicherpool versetzt.

#### Dauer

Die Anzahl Minuten, die die Speicherregel die Daten verarbeitet, wenn alle zugeordneten Prozesse abgeschlossen sind. Kein Wert gibt an, dass die Verarbeitung bis zur Beendigung fortgesetzt wird.

#### Beschreibung

Eine Beschreibung der Speicherregel.

#### Quellenspeicherpools

Der Name der Speicherpools, aus denen die Speicherregel Objekte versetzt.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY STGRULE

| Befehl         | Beschreibung                                       |
|----------------|--|
| DEFINE STGRULE | Definiert eine Speicherregel für Speicherpools.    |
| DELETE STGRULE | Löscht Speicherregeln für Speicherpools.           |
| UPDATE STGRULE | Aktualisiert eine Speicherregel für Speicherpools. |

## QUERY SUBSCRIBER (Informationen zu Subskribenten anzeigen)

Mit diesem Befehl können auf einem Konfigurationsmanager Informationen über Subskribenten und ihre Profilsubskriptionen angezeigt werden.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
..*-----.  
>>-Query SUBSCRIBer--+----->  
      '-Servername-'  
  
.-PROFIle---*-----.  
>--+-----><  
      '-PROFIle---Profilname-'
```

## Parameter

#### Servername

Gibt den Namen eines verwalteten Servers an, für den Subskriptionsinformationen angezeigt werden sollen. Es können Platzhalterzeichen verwendet werden, um mehrere Server-Namen anzugeben. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle verwalteten Server.

#### PROFIle

Gibt einen Profilnamen an, für den Informationen angezeigt werden sollen. Es können Platzhalterzeichen verwendet werden, um mehrere Profilnamen anzugeben. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Profile.

## Beispiel: Die Profilsubskriptionen eines Konfigurationsmanagers auflisten

Subskribenteninformationen für alle Profilsubskriptionen für diesen Konfigurationsmanager anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query subscriber
```

```
Subskribent      Profilname      Aktuell?      Datum/Zeit der  
-----      -  
SERVER2         DEFAULT_PROFILE  Yes           Thu, May 14, 1998  
                                         01:14:42 PM
```

## Feldbeschreibungen

### Subskribent

Der Name des Subskribenten (verwalteter Server).

### Profilname

Der Name des Profils.

### Aktuell?

Angabe, ob die Subskription mit den aktuellen Informationen, die dem Profil zugeordnet sind, aktualisiert wurde. Gültige Werte:

#### Yes

Der verwaltete Server ist auf dem aktuellen Stand.

#### No

Der verwaltete Server ist nicht auf dem aktuellen Stand. Enthält dieses Feld den Wert NO, nachdem das Profil aktualisiert wurde, die Servernachrichten auf Fehlerbedingungen überprüfen, die möglicherweise das Fehlschlagen der Aktualisierung verursacht haben.

#### Unknown

Entweder verfügt der verwaltete Server über eine neuere Version des Profils als der Konfigurationsmanager oder das Profil ist nicht mehr auf dem Konfigurationsmanager vorhanden, die Subskription ist jedoch noch dem Profil zugeordnet.

### Datum/Zeit der letzten Aktualisierung

Gibt das Datum und die Uhrzeit an, an dem bzw. zu der die Konfigurationsdaten für die Subskription erfolgreich an den Subskribenten verteilt wurden.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SUBSCRIBER

| Befehl              | Beschreibung   |
|---------------------|--|
| DEFINE SUBSCRIPTION | Subskribiert einen verwalteten Server für ein Profil.                            |
| DELETE SUBSCRIBER   | Löscht veraltete Subskriptionen verwalteter Server.                              |
| DELETE SUBSCRIPTION | Löscht eine angegebene Profilsubskription.                                       |
| NOTIFY SUBSCRIBERS  | Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin. |
| SET CONFIGMANAGER   | Gibt an, ob ein Server ein Konfigurationsmanager ist.                            |
| QUERY SUBSCRIPTION  | Zeigt Informationen über Profilsubskriptionen an.                                |

## QUERY SUBSCRIPTION (Subskriptionsinformationen anzeigen)

Mit diesem Befehl können auf einem verwalteten Server Profilsubskriptionsinformationen angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query SUBSCRIPTION--*-----<
                        +-----+
                        |'-Profilname-'|
```

### Parameter

#### Profilname

Gibt den Namen des Profils an, für das Subskriptionsinformationen angezeigt werden. Es können Platzhalterzeichen verwendet werden, um mehrere Namen anzugeben. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Profile.

### Beispiel: Subskriptionsinformationen anzeigen

Subskriptionsinformationen für alle Profile anzeigen.

```
query subscription
```

| Konfigurations-<br>manager | Profilname | Datum/Zeit der<br>letzten Aktualisierung |          |                                      |
|----------------------------|------------|--|----------|--------------------------------------|
| SERVER1                    | ADMIN_INFO | Thu, May 14, 1998<br>01:35:13 PM         | SERVER1  | DEFAULT_PROFILE Thu, May<br>14, 1998 |
|                            |            | 01:35:13 PM                              | EMPLOYEE | Thu, May<br>14, 1998                 |
|                            |            | 01:35:13 PM                              |          |                                      |

## Feldbeschreibungen

Konfigurationsmanager

Der Name des Konfigurationsmanagers.

Profilname

Der Name des Profils.

Datum/Zeit der letzten Aktualisierung

Das Datum und die Uhrzeit, an dem bzw. zu der die neuesten Konfigurationsdaten erfolgreich an den Subskribenten verteilt wurden.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SUBSCRIPTION

| Befehl              | Beschreibung   |
|---------------------|--|
| DEFINE SUBSCRIPTION | Subskribiert einen verwalteten Server für ein Profil.                            |
| DELETE SUBSCRIBER   | Löscht veraltete Subskriptionen verwalteter Server.                              |
| DELETE SUBSCRIPTION | Löscht eine angegebene Profilsubskription.                                       |
| NOTIFY SUBSCRIBERS  | Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin. |
| QUERY SUBSCRIBER    | Zeigt Informationen über Subskribenten und ihre Subskriptionen für Profile an.   |

## QUERY SYSTEM (Systemkonfiguration und Kapazität abfragen)

Mit diesem Befehl können konsolidierte Informationen zur Konfiguration und Kapazität des Servers abgerufen werden.

Dieser Befehl konsolidiert die Ausgabe aus Anweisungen SELECT, Befehlen SHOW und anderen IBM Spectrum Protect-Befehlen. Die Ausgabe wird von mehreren IBM Spectrum Protect-Befehlen generiert, wie z. B.:

- QUERY ASSOCIATION
- QUERY COPYGROUP
- QUERY DATAMOVER
- QUERY DB
- QUERY DBSPACE
- QUERY DEVCLASS
- QUERY DIRSPACE
- QUERY DOMAIN
- QUERY LIBRARY
- QUERY LOG
- QUERY MGMTCLASS
- QUERY OPTION
- QUERY PROCESS
- QUERY REPLRULE
- QUERY SCHEDULE
- QUERY SERVER
- QUERY SESSION
- QUERY STATUS
- QUERY STGPOOL
- QUERY VOLHISTORY



- QUERY VOLUME

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-Query SYStem-----><
```

## Beispiel: Konsolidierte Systeminformationen anzeigen

Den Befehl QUERY SYSTEM ausgeben, um konsolidierte Systeminformationen abzurufen. Beispielausgabedaten für diese Abfragebefehle befinden sich in den Erläuterungen zum jeweiligen Befehl.

```
query system
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SYSTEM

| Befehl            | Beschreibung   |
|-------------------|--|
| QUERY ASSOCIATION | Zeigt die Clients an, die einem oder mehreren Zeitplänen zugeordnet sind.  |
| QUERY COPYGROUP   | Zeigt die Attribute einer Kopiengruppe an.   |
| QUERY DB          | Zeigt Zuordnungsinformationen zu der Datenbank an.   |
| QUERY DBSPACE     | Zeigt Informationen zum Speicherplatz an, der für die Datenbank definiert ist.                                       |
| QUERY DEVCLASS    | Zeigt Informationen zu Einheitenklassen an.  |
| QUERY DOMAIN      | Zeigt Informationen über Maßnahmendomänen an.  |
| QUERY LOG         | Zeigt Informationen zum Wiederherstellungsprotokoll an.  |
| QUERY MGMTCLASS   | Zeigt Informationen zu Verwaltungsklassen an.  |
| QUERY OPTION      | Zeigt Informationen über Serveroptionen an.  |
| QUERY PROCESS     | Zeigt Informationen über Hintergrundprozesse an.   |
| QUERY SCHEDULE    | Zeigt Informationen über Zeitpläne an.   |
| QUERY SESSION     | Zeigt Informationen zu allen aktiven Administrator- und Clientsitzungen mit IBM Spectrum Protect an.                 |
| QUERY STATUS      | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| QUERY STGPOOL     | Zeigt Informationen zu Speicherpools an.   |
| QUERY VOLHISTORY  | Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.                                   |
| QUERY VOLUME      | Zeigt Informationen über Speicherpooldatenträger an.   |

## QUERY TAPEALERTMSG (Status des Befehls SET TAPEALERTMSG anzeigen)

Mit diesem Befehl kann der Status des Befehls SET TAPEALERTMSG angezeigt werden. Sie können Bandalerts aktivieren oder inaktivieren. Bei einer Aktivierung kann IBM Spectrum Protect Diagnoseinformationen aus einer Band- oder Kassettenarchivereinheit abrufen und mit Hilfe von ANR-Nachrichten anzeigen. Bei einer Inaktivierung fragt IBM Spectrum Protect diese Informationen nicht ab.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-Query TAPEAlertmsg-----><
```

## Beispiel: Den Status des Befehls QUERY TAPEALERTMSG anzeigen

Stellen Sie mit dem Befehl QUERY TAPEALERTMSG fest, ob Bandalerts aus Einheiten abgerufen und in Form von ANR-Nachrichten angezeigt werden sollen.

```
query tapealertmsg
```

```
ANR2017I Administrator SERVER_CONSOLE hat folgenden Befehl ausgegeben:  
QUERY TAPEALERTMSGANR8960I QUERY TAPEALERTMSG: Die Anzeige von Bandalerts von SCSI-Einheiten  
ist aktiviert.
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY TAPEALERTMSG

| Befehl           | Beschreibung   |
|------------------|--|
| SET TAPEALERTMSG | Gibt an, ob Band- und Kassettenarchiveinheiten Diagnoseinformationen an den Server melden. |

## QUERY TOC (Inhaltsverzeichnis für ein Sicherungsimagen anzeigen)

Mit diesem Befehl können Verzeichnis- und Dateiangaben im Inhaltsverzeichnis (TOC) für ein angegebenes Sicherungsimagen angezeigt werden. Mit diesem Befehl werden keine Inhaltsverzeichnisinformationen in die IBM Spectrum Protect-Datenbank geladen. Das angegebene Inhaltsverzeichnis wird aus einem Speicherpool gelesen, wenn der Befehl QUERY TOC ausgegeben wird.

Dieser Befehl kann nicht von der Serverkonsole ausgegeben werden. Ist das Inhaltsverzeichnis auf einem austauschbaren Datenträger gespeichert, ist ein Mountpunkt erforderlich und die Ausgabe wird verzögert, während der Speicherpoolatenträger geladen wird.

## Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie entweder System- oder Maßnahmenberechtigung für die Domäne, der der Knoten zugeordnet ist, oder Clientteigenerberechtigung für den Knoten haben.

## Syntax

```
>>-Query TOC--Knotenname--Dateibereichsname----->  
>+-----+----->  
'-CREATIONDate----Datum--CREATIONTime----Zeit-'  
. -Format----Standard----.  
>+-----+-----><  
'-Format----+Standard-+-'  
'-Detailed-'
```

## Parameter

### Knotenname (Erforderlich)

Gibt den Namen des NAS-Knotens an, zu dem das Inhaltsverzeichnis gehört. Sie können zur Angabe dieses Namens keine Platzhalterzeichen verwenden.

### Dateibereichsname (Erforderlich)

Gibt den Namen des Dateibereichs an, zu dem das Inhaltsverzeichnis gehört. Der angegebene Dateibereichsname darf keine Platzhalterzeichen enthalten.

### CREATIONDate

Gibt das Erstellungsdatum des Sicherungsimagen an, für das das Inhaltsverzeichnis angezeigt werden soll. Dieser Parameter ist wahlfrei. Wird CREATIONDATE angegeben, muss auch CREATIONTIME angegeben werden. Werden diese Parameter nicht angegeben, wird der Inhalt des letzten Sicherungsimagen für den angegebenen Knoten und Dateibereich angezeigt, vorausgesetzt, dieses Image hat ein Inhaltsverzeichnis. Das Erstellungsdatum kann nur wie folgt angegeben werden:

| Wert       | Beschreibung         | Beispiel   |
|------------|----------------------|------------|
| MM/TT/JJJJ | Ein bestimmtes Datum | 05/15/2002 |

Gibt an, dass der Inhalt des Sicherungsimages angezeigt werden soll, das an diesem Datum erstellt wurde. Sie können dieses Datum der Ausgabe des Befehls QUERY NASBACKUP entnehmen.

#### CREATIONTime

Gibt die Erstellungszeit des Sicherungsimages an, für das das Inhaltsverzeichnis angezeigt werden soll. Dieser Parameter ist wahlfrei. Wird CREATIONTIME angegeben, muss auch CREATIONDATE angegeben werden. Werden diese Parameter nicht angegeben, wird der Inhalt des letzten Sicherungsimages für den angegebenen Knoten und Dateibereich angezeigt, vorausgesetzt, dieses Image hat ein Inhaltsverzeichnis. Die Erstellungszeit kann nur wie folgt angegeben werden:

| Wert     | Beschreibung  | Beispiel |
|----------|---|----------|
| HH:MM:SS | Eine bestimmte Uhrzeit am angegebenen Erstellungsdatum. | 10:30:08 |

Gibt an, dass der Inhalt des Sicherungsimages angezeigt werden soll, das zu dieser Uhrzeit am angegebenen Datum erstellt wurde. Sie können diese Uhrzeit der Ausgabe des Befehls QUERY NASBACKUP entnehmen.

#### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

##### Standard

Gibt an, dass Teilinformationen für die Dateien angezeigt werden.

##### Detailed

Gibt an, dass die vollständigen Informationen für die Dateien angezeigt werden, einschließlich der hexadezimalen Darstellung jedes Datei- oder Verzeichnisnamens.

## Beispiel: Ausführliche Informationen zum Inhaltsverzeichnis für einen bestimmten Knoten anzeigen

Mit dem Befehl QUERY TOC Informationen in dem Inhaltsverzeichnis anzeigen, das zum NAS-Knoten NETAPP im Dateibereich /vol/vol1 gehört, der am 12/06/2002 um 11:22:46 Uhr erstellt wurde. Ein detailliertes Format angeben.

```
query toc netapp /vol/vol1 creationdate=12/06/2002 creationtime=11:22:46
format=detailed
```

Objekte im Image, die am 12/06/2002 um 11:22:46 Uhr für Dateibereich /vol/vol1 in Knoten NETAPP gesichert wurden:

```

Objektname: /.etc
Hexadezimaler Objektname: 2f657463
Objekttyp: Verzeichnis
Objektgröße: 4.096
Datum/Zeit der letzten Datenänderung: 07/31/2002 14:21:19

Objektname: /.etc/oldmaps/ndmp
Hexadezimaler Objektname: 2f6574632f6f6c646d6170
732f6e646d70
Objekttyp: Verzeichnis
Objektgröße: 4.096
Datum/Zeit der letzten Datenänderung: 07/31/2002 14:21:19

Objektname: /.etc/oldmaps/ndmp/TSM
/vol/vol1/3df0e8fd
Hexadezimaler Objektname: 2f6574632f6f6c646d6170
732f6e646d702f54534d2
02f766f6c2f766f6c312f3
364663065386664
Objekttyp: Datei
Objektgröße: 36,864
Datum/Zeit der letzten Datenänderung: 12/06/2002 11:14:22
```

## Feldbeschreibungen

### Objektname

Der Name des Objekts.

### Hexadezimaler Objektname

Der Name des Objekts im Hexadezimalformat.

### Objekttyp

Der Typ des Objekts.

Objektgröße

Die Größe des Objekts.

Datum/Zeit der letzten Datenänderung

Der Zeitpunkt (Datum und Uhrzeit), an dem das Objekt zuletzt geändert wurde.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY TOC

| Befehl          | Beschreibung   |
|-----------------|--|
| BACKUP NODE     | Sichert einen NAS-Knoten (NAS = Network Attached Storage).         |
| QUERY NASBACKUP | Zeigt Informationen zu NAS-Sicherungsimages an.                    |
| RESTORE NODE    | Schreibt einen NAS-Knoten (NAS = Network Attached Storage) zurück. |

## QUERY VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs abfragen)

Verwenden Sie diesen Befehl, um eine Definition für die Zuordnung des virtuellen Dateibereichs abzufragen.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-Query VIRTUALFSmapping ----->>
.
.*-----
>+-----+-----><
|          .*-----|
|'-Knotenname-----+'
|          '-Name_des_virtuellen_Dateibereichs-'|
```

### Parameter

#### Knotenname

Gibt den Clientknoten an, zu dem der virtuelle Dateibereich gehört. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert ist alle Clientknotenamen. Für diesen Parameter muss ein Wert angegeben werden, wenn der Name eines virtuellen Dateibereichs angegeben wird.

#### Name\_des\_virtuellen\_Dateibereichs

Gibt den Namen der abzufragenden Zuordnung des virtuellen Dateibereichs an. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Wird kein Wert angegeben, werden alle Zuordnungen des virtuellen Dateibereichs abgefragt. Bei den Zuordnungsamen des virtuellen Dateibereichs muss die Groß-/Kleinschreibung berücksichtigt werden. Mit dem Befehl QUERY VIRTUALFSMAPPING kann die korrekte Schreibweise für die abzufragende Zuordnung des virtuellen Dateibereichs bestimmt werden.

## Beispiel: Virtuelle Dateibereiche für einen bestimmten Knoten anzeigen

Die gegenwärtig definierten virtuellen Dateibereiche für Knoten NAS1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query virtualfsmapping nas1
```

| Knotenname | Name d. virt. Dateiber. | Name d. Zuordnung | Dateiber. Name   | Pfad | Hexadezimaler Pfad? |
|------------|-------------------------|-------------------|------------------|------|---------------------|
| NAS1       | /mikesdir               | /vol/vol2         | /mikes           | No   |                     |
| NAS1       | /tmpdir                 | /vol/vol1         | /tmp             | No   |                     |
| NAS1       | /nonASCIIIDir           | /vol/vol3         | 2f73657276657231 | Yes  |                     |

### Feldbeschreibungen

Knotenname

Gibt den Namen des Clientknotens an.  
 Name der Zuordnung des virtuellen Dateibereichs  
 Gibt den Namen der Zuordnung des virtuellen Dateibereichs an.  
 Dateibereichsname

Der Name des Dateibereichs, der zu dem Knoten gehört.

Dateibereichsnamen können eine andere Zeichenumsetzungstabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetzungstabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetzungstabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetzungstabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

Pfad  
 Gibt den Pfad zum Clientknoten an.  
 Hexadezimaler Pfad  
 Gibt an, ob der Pfad ein hexadezimaler Pfad ist.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY VIRTUALFSMAPPING

| Befehl                  | Beschreibung  |
|-------------------------|---|
| DEFINE VIRTUALFSMAPPING | Zuordnung eines virtuellen Dateibereichs definieren.    |
| DELETE VIRTUALFSMAPPING | Zuordnung eines virtuellen Dateibereichs löschen.       |
| UPDATE VIRTUALFSMAPPING | Zuordnung eines virtuellen Dateibereichs aktualisieren. |

## QUERY VOLHISTORY (History-Daten für sequentielle Datenträger anzeigen)

Mit diesem Befehl können History-Daten von sequenziellen Datenträgern angezeigt werden. Um Protokolldaten sequenzieller Datenträger in einer oder mehreren Dateien zu speichern, verwenden Sie den Befehl BACKUP VOLHISTORY.

Verwenden Sie die Serveroption VOLUMEHISTORY, um eine oder mehrere Protokolldateien für Datenträger anzugeben. Nachdem der Server erneut gestartet wurde, aktualisiert IBM Spectrum Protect die Datenträgerinformationen in der Datenbank und in den Dateien.

Mit dem Befehl QUERY BACKUPSET können Informationen zur angegebenen Sicherungsgruppe abgefragt werden.

## Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```

      .-BEGINDate-----frühestes_Datum-.
>>-Query VOLHistory--+-+-----+----->
      '-BEGINDate-----Datum-----'

      .-ENDDate-----aktuelles_Datum-.
>--+-+-----+----->
      '-ENDDate-----Datum-----'

      .-BEGINTime-----00:00:00-.
>--+-+-----+----->
      '-BEGINTime-----Zeit-----'

      .-ENDTime-----aktuelle_Uhrzeit-.
>--+-+-----+----->
      '-ENDTime-----Zeit-----'

      .-Type-----All-----
>--+-+-----+-----<

```

```
'-Type--==--All-----+'
+-BACKUPSET----+
+-DBBackup-----+
+-DBRpf-----+
+-DBSnapshot--+
+-EXPort-----+
|                |
|      (1)      |
+-REmote-----+
+-RPFile-----+
+-RPFSSnapshot+
+-STGDelete---+
+-STGNew-----+
+-STGReuse----+'
```

Anmerkungen:

1. Dieser Parameter ist nur für die Betriebssysteme AIX, HP-UX, Linux, Solaris und Windows verfügbar.

## Parameter

### BEGINDate

Gibt an, dass Informationen beginnend mit den Sätzen angezeigt werden sollen, die an einem angegebenen Datum erstellt wurden. Dieser Parameter ist wahlfrei. Standardwert ist das früheste Datum, ab dem History-Daten vorliegen.

Sie können das Datum unter Verwendung der folgenden Werte angeben:

| Wert                           | Beschreibung   | Beispiel  |
|--------------------------------|--|---|
| MM/TT/JJJJ                     | Ein bestimmtes Datum                                     | 09/15/1998  |
| TODAY                          | Das aktuelle Datum                                       | TODAY   |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage | TODAY-7 <b>oder</b> -7.<br><br>Sollen Informationen beginnend mit den Sätzen, die vor einer Woche erstellt wurden, angezeigt werden, BEGINDATE=TODAY-7 oder BEGINDATE=-7 angeben. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.                            | EOLM  |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.      | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.  |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.                      | BOTM  |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage. | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.   |

### ENDDate

Gibt an, dass Informationen bis zu den Sätzen angezeigt werden sollen, die an dem angegebenen Datum erstellt wurden. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum.

Sie können das Datum unter Verwendung der folgenden Werte angeben:

| Wert                           | Beschreibung   | Beispiel  |
|--------------------------------|--|---|
| MM/TT/JJJJ                     | Ein bestimmtes Datum   | 09/15/1998  |
| TODAY                          | Das aktuelle Datum   | TODAY   |
| TODAY-Tage <b>oder</b> -Tage   | Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage beträgt 9999. | TODAY-1 <b>oder</b> -1.<br><br>Sollen Sätze angezeigt werden, die bis gestern erstellt wurden, ENDDATE=TODAY-1 oder ENDDATE=-1 angeben. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.  | EOLM  |

| Wert                        | Beschreibung   | Beispiel   |
|-----------------------------|--|--|
| EOLM-Tage                   | Der letzte Tag des Vormonats minus angegebene Tage.      | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats) | Der erste Tag des aktuellen Monats.                      | BOTM   |
| BOTM+Tage                   | Der erste Tag des aktuellen Monats plus angegebene Tage. | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

#### BEGINTime

Gibt an, dass Informationen beginnend mit den Sätzen angezeigt werden sollen, die zu der angegebenen Uhrzeit erstellt wurden. Dieser Parameter ist wahlfrei. Der Standardwert ist Mitternacht (00:00:00).

Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

| Wert                         | Beschreibung   | Beispiel  |
|------------------------------|--|---|
| HH:MM:SS                     | Eine bestimmte Uhrzeit am angegebenen Anfangsdatum                             | 12:33:28  |
| NOW                          | Die aktuelle Uhrzeit am angegebenen Anfangsdatum                               | NOW   |
| NOW+HH:MM <b>oder</b> +HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Anfangsdatum  | NOW+03:00 <b>oder</b> +03:00.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTIME=NOW+03:00 oder BEGINTIME=+03:00 ausgegeben, zeigt IBM Spectrum Protect Sätze mit der Uhrzeit 12:00 Uhr oder später am Anfangsdatum an. |
| NOW-HH:MM <b>oder</b> -HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Anfangsdatum | NOW-03:30 <b>oder</b> -03:30.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTIME=NOW-03:30 oder BEGINTIME=-03:30 ausgegeben, zeigt IBM Spectrum Protect Sätze mit der Uhrzeit 5:30 Uhr oder später am Anfangsdatum an.  |

#### ENDTime

Gibt an, dass Informationen bis zu den Sätzen angezeigt werden sollen, die zu der angegebenen Uhrzeit am Enddatum erstellt wurden. Dieser Parameter ist wahlfrei. Standardwert ist die aktuelle Uhrzeit.

Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

| Wert                         | Beschreibung   | Beispiel  |
|------------------------------|--|---|
| HH:MM:SS                     | Eine bestimmte Uhrzeit am angegebenen Enddatum                             | 10:30:08  |
| NOW                          | Die aktuelle Uhrzeit am angegebenen Enddatum                               | NOW   |
| NOW+HH:MM <b>oder</b> +HH:MM | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum  | NOW+03:00 <b>oder</b> +03:00.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW+03:00 oder ENDTIME=+03:00 ausgegeben, zeigt IBM Spectrum Protect Sätze mit der Uhrzeit 12:00 Uhr oder später am Enddatum an. |
| NOW-HH:MM <b>oder</b> -HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum | NOW-03:30 <b>oder</b> -03:30<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW-3:30 oder ENDTIME=-3:30 ausgegeben, zeigt IBM Spectrum Protect Sätze mit der Uhrzeit 5:30 Uhr oder früher am Enddatum an.     |

#### Type

Gibt die Art der Sätze an, die aus der Datenträger-History-Datei angezeigt werden sollen. Dieser Parameter ist wahlfrei. Standardwert ist ALL. Gültige Werte:

Alle

Gibt alle Sätze an.

**BACKUPSET**  
Gibt an, dass nur Informationen über Datenträger mit Sicherungsgruppen angezeigt werden.

**DBBackup**  
Gibt an, dass nur Sätze angezeigt werden, die Informationen über Datenträger mit Gesamt- und Teilsicherungen der Datenbank enthalten (Datenträgertypen BACKUPFULL und BACKUPINCR).

**DBRpf**  
Gibt an, dass nur Sätze angezeigt werden, die Informationen über Datenträger mit Gesamt- und Teilsicherungen der Datenbank und über Datenträger mit Wiederherstellungsplandateiobjekten enthalten (Datenträgertypen BACKUPFULL, BACKUPINCR und RPFfile).

**DBSnapshot**  
Gibt an, dass nur Sätze angezeigt werden sollen, die Informationen über Datenträger enthalten, die für Datenbankmomentaufnahmesicherungen verwendet werden.

**EXPort**  
Gibt nur Sätze an, die Informationen über Exportdatenträger enthalten.

**REMOte**  
Gibt an, dass nur Sätze angezeigt werden sollen, die Informationen zu Datenträgern enthalten, die von Kassettenarchivclients verwendet werden.

**RPFfile**  
Gibt an, dass nur Sätze angezeigt werden sollen, die Informationen zu Dateiobjekten eines Wiederherstellungsplans enthalten, die auf einem Zielsever gespeichert sind und unter der Annahme von Datenbankgesamtsicherungen und Teilsicherungen erstellt wurden. Mit dem Parameter werden nur Sätze zu Wiederherstellungsplandateien angezeigt, die unter Verwendung der IBM Spectrum Protect-Funktion für virtuelle Datenträger für die Übertragung zwischen Servern auf einem anderen IBM Spectrum Protect-Server gespeichert werden.

**RPFSnapshot**  
Gibt an, dass nur Sätze angezeigt werden sollen, die Informationen zu Dateiobjekten eines Wiederherstellungsplans enthalten, die auf einem Zielsever gespeichert sind und unter der Annahme von Datenbankmomentaufnahmesicherungen erstellt wurden. Mit RPFSnapshot werden nur Sätze zu Wiederherstellungsplandateien angezeigt, die unter Verwendung der IBM Spectrum Protect-Funktion für virtuelle Datenträger für die Übertragung zwischen Servern auf einem anderen IBM Spectrum Protect-Server gespeichert werden.

**STGDelete**  
Gibt nur Sätze an, die Informationen über gelöschte sequenzielle Datenträger aus dem Speicherpool enthalten.

**STGNew**  
Gibt nur Sätze an, die Informationen über neue Speicherdatenträger mit sequenziellem Zugriff enthalten.

**STGReuse**  
Gibt nur Sätze an, die Informationen über wiederverwendete sequenzielle Datenträger aus dem Speicherpool enthalten.

## Beispiel: Datenträgerprotokolldaten für einen Speicherpoolatenträger anzeigen

Zeigen Sie Datenträgerprotokolldaten für einen Speicherpoolatenträger an, der in der Datenbank gespeichert ist. Für Feldbeschreibungen siehe Feldbeschreibungen. Den folgenden Befehl ausgeben:

```
query volhistory type=stgnew
```

```

Datum/Uhrzeit: 02/25/2011 18:28:06
Datenträgertyp: STGNEW
Sicherungsserie:
Sicherungsoperation:
Datenträgerfolge:
Einheitenklasse: FILE
Datenträgername: /adsmfct/server/prvoll
Datenträgerstandort:
Befehl:
Obere Datenbanksicherungs-ID:
Untere Datenbanksicherungs-ID:
Ausgangsposition für Datenbanksicherung:
Adresse der höheren Ebene für Datenbanksicherung:
Adresse der unteren Ebene für Datenbanksicherung:
Summe der Datenbyte für Datenbanksicherung (MB):
Summe der Protokollbyte für Datenbanksicherung (MB):
Obere Blocknummer für Datenbanksicherung:
Untere Blocknummer für Datenbanksicherung:
Datenbanksicherungsdatenstrom-ID:
Folgenummer des Datenbanksicherungsdatenträgers für Datenstrom:

```

Anmerkung: Die Datenträgerhistorydatei enthält zusätzliche Felder, die in der Ausgabe der Abfrage nicht angezeigt werden. Diese Felder beziehen sich speziell auf die Unterstützung der Datenbanksicherung und -zurückschreibung. Sie sind nicht für die Verwendung oder Änderung durch IBM Spectrum Protect-Administratoren bestimmt. Die Felder sind mit einer Nachricht in Klammern versehen, die angibt, dass die Felder nur für die interne IBM Spectrum Protect-Verwendung und nicht für die Änderung bestimmt sind.



## Beispiel: Datenträgerprotokolldaten für einen Datenbanksicherungsdatenträger anzeigen

Zeigen Sie Datenträgerprotokolldaten für einen Datenbanksicherungsdatenträger an, der in der Datenbank gespeichert ist. Für Feldbeschreibungen siehe Feldbeschreibungen. Den folgenden Befehl ausgeben:

```
query volhistory type=dbb
```

```

Datum/Uhrzeit: 02/25/2011 18:28:06
Datenträgertyp: BACKUPFULL
Sicherungsserie: 176
Sicherungsoperation: 0
Datenträgerfolge: 0
Einheitenklasse: FILE
Datenträgername: /adsmfct/server/prvoll
Datenträgerstandort:
    Befehl:
        Obere Datenbanksicherungs-ID: 0
        Untere Datenbanksicherungs-ID: 0
        Ausgangsposition für Datenbanksicherung: 0
        Adresse der höheren Ebene für Datenbanksicherung:
        Adresse der unteren Ebene für Datenbanksicherung:
        Summe der Datenbyte für Datenbanksicherung (MB): 0
        Summe der Protokollbyte für Datenbanksicherung (MB): 0
        Obere Blocknummer für Datenbanksicherung: 0
        Untere Blocknummer für Datenbanksicherung: 0
        Datenbanksicherungsdatenstrom-ID: 1
Folgenummer des Datenbanksicherungsdatenträgers für Datenstrom: 10.001
```

Anmerkung: Die Datenträgerhistorydatei enthält zusätzliche Felder, die in der Ausgabe der Abfrage nicht angezeigt werden. Diese Felder beziehen sich speziell auf die Unterstützung der Datenbanksicherung und -zurückschreibung. Sie sind nicht für die Verwendung oder Änderung durch IBM Spectrum Protect-Administratoren bestimmt. Die Felder sind mit einer Nachricht in Klammern versehen, die angibt, dass die Felder nur für die interne IBM Spectrum Protect-Verwendung und nicht für die Änderung bestimmt sind.

## Feldbeschreibungen

### Datum/Uhrzeit

Das Datum und die Uhrzeit, an dem bzw. zu der der Datenträger erstellt wurde.

### Datenträgertyp

Der Typ des Datenträgers:

#### BACKUPFULL

Datenträger mit Gesamtsicherung der Datenbank.

#### BACKUPINCR

Datenträger mit Teilsicherung der Datenbank.

#### BACKUPSET

Datenträger mit Clientsicherungsgruppe.

#### DBSNAPSHOT

Datenträger mit Datenbankmomentaufnahmesicherung.

#### EXPORT

Exportdatenträger.

#### REMOTE

Ein Datenträger, der auf dem Kassettenarchivclient verwendet wird, der der im Feld für den Datenträgerstandort angegebene IBM Spectrum Protect-Server ist. Die Datenträger-History auf dem Server, der der Kassettenarchivclient ist, enthält ausführliche Informationen zur Verwendung des Datenträgers.

#### RPFIL

Datenträger mit Wiederherstellungsplandateiobjekt, der unter der Annahme von Gesamt- und Teilsicherungen der Datenbank erstellt wurde.

#### RPFSnapshot

Datenträger mit Wiederherstellungsplandateiobjekt, der unter der Annahme von Datenbankmomentaufnahmesicherungen erstellt wurde.

#### STGDELETE

Gelöschter Datenträger aus dem Speicherpool mit sequenziellem Zugriff.

#### STGNEW

Hinzugefügter Datenträger aus dem Speicherpool mit sequenziellem Zugriff.

#### STGREUSE

Wiederverwendeter Datenträger aus dem Speicherpool mit sequenziellem Zugriff.

### Sicherungsserie

Der Wert dieses Felds hängt vom Datenträgertyp ab:

- Für den Datenträgertyp BACKUPFULL oder BACKUPINCR: Die Kennung der Sicherungsserie.
- Für den Datenträgertyp DBSNAPSHOT: Die Kennung der Sicherungsserie, die dem Eintrag DBSNAPSHOT zugeordnet ist.
- Für den Datenträgertyp RPFIL: Die Kennung der Sicherungsserie, die dem Eintrag RPFIL zugeordnet ist.
- Für den Datenträgertyp RPFNSNAPSHOT: Die Kennung der Sicherungsserie, die dem Eintrag RPFNSNAPSHOT zugeordnet ist.
- Für den Datenträgertyp BACKUPSET: Dieses Feld ist leer.
- Für alle anderen Datenträgertypen: Immer 0.

Eine Sicherungsserie besteht aus einer Gesamtsicherung und aus allen Teilsicherungen, die zu dieser Gesamtsicherung gehören. Eine neue Sicherungsserie beginnt bei der nächsten Gesamtsicherung der Datenbank.

#### Sicherungsoperation

Für den Datenträgertyp BACKUPFULL oder BACKUPINCR: Die Operationsnummer dieses Sicherungsdatenträgers innerhalb der Sicherungsserie. Eine Gesamtsicherung innerhalb einer Sicherungsserie wird als Operation 0 angegeben. Die erste Teilsicherung für diese Gesamtsicherung wird als Operation 1 bezeichnet, die zweite Teilsicherung als Operation 2 usw.

Für Datenträgertypen DBSNAPSHOT: Die Operationsnummer dieses DBSNAPSHOT-Datenträgers innerhalb der DBSNAPSHOT-Serie.

Für alle anderen Datenträgertypen: Immer 0.

Dieses Feld ist leer, wenn der Datenträgertyp BACKUPSET lautet.

#### Datenträgerfolge

Die Folge oder Position des Datenträgers innerhalb der Sicherungsserie.

- Für den Datenträgertyp BACKUPFULL oder BACKUPINCR: Die Folge oder Position des Datenträgers innerhalb der Sicherungsserie. Die Datenträgerfolge 1 kennzeichnet den für die erste Operation (eine Gesamtsicherung) verwendeten ersten Datenträger usw. Belegt die Gesamtsicherung beispielsweise drei Datenträger, werden diese Datenträger als Datenträgerfolge 1, 2 und 3 gekennzeichnet. Der erste Datenträger der nächsten Operation (die erste Teilsicherung) wird demnach als Datenträgerfolge 4 bezeichnet.
- Für Datenträgertypen BACKUPSET: Die Folge oder Position des Datenträgers innerhalb der BACKUPSET-Serie.
- Für Datenträgertypen DBSNAPSHOT: Die Folge oder Position des Datenträgers innerhalb der DBSNAPSHOT-Serie. Die Datenträgerfolge 1 gibt den ersten Datenträger für die erste DBSNAPSHOT-Operation an, usw.
- Für den Datenträgertyp EXPORT: Die Folgennummer des Datenträgers, wenn er zum Exportieren von Daten verwendet wurde.
- Für den Datenträgertyp RPFIL: Der Wert dieses Feldes ist immer 1.
- Für alle anderen Datenträgertypen: Immer 0.

#### Einheitenklasse

Der Name der Einheitenklasse, die diesem Datenträger zugeordnet ist.

#### Datenträgername

Der Name des Datenträgers.

#### Datenträgerstandort

Der Standort des Datenträgers. Diese Informationen sind nur für die folgenden Datenträgertypen verfügbar:

- BACKUPFULL
- BACKUPINCR
- EXPORT
- REMOTE
- RPFIL

Für den Datenträgertyp REMOTE ist dieses Feld für den Standort der Servername des Kassettenarchivclients, der Eigner dieses Datenträgers ist.

Für den Datenträgertyp RPFIL ist dieses Feld für den Standort der Servername, der in der Einheitenklassendefinition definiert ist, die von dem Befehl PREPARE verwendet wird, wenn der Parameter DEVCLASS angegeben ist.

#### Befehl

Lautet der Datenträgertyp EXPORT oder BACKUPSET und lautet die Datenträgerfolge 1 (der erste Datenträger), zeigt dieses Feld den Befehl, der zum Generieren des Datenträgers verwendet wurde. Befindet sich EXPORT oder BACKUPSET auf mehreren Datenträgern, wird der Befehl mit dem ersten Datenträger, aber nicht mit allen anderen Datenträgern angezeigt.

Bei einem anderen Datenträgertyp als EXPORT oder BACKUPSET ist dieses Feld leer.

Tipp: Die folgenden Felder werden von IBM Spectrum Protect-Servern mit Version 6.3 oder höher nicht verwendet. Die Felder werden jedoch für die Kompatibilität mit früheren Releases angezeigt.

- Obere Datenbanksicherungs-ID
- Untere Datenbanksicherungs-ID
- Ausgangsposition für Datenbanksicherung
- Adresse der höheren Ebene für Datenbanksicherung
- Adresse der unteren Ebene für Datenbanksicherung
- Summe der Datenbyte für Datenbanksicherung (MB)
- Summe der Protokollbyte für Datenbanksicherung (MB)
- Obere Blocknummer für Datenbanksicherung
- Untere Blocknummer für Datenbanksicherung

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY VOLHISTORY

| Befehl            | Beschreibung   |
|-------------------|--|
| BACKUP VOLHISTORY | Zeichnet Datenträger-History-Daten in externen Dateien auf.  |
| DELETE VOLHISTORY | Löscht History-Daten sequenzieller Datenträger aus der Datenträger-History-Datei.                                  |
| PREPARE           | Erstellt eine Wiederherstellungsplandatei.   |
| QUERY RPFIL       | Zeigt Informationen über Wiederherstellungsplandateien an.   |
| QUERY BACKUPSET   | Zeigt Sicherungsgruppen an.  |
| UPDATE VOLHISTORY | Ändert Standortinformationen für einen Datenträger in der Datenträger-History-Datei oder fügt Informationen hinzu. |

## QUERY VOLUME (Speicherpooldatenträger abfragen)

Mit diesem Befehl können Informationen über einen oder mehrere Speicherpooldatenträger angezeigt werden.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

>>-Query Volume .-*-----
                |-----|----->
                |'-Datenträgername-'|
                |-----|----->
                |-----|-----|
                | v | |
                |'-ACcess-----+READWrite-----+'|
                |             +-READOnly-----+|
                |             +-UNAvailable--+|
                |             +-Offsite-----+|
                |             |'-DEStroyed---'|
                |-----|-----|
                |-----|-----|'-STGpool----*-----'
                |-----|-----|----->
                |-----|-----|'-STGpool----Poolname-'|
                |-----|-----| v | |
                |'-Status-----+ONline-----+'|
                |             +-Offline--+|
                |             +-EMPTy---+|
                |             +-PENding--+|
                |             +-FILLing--+|
                |             |'-FULl----'|
                |-----|-----|
                |-----|-----|'-DEVclass----*-----'
                |-----|-----|----->
                |'-DEVclass----Einheitenklassenname-'|
                |-----|-----|
                |-----|-----|'-Format----Standard-----'
                |-----|-----|-----><
                |'-Format-----+Standard-+'|

```

## Parameter

---

### Datenträgername

Gibt den Datenträger an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Name angegeben, werden alle Speicherpooldatenträger in der Abfrage berücksichtigt.

### ACcEss

Gibt an, daß die Ausgabe auf bestimmte Datenträgerzugriffsmodi beschränkt ist. Dieser Parameter ist wahlfrei. Es können mehrere Zugriffsmodi angegeben werden, indem die Modi ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird kein Wert für diesen Parameter angegeben, wird die Ausgabe nicht auf bestimmte Zugriffsmodi beschränkt. Gültige Werte:

#### READWrite

Datenträger mit dem Zugriffsmodus READWRITE anzeigen. Client-Knoten und Server-Prozesse haben Lese- und Schreibzugriff auf Dateien, die auf den Datenträgern gespeichert sind.

#### READOnly

Datenträger mit dem Zugriffsmodus READONLY anzeigen. Clientknoten und Serverprozesse haben nur Lesezugriff auf Dateien, die auf den Datenträgern gespeichert sind.

#### UNAVailable

Datenträger mit dem Zugriffsmodus UNAVAILABLE anzeigen. Clientknoten und Serverprozesse können nicht auf Dateien zugreifen, die auf den Datenträgern gespeichert sind.

#### OFFsite

Kopierspeicherpooldatenträger mit dem Zugriffsmodus OFFSITE anzeigen. Die Datenträger befinden sich an ausgelagerten Standorten, von denen aus sie nicht geladen werden können.

#### DESTroyed

Datenträger für primären Speicherpool mit dem Zugriffsmodus DESTROYED anzeigen. Die Datenträger sind als permanent beschädigt gekennzeichnet.

### STatus

Gibt an, daß die Ausgabe auf bestimmte Datenträgerstatus beschränkt ist. Dieser Parameter ist wahlfrei. Es können mehrere Statuswerte angegeben werden, indem die Werte ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird kein Wert für diesen Parameter angegeben, wird die Ausgabe auf keinen bestimmte Status beschränkt. Gültige Werte:

#### ONline

Datenträger mit wahlfreiem Zugriff anzeigen, die für den Server verfügbar sind.

#### Offline

Datenträger mit wahlfreiem Zugriff anzeigen, die für den Server nicht verfügbar sind.

#### EMPTy

Datenträger mit sequenziellem Zugriff anzeigen, die keine Daten enthalten.

#### PENding

Datenträger mit dem Status PENDING anzeigen. Diese Datenträger können Datenträger mit sequenziellem Zugriff sein, auf denen alle Dateien gelöscht wurden, aber für die die mit dem Parameter REUSEDELAY im Befehl DEFINE STGPOOL angegebene Zeit noch nicht abgelaufen ist. Bei diesen Datenträgern kann es sich auch um Plattendatenträger mit wahlfreiem Zugriff handeln, die gelöscht wurden, aber noch gelöschte Daten enthalten, die auf das Schreddern warten. Nach dem Schreddern der Daten wird der Datenträger physisch gelöscht.

#### FILLing

Datenträger mit sequenziellem Zugriff anzeigen, auf die der Server geschrieben hat, die aber noch nicht vollständig beschrieben sind.

#### FULL

Datenträger mit sequenziellem Zugriff anzeigen, die vom Server gefüllt wurden.

### STGPool

Gibt den Speicherpool an, der in der Abfrage berücksichtigt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Speicherpoolname angegeben, werden alle Speicherpools in der Abfrage berücksichtigt.

### DEVclass

Gibt die Einheitenklasse an, die in der Abfrage berücksichtigt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Einheitenklassenname angegeben, werden alle Einheiten in der Abfrage berücksichtigt.

### Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

#### Standard

Gibt an, dass Teilinformationen angezeigt werden.

#### Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

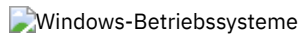
 

## Beispiel: Alle Dateispeicherpooldatenträger auflisten

Informationen zu allen Speicherpooldatenträgern mit dem Einheitenklassenname FILE anzeigen. Für Felddesreibungen siehe Felddesreibungen.

```
query volume devclass=file
```

| Datenträger-<br>name | Speicher-<br>poolname | Einheiten-<br>klassen- | Gesch.<br>Kapazit. | %<br>Ausl. | Datentr.-<br>status |
|----------------------|-----------------------|------------------------|--------------------|------------|---------------------|
| /FCT/SERVER/COV011   | COPYSTG               | FILE                   | 0,0 M              | 0,0        | Pending             |
| /FCT/SERVER/COV012   | COPYSTG               | FILE                   | 0,0 M              | 0,0        | Empty               |
| /FCT/SERVER/COV013   | COPYSTG               | FILE                   | 0,0 M              | 0,0        | Empty               |
| /FCT/SERVER/PRV011   | PRIMESTG              | FILE                   | 0,0 M              | 0,0        | Empty               |
| /FCT/SERVER/PRV012   | PRIMESTG              | FILE                   | 0,0 M              | 0,0        | Empty               |



## Beispiel: Alle Speicherpooldatenträger mit demselben Präfix auflisten

Informationen zu allen Speicherpooldatenträgern, deren Name mit dem Präfix ATF beginnt, anzeigen. Für Felddesreibungen siehe Felddesreibungen.

```
query volume atf*
```

| Datenträger-<br>name | Speicher-<br>poolname | Einheiten-<br>klassen- | Gesch.<br>Kapazit. | %<br>Ausl. | Datentr.-<br>status |
|----------------------|-----------------------|------------------------|--------------------|------------|---------------------|
| ATF001               | 8MMPOOL               | 8MMTAPE                | 4,8 G              | 18,2       | Filling             |
| ATF002               | 8MMPOOL               | 8MMTAPE                | 4,8 G              | 18,2       | Filling             |

## Beispiel: Ausführliche Informationen zu einem bestimmten Speicherpooldatenträger anzeigen

Ausführliche Informationen über den Speicherpooldatenträger /fct/server/covol1 anzeigen. Für Felddesreibungen siehe Felddesreibungen.

```
query volume covol1 format=detailed
```

```
Datenträgername: /FCT/SERVER/COV011
  Speicherpoolname: COPYSTG
  Einheitenklassenname: DISK
  Geschätzte Kapazität: 10,0 M
Skalierte Kapazität angewendet:
  Auslastung in %: 6,7
  Datenträgerstatus: On-line
  Zugriff: Read/Write
Wiederherstellbarer Speicher in %: 3,2
  Arbeitsdatenträger?: Yes
  Im Fehlerstatus?: No
Anzahl beschreibbarer Seiten: 1
  Anzahl Mounts: 11
Anzahl Schreibarbeitsgänge: 1
Ungefähres Datum des letzten Schreibens: 04/14/1998 16:17:26
Ungefähres Datum des letzten Lesens: 04/01/1998 13:26:18
  Anstehend seit:
  Anzahl Schreibfehler: 0
  Anzahl Lesefehler: 0
  Datenträgerstandort:
Datenträger kann in MVS LAN-frei sein: No
Letzte Aktualisierung durch (Administrator): COLLIN
Datum/Zeit der letzten Aktualisierung: 05/01/1998 14:07:27
Anfang der Wiederherstellungsperiode:
  Ende der Wiederherstellungsperiode:
  Geschützter logischer Block:
Manager für Laufwerkverschlüsselungsschlüssel:
```



## Beispiel: Ausführliche Informationen zu einem bestimmten Speicherpooldatenträger anzeigen

Ausführliche Informationen über den Speicherpooldatenträger WPDV00 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query volume wpdv00 format=detailed
```

```
Datenträgername: WPDV00
  Speicherpoolname: TAPEPOOL
    Einheitenklassenname: TAPE
    Geschätzte Kapazität: 5,8 M
Skalierte Kapazität angewendet:
  Auslastung in %: 0,1
  Datenträgerstatus: On-line
    Zugriff: Read/Write
Wiederherstellbarer Speicher in %: 3,2
  Arbeitsdatenträger?: Yes
  Im Fehlerstatus?: No
  Anzahl beschreibbarer Seiten: 1
    Anzahl Mounts: 11
  Anzahl Schreibarbeitsgänge: 1
Ungefähres Datum des letzten Schreibens: 04/14/1998 16:17:26
Ungefähres Datum des letzten Lesens: 04/01/1998 13:26:18
  Anstehend seit:
  Anzahl Schreibfehler: 0
  Anzahl Lesefehler: 0
  Datenträgerstandort:
  Datenträger kann in MVS LAN-frei sein: No
  Letzte Aktualisierung durch (Administrator): COLLIN
  Datum/Zeit der letzten Aktualisierung: 05/01/1998 14:07:27
  Anfang der Wiederherstellungsperiode:
  Ende der Wiederherstellungsperiode:
  Geschützter logischer Block:
Manager für Laufwerkverschlüsselungsschlüssel:
```

## Beispiel: Ausführliche Informationen zu einem Speicherpooldatenträger mit einer bestimmten Einheitenklasse anzeigen

Ausführliche Informationen zu einem Datenträger in einem Speicherpool mit dem Einheitenklassenamen FILECLASS anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query volume devclass=fileclass format=detailed
```

```
Windows-BetriebssystemeDatenträgername: Z:\WORM_CFS\0000000E.BFS
AIX-BetriebssystemeLinux-BetriebssystemeDatenträgername:
/WORM_FILESYS/0000000E.BFS
  Speicherpoolname: FILEPOOL
  Einheitenklassenname: FILECLASS
  Geschätzte Kapazität: 2,0 G
Skalierte Kapazität angewendet:
  Auslastung in %: 0,0
  Datenträgerstatus: Filling
    Zugriff: Read/Write
Wiederherstellbarer Speicher in %: 0,0
  Arbeitsdatenträger?: Yes
  Im Fehlerstatus?: No
  Anzahl beschreibbarer Seiten: 1
    Anzahl Mounts: 1
  Anzahl Schreibarbeitsgänge: 1
Ungefähres Datum des letzten Schreibens: 03/22/2004 15:23:46
Ungefähres Datum des letzten Lesens: 03/22/2004 15:23:46
  Anstehend seit:
  Anzahl Schreibfehler: 0
  Anzahl Lesefehler: 0
  Datenträgerstandort:
  Datenträger kann in MVS LAN-frei sein: No
  Letzte Aktualisierung durch (Administrator):
  Datum/Zeit der letzten Aktualisierung: 03/22/2004 15:23:46
  Anfang der Wiederherstellungsperiode: 03/22/2005
  Ende der Wiederherstellungsperiode: 04/22/2005
  Geschützter logischer Block:
Manager für Laufwerkverschlüsselungsschlüssel:
```

## Beispiel: Ausführliche Informationen zu einem bestimmten Speicherpooldatenträger anzeigen

Ausführliche Informationen zu dem Speicherpooldatenträger 000642 anzeigen. Der Datenträger befindet sich in einem Speicherpool, dem die Einheitenklasse 3592 zugeordnet ist. Für Felddesreibungen siehe Felddesreibungen.

```
query volume 000642 format=detailed
```

```
Datenträgername: 000642
  Speicherpoolname: 3592POOL
  Einheitenklassenname: 3592CLASS
  Geschätzte Kapazität: 2,0 G
Skalierte Kapazität angewendet:
  Auslastung in %: 0,0
  Datenträgerstatus: Filling
  Zugriff: Read/Write
Wiederherstellbarer Speicher in %: 0,0
  Arbeitsdatenträger?: Yes
  Im Fehlerstatus?: No
  Anzahl beschreibbarer Seiten: 1
  Anzahl Mounts: 1
  Anzahl Schreibarbeitsgänge: 1
Ungefähres Datum des letzten Schreibens: 03/22/2004 15:23:46
Ungefähres Datum des letzten Lesens: 03/22/2004 15:23:46
  Anstehend seit:
  Anzahl Schreibfehler: 0
  Anzahl Lesefehler: 0
  Datenträgerstandort:
Datenträger kann in MVS LAN-frei sein: No
Letzte Aktualisierung durch (Administrator):
Datum/Zeit der letzten Aktualisierung: 03/22/2004 15:23:46
  Anfang der Wiederherstellungsperiode: 03/22/2005
  Ende der Wiederherstellungsperiode: 04/22/2005
  Geschützter logischer Block: Yes
Manager für Laufwerkverschlüsselungsschlüssel: IBM Spectrum Protect
```

## Felddesreibungen

---

### Datenträgername

Der Name des Speicherpooldatenträgers.

### Speicherpoolname

Der Speicherpool, für den der Datenträger definiert ist.

### Einheitenklassenname

Die Einheitenklasse, die dem Speicherpool zugeordnet ist.

### Geschätzte Kapazität

Die geschätzte Kapazität des Datenträgers in Megabyte (M), Gigabyte (G) oder Terabyte (T).

Bei Platteneinheiten ist dies die Kapazität des Datenträgers.

Bei Einheiten mit sequenziellem Zugriff ist dieser Wert der geschätzte Gesamtspeicherbereich, der auf dem Datenträger verfügbar ist (auf der Basis der Einheitenklasse).

### Skalierte Kapazität angewendet

Der Prozentsatz der Kapazität, der als Maßstabsfaktor für einen Datenträger dient. Beispiel: Der Wert 20 für einen Datenträger, dessen maximale Kapazität 300 GB beträgt, gibt an, dass der Datenträger nur 20 Prozent von 300 GB oder 60 GB speichern kann. Dieses Attribut gilt nur für Einheiten IBM® 3592.

### Auslastung in %

Die geschätzte Auslastung des Datenträgers. Die Auslastung umfasst den gesamten Speicherbereich, der sowohl von Dateien als auch von Aggregaten belegt ist, einschließlich des leeren Speicherbereichs innerhalb der Aggregate.

Bei Plattendatenträgern umfasst die Auslastung auch den Speicherbereich, der von zwischengespeicherten Daten belegt wird.

### Datenträgerstatus

Der Status des Datenträgers.

### Zugriff

Angabe, ob der Datenträger für den Server verfügbar ist.

### Wiederherstellbarer Speicher in % (nur Datenträger mit sequenziellem Zugriff)

Der Speicherbereich auf diesem Datenträger, der zurückgefordert werden kann, da Daten verfallen sind oder gelöscht wurden. Dieser Wert wird mit der Wiederherstellungsschwelle für den Speicherpool verglichen, um zu bestimmen, ob eine Wiederherstellung erforderlich ist. Wiederherstellbarer Speicherbereich schließt leeren Speicherbereich innerhalb von Aggregaten ein.

Bei der Bestimmung der wiederherzustellenden Datenträger in einem Speicherpool bestimmt der Server zuerst den Wiederherstellungsschwellenwert. Der Wiederherstellungsschwellenwert wird durch den Wert des Parameters THRESHOLD im

Befehl RECLAIM STGPOOL oder, wenn dieser Wert nicht angegeben wurde, durch den Wert des Parameters RECLAIM in einer Speicherpooldefinition angegeben. Der Server überprüft dann den Prozentsatz des wiederherstellbaren Speicherbereichs für jeden Datenträger in dem Speicherpool. Ist der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools, ist der Datenträger ein Kandidat für die Wiederherstellung.

Beispiel: Angenommen, der Speicherpool FILEPOOL hat einen Wiederherstellungsschwellenwert von 70 Prozent. Dieser Wert gibt an, dass der Server jeden Datenträger in dem Speicherpool wiederherstellen kann, der einen höheren Prozentsatz des wiederherstellbaren Speicherbereichs als 70 Prozent hat. Der Speicherpool verfügt über drei Datenträger:

- FILEVOL1 hat 65 Prozent wiederherstellbaren Speicherbereich
- FILEVOL2 hat 80 Prozent wiederherstellbaren Speicherbereich
- FILEVOL3 hat 95 Prozent wiederherstellbaren Speicherbereich

Wenn die Wiederherstellung beginnt, vergleicht der Server den Prozentsatz des wiederherstellbaren Speicherbereichs für jeden Datenträger mit dem Wiederherstellungsschwellenwert von 70 Prozent. In diesem Beispiel sind FILEVOL2 und FILEVOL3 Kandidaten für die Wiederherstellung, da ihr Prozentsatz des wiederherstellbaren Speicherbereichs größer als 70 Prozent ist.

Für Datenträger, die zu einem SnapLock-Speicherpool gehören, wird der Wert angezeigt, aber nicht verwendet.

Arbeitsdatenträger? (nur Datenträger mit sequenziellem Zugriff)

Angabe, ob dieser Datenträger wieder als Arbeitsdatenträger verwendet wird, wenn er leer wird.

Im Fehlerstatus?

Angabe, ob ein Fehler beim Datenträger vorliegt. Der Server kann nicht auf Datenträger schreiben, die sich im Fehlerstatus befinden.

Anzahl beschreibbarer Seiten

Diese Informationen sind für IBM Spectrum Protect reserviert.

Anzahl Mounts

Die Häufigkeit, mit der der Server den Datenträger für die Verwendung geöffnet hat. Die Häufigkeit, mit der der Server den Datenträger geöffnet hat, ist nicht immer mit der Häufigkeit identisch, mit der der Datenträger physisch in ein Laufwerk geladen wurde. Nachdem ein Datenträger physisch geladen wurde, kann der Server denselben Datenträger mehrere Male für verschiedene Operationen öffnen, beispielsweise für verschiedene Clientsicherungssitzungen.

Anzahl Schreibarbeitsgänge (nur Datenträger mit sequenziellem Zugriff)

Angabe, wie oft der Datenträger von Anfang bis Ende beschrieben wurde.

Ungefähres Datum des letzten Schreibens

Das ungefähre Datum, an dem der Datenträger zuletzt beschrieben wurde.

Ungefähres Datum des letzten Lesens

Das ungefähre Datum, an dem der Datenträger zuletzt gelesen wurde.

Anstehend seit

Das Datum, an dem der Status des Datenträgers in 'Anstehend' geändert wurde.

Anzahl Schreibfehler

Die Anzahl Schreibfehler, die auf dem Datenträger aufgetreten sind.

Anzahl Lesefehler

Die Anzahl Lesefehler, die auf dem Datenträger aufgetreten sind.

Datenträgerstandort

Der Standort des Datenträgers.

Datenträger kann in MVS LAN-frei sein

Gibt an, ob der Datenträger LAN-unabhängig ist. Ein LAN-unabhängiger Datenträger ist ein Datenträger, der definiert und (mindestens einmal) von dem IBM Spectrum Protect z/OS-Datenmanagerserver verwendet wurde.

Letzte Aktualisierung durch (Administrator)

Der Administrator, der den Datenträger definiert oder zuletzt aktualisiert hat.

Datum/Zeit der letzten Aktualisierung

Das Datum und die Uhrzeit, an dem bzw. zu der der Datenträger definiert oder zuletzt aktualisiert wurde.

Anfang der Wiederherstellungsperiode

Stellt das Datum dar, nach dem der Server mit der Wiederherstellung dieses Datenträgers beginnt. Dieses Datum darf nicht nach dem Datum liegen, das durch das Ende der Wiederherstellungsperiode dargestellt ist. Befinden sich bei Beginn der Wiederherstellungsperiode Dateien auf dem Datenträger, die nicht verfallen sind, werden sie während der Wiederherstellungsverarbeitung auf einen neuen WORM-Datenträger versetzt. Dieses Feld zeigt nur dann ein Datum an, wenn sich dieser Datenträger in einem Speicherpool befindet, für den der Wert des Parameters RECLAMATIONTYPE SNAPLOCK lautet.

Sind mehrere Archivierungen auf demselben Datenträger gespeichert, basiert der Anfang der Wiederherstellungsperiode des Datenträgers auf dem Datum der neuesten Archivierung. Für SnapLock-Datenträger bestimmt der Parameter RETVer des Befehls DEFINE COPYGROUP, wie lange eine Archivierung gespeichert wird. Ist RETVer auf 100 Tage gesetzt, beginnt die Wiederherstellungsperiode des Datenträgers 100 Tage nach dem Speichern der ersten Archivierung auf dem Datenträger. Wird eine zweite Archivierung auf demselben Datenträger gespeichert, wird das Anfangsdatum der Wiederherstellung auf 100 Tage nach dem Speichern der neuen Archivierung angepasst. Wird der Wert für RETVer geändert, nachdem die erste Archivierung gespeichert wurde, gilt das älteste Wiederherstellungsdatum für alle Archivierungen auf dem Datenträger. Beispiel: Angenommen,



RETVer ist für eine anfängliche Archivierung auf 100 gesetzt, aber wird dann in 50 geändert. Wird eine zweite Archivierung auf dem Datenträger drei Tage nach der ersten Archivierung gespeichert, beginnt die Wiederherstellungsperiode erst 100 Tage nach dem Speichern der ersten Archivierung.

#### Ende der Wiederherstellungsperiode

Stellt das Datum dar, bis zu dem der IBM Spectrum Protect-Server die Wiederherstellungsverarbeitung auf diesem Datenträger beenden muss, um den ununterbrochenen Schutz der Daten sicherzustellen. Es stellt außerdem das Attribut der physischen Datei für das Datum des letzten Zugriffs im NetApp-Dateiserver dar, mit dem verhindert wird, dass die Datei vor diesem Datum gelöscht wird. Dieses Feld zeigt nur dann ein Datum an, wenn sich dieser Datenträger in einem Speicherpool befindet, für den der Wert des Parameters RECLAMATIONTYPE SNAPLOCK lautet.

#### Manager für Laufwerkverschlüsselungsschlüssel

Der Manager für Laufwerkverschlüsselungsschlüssel. Dieses Feld gilt nur für Datenträger in einem Speicherpool, dem der Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet ist.

#### Geschützter logischer Block

Gibt an, ob der Schutz logischer Blöcke für den Datenträger aktiviert ist. Sie können den Schutz logischer Blöcke nur mit den folgenden Typen von Laufwerken und Datenträgern verwenden:

- IBM LTO5 und höher
- IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
- Oracle StorageTek T10000C- und T10000D-Laufwerke

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY VOLUME

| Befehl          | Beschreibung   |
|-----------------|--|
| DEFINE DEVCLASS | Definiert eine Einheitenklasse.  |
| DEFINE VOLUME   | Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll. |
| DELETE VOLUME   | Löscht einen Datenträger aus einem Speicherpool.   |
| UPDATE DEVCLASS | Ändert die Attribute einer Einheitenklasse.  |
| UPDATE VOLUME   | Aktualisiert die Attribute der Speicherpooldatenträger.  |
| VARY            | Gibt an, ob ein Plattendatenträger für die Verwendung durch den Server verfügbar ist.                          |

## QUIT (Interaktiven Modus des Verwaltungsclient verlassen)

Mit diesem Befehl kann eine Verwaltungs-Client-Sitzung im interaktiven Modus beendet werden.

Der Befehl QUIT kann nicht von der Verwaltungs-ID SERVER\_CONSOLE oder im Konsolenmodus, Stapelbetrieb oder Mountmodus des Verwaltungsclients verwendet werden.

## Berechtigungs-klasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
>>-QUIT-----<<
```

## Parameter

Keine.

## Beispiel: Eine interaktive Verwaltungsclientsitzung beenden

Eine im interaktiven Modus befindliche Verwaltungssitzung des Clients verlassen.

```
quit
```

## Zugehörige Befehle

---

Keine.

## RECLAIM STGPOOL (Datenträger im Speicherpool mit sequenziellem Zugriff wiederherstellen)

---

Verwenden Sie diesen Befehl, um Datenträger in einem Speicherpool mit sequenziellem Zugriff wiederherzustellen. Bei der Wiederherstellung werden keine inaktiven Versionen von Sicherungsdaten von Datenträgern in Pools für aktive Daten versetzt.

Dieser Befehl kann für die folgenden Typen von Speicherpools nicht verwendet werden:

- Containerkopierspeicherpools. Speicherbereich in diesen Speicherpools wird im Rahmen der Verarbeitung wiederhergestellt, die durch die Befehle PROTECT STGPOOL erfolgt.
- Speicherpools mit einem der folgenden Datenformate:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP
- Speicherpools, die eine Einheitenklasse CENTERA verwenden.
- Speicherpools, die eine Einheitenklasse WORM (Write Once Read Many) verwenden. Die Wiederherstellung ist nicht erforderlich, da WORM-Datenträger nicht wiederverwendbar sind. Sie können jedoch eine Wiederherstellung ausführen, um Daten auf weniger Datenträgern zusammenzufassen.

Verwenden Sie diesen Befehl nur, wenn die automatische Wiederherstellung für den Speicherpool nicht verwendet wird. Dieser Befehl akzeptiert die Werte der Attribute RECLAIMPROCESS und RECLAIMSTGPOOL der Speicherpooldefinition. Dieser Befehl akzeptiert auch die Werte der Parameter OFFSITERECLAIMLIMIT und RECLAIM der Speicherpooldefinition, sofern sie nicht durch die Befehlsparameter OFFSITERECLAIMLIMIT und THRESHOLD überschrieben werden.

Tipps:

- Wird dieser Befehl ausgegeben, werden doppelte Daten in einem primären Speicherpool, Kopierspeicherpool oder Pool für aktive Daten entfernt, der für die Deduplizierung von Daten definiert ist.
- Wenn Sie diesen Befehl verwenden, um deduplizierte Objekte in denselben Speicherpool zurückzuschreiben, werden alle doppelten Datenblöcke durch Referenzen auf deduplizierte Speicherbereiche ersetzt.

Für Speicherpools, die mit RECLAMATIONTYPE=SNAPLOCK definiert sind, löscht dieser Befehl auch leere WORM-FILE-Datenträger, die ihren Wiederherstellungszeitraum überschritten haben.

## Berechtigungsklasse

---

Um diesen Befehl auszugeben, benötigen Sie die Systemberechtigung, die uneingeschränkte Speicherberechtigung oder die eingeschränkte Speicherberechtigung für den Speicherpool, der wiederhergestellt wird, und den Wiederherstellungsspeicherpool, sofern zutreffend.

## Syntax

---

```
>>-RECLaim STGpool--Poolname--+-----+----->
                                     '-Threshold----Zahl-'
                                     .-Wait----No-----
>--+-----+----->
   '-Duration----Minuten-'   '-Wait-----+No--+-'
                                   '-Yes-'

>--+-----+-----<
   '-OFFSITERECLAIMLimit----Anzahl_Datenträger-'
```

## Parameter

---

Poolname (Erforderlich)

Gibt den Speicherpool an, in dem Datenträger wiederhergestellt werden sollen.

DURATION

Gibt die maximale Anzahl Minuten an, die die Wiederherstellung ausgeführt wird, bevor sie automatisch abgebrochen wird. Sie können eine Zahl von 1 bis 9999 angeben. Dieser Parameter ist wahlfrei.

Nachdem die angegebene Anzahl Minuten verstrichen ist, stoppt der Server den Wiederherstellungsprozess, wenn er den Prozess das nächste Mal überprüft. Der Server überprüft den Wiederherstellungsprozess, wenn er einen anderen auswählbaren Datenträger aus dem Speicherpool lädt, der wiederhergestellt wird. Außerdem überprüft der Server den Wiederherstellungsprozess, wenn er mit der Wiederherstellung eines neuen Stapels Dateien auf dem gegenwärtig geladenen Datenträger beginnt. Aus diesem Grund kann die Wiederherstellung länger dauern als mit dem Wert für diesen Parameter angegeben ist.

Bis zur Überprüfung des Wiederherstellungsprozesses durch den Server gibt es keinen Hinweis darüber, dass die Dauer abgelaufen ist. Wenn der Server den Wiederherstellungsprozess stoppt, gibt er die Nachricht ANR4927W aus:  
Wiederherstellung für Datenträger xxx beendet - Dauer überschritten.

Wenn Sie diesen Parameter nicht angeben, wird der Prozess nur gestoppt, wenn keine weiteren Datenträger dem Schwellenwert entsprechen.

Wird ein Wert für die Dauer der Wiederherstellung eines Kopierspeicherpools mit ausgelagerten Datenträgern angegeben, kann die Wiederherstellung beendet werden, bevor Datenträger wiederhergestellt werden. In den meisten Fällen sollte beim Einleiten der Wiederherstellung für einen Kopierspeicherpool mit ausgelagerten Datenträgern die Anzahl der ausgelagerten Datenträger, die wiederhergestellt werden sollen, und nicht die Dauer begrenzt werden. Ausführliche Informationen befinden sich in der Beschreibung des Parameters OFFSITERECLAIMLIMIT.

#### Threshold

Gibt den Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger an, mit dem der Datenträger für die Wiederherstellung auswählbar ist. Der wiederherstellbare Speicherbereich ist der Speicherbereich, der durch Dateien belegt ist, die verfallen sind oder aus der Serverdatenbank gelöscht wurden. Der wiederherstellbare Speicherbereich schließt auch freien Speicherbereich ein.

Sie können eine Zahl von 1 bis 99 angeben. Dieser Parameter ist wahlfrei. Falls nicht angegeben, wird das Attribut RECLAIM der Speicherpooldefinition verwendet.

Um den Prozentsatz des wiederherstellbaren Speicherbereichs für einen Datenträger zu bestimmen, geben Sie den Befehl QUERY VOLUME aus und geben Sie FORMAT=DETAILED an. Der Wert im Feld 'Wiederherstellbarer Speicher in %' ist der Prozentsatz des wiederherstellbaren Speicherbereichs für den Datenträger.

Geben Sie einen Wert von 50 Prozent oder höher für diesen Parameter an, so dass Dateien, die auf zwei Datenträgern gespeichert sind, auf einem einzigen Zieldatenträger gespeichert werden können.

#### OFFSITERECLAIMLimit

Gibt die maximale Anzahl ausgelagerter Speicherpooldatenträger an, die der Server wiederherzustellen versucht. Dieser Parameter ist nur für Kopierspeicherpools gültig. Sie können eine Zahl von 0 bis 99999 angeben. Dieser Parameter ist wahlfrei. Falls nicht angegeben, wird das Attribut OFFSITERECLAIMLIMIT der Speicherpooldefinition verwendet.

#### Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

##### No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet.

Sie können mit anderen Tasks fortfahren, während der Befehl verarbeitet wird. Nachrichten, die von dem Hintergrundprozess erstellt werden, werden entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Wird dieser Prozess abgebrochen, wurden möglicherweise bereits einige Dateien vor dem Abbruch auf neue Datenträger versetzt.

##### Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Ausgabenachrichten werden dem Verwaltungsclient angezeigt, wenn die Operation beendet ist. Nachrichten werden auch im Aktivitätenprotokoll und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.

Einschränkung: Sie können nicht WAIT=YES an der Serverkonsole angeben.

## Beispiel: Datenträger in einem Speicherpool mit sequenziellem Zugriff wiederherstellen

Datenträger in dem Speicherpool TAPEPOOL wiederherstellen. Angeben, dass die Wiederherstellung so schnell wie möglich nach 60 Minuten beendet werden soll.

```
reclaim stgpool tapepool duration=60
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RECLAIM STGPOOL

| Befehl          | Beschreibung  |
|-----------------|---|
| CANCEL PROCESS  | Bricht einen Serverhintergrundprozess ab.   |
| MIGRATE STGPOOL | Lagert Dateien aus einem primären Speicherpool in den nächsten Speicherpool in der Hierarchie um. |
| MOVE DRMEDIA    | Versetzt DRM-Datenträger vor Ort und lagert sie aus.  |
| QUERY DRMEDIA   | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.     |
| QUERY PROCESS   | Zeigt Informationen über Hintergrundprozesse an.  |
| QUERY STGPOOL   | Zeigt Informationen zu Speicherpools an.  |

## RECONCILE VOLUMES (Unterschiede abstimmen)

Diesen Befehl vom Quellen-Server ausgeben, um Unterschiede zwischen den Definitionen der virtuellen Datenträger auf dem Quellen-Server und den Archivierungsdateien auf dem Ziel-Server abzustimmen. IBM Spectrum Protect sucht alle Datenträger mit der angegebenen Einheitenklasse auf dem Quellen-Server und alle entsprechenden Archivierungsdateien auf dem Ziel-Server. Der Datenträgerbestand auf dem Ziel-Server wird auch mit der lokalen Definition für virtuelle Datenträger verglichen, um festzustellen, ob Inkonsistenzen vorhanden sind.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```

>>-REConcile Volumes-----*----->
                          '-Einheitenklassenname-'

.-Fix----No-----
>-----+----->
  '-Fix-----+No---+'
      '-Yes-'
  
```

### Parameter

#### Einheitenklassenname

Gibt den Einheitenklassennamen der virtuellen Datenträger an. Wird kein Name angegeben, werden alle virtuellen Datenträger von IBM Spectrum Protect abgestimmt. Dieser Parameter ist wahlfrei.

#### FIX

Gibt an, ob IBM Spectrum Protect versucht, die gefundenen Inkonsistenzen zu korrigieren. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

#### No

Gibt an, daß IBM Spectrum Protect keine Inkonsistenzen korrigiert.

#### Yes

Gibt an, daß IBM Spectrum Protect die folgenden Korrekturen vornimmt:

- Speicherpooldatenträger auf dem Quellen-Server, die auf dem Ziel-Server nicht gefunden werden, werden von IBM Spectrum Protect als nicht verfügbar markiert. Datenträger, die nur in der Datenträger-History gefunden werden, wie beispielsweise Datenbanksicherungen und Import- und Exportdatenträger, werden als inkonsistent gemeldet.
- Archivierungsdateien auf dem Ziel-Server, die nicht mit virtuellen Datenträgern auf dem Quellen-Server übereinstimmen, werden zum Löschen vom Ziel-Server markiert.

Die folgende Tabelle zeigt Details zu den Aktionen:

| FIX= | Auf dem Quellen-Server | Auf dem Ziel-Server | Aktion |
|------|------------------------|---------------------|--------|
|------|------------------------|---------------------|--------|

| FIX=   | Auf dem Quellen-Server      | Auf dem Ziel-Server  | Aktion   |
|--|-----------------------------|--|--|
| NO   | Datenträger vorhanden       | Keine Dateien vorhanden  | Fehler berichten   |
|  |                             | Dateien vorhanden, aber zum Löschen markiert                   |  |
|  |                             | Aktive Dateien vorhanden, aber Attribute stimmen nicht überein |  |
|  | Datenträger nicht vorhanden | Aktive Dateien vorhanden                                       | Fehler berichten   |
| Dateien vorhanden, aber zum Löschen markiert |                             | Keine.   |  |
| YES  | Datenträger vorhanden       | Keine Dateien vorhanden  | Fehler berichten<br><b>Speicherpooldatenträger:</b> Als nicht verfügbar markiert   |
|  |                             | Dateien vorhanden, aber zum Löschen markiert                   | Fehler berichten<br><b>Speicherpooldatenträger:</b> Stimmen die Attribute überein, sind die Dateien auf dem Ziel-Server erneut als aktiv zu markieren; die Datenträger auf dem Quellen-Server sind als nicht verfügbar zu markieren und es empfiehlt sich, ein AUDIT VOLUME durchzuführen, um die Daten zu prüfen. Stimmen die Attribute nicht überein, sind die Datenträger als nicht verfügbar zu markieren. |
|  |                             | Aktive Dateien vorhanden, aber Attribute stimmen nicht überein | Fehler berichten<br><b>Speicherpooldatenträger:</b> Als nicht verfügbar markieren und empfehlen, daß ein AUDIT VOLUME durchgeführt wird, um die Daten zu prüfen.   |
|  | Datenträger nicht vorhanden | Aktive Dateien vorhanden                                       | Dateien zum Löschen auf dem Ziel-Server markieren.   |
|  |                             | Dateien vorhanden, aber zum Löschen markiert                   | Keine.   |

## Beispiel: Abweichungen zwischen den Definitionen der virtuellen Datenträger abstimmen

Die Unterschiede zwischen allen Definitionen der virtuellen Datenträger auf dem Quellen-Server und den Archivierungsdateien auf dem Ziel-Server abstimmen, um alle Inkonsistenzen zu korrigieren.

```
reconcile volumes remotel fix=yes
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RECONCILE VOLUMES

| Befehl          | Beschreibung   |
|-----------------|--|
| DEFINE DEVCLASS | Definiert eine Einheitenklasse.                              |
| DEFINE SERVER   | Definiert einen Server für die Übertragung zwischen Servern. |
| DELETE SERVER   | Löscht die Definition eines Servers.                         |
| QUERY SERVER    | Zeigt Informationen über Server an.                          |
| UPDATE SERVER   | Aktualisiert Informationen über einen Server.                |

## REGISTER-Befehle

Mit den REGISTER-Befehlen können Objekte in IBM Spectrum Protect definiert oder hinzugefügt werden.

- REGISTER ADMIN (Administrator-ID registrieren)

- REGISTER LICENSE (Neue Lizenz registrieren)
- REGISTER NODE (Knoten registrieren)

## REGISTER ADMIN (Administrator-ID registrieren)

Verwenden Sie diesen Befehl, um dem Server einen Administrator hinzuzufügen. Nach der Registrierung kann der Administrator eine begrenzte Gruppe von Befehlen, einschließlich aller Abfragebefehle, ausgeben. Sollen weitere Berechtigungen zur Verfügung gestellt werden, verwenden Sie den Befehl GRANT AUTHORITY.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Wenn Sie einen Administrator mit dem Namen eines vorhandenen Knotens registrieren, beachten Sie die Authentifizierungsmethode des Administrators und die Einstellung für SSLREQUIRED. Jeder Knoten, der denselben Namen wie der Administrator hat, der registriert wird, übernimmt diese Einstellungen.

Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol):

- Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.
- Geben Sie keine Benutzer-ID mit Administratorberechtigung an, die mit einem Knotennamen identisch ist. Wenn die Benutzer-ID mit Administratorberechtigung mit dem Knotennamen übereinstimmt, stellen Sie möglicherweise ein nicht erwartetes Verhalten fest, weil automatische Kennwortänderungen dasselbe Kennwort zweimal aktualisieren. Dies hat zur Folge, dass das Kennwort für die Benutzer-ID mit Administratorberechtigung unbekannt ist. Es kann aber auch vorkommen, dass die Kennwortaktualisierungsoperation fehlschlägt.

### Syntax

```
>>-REGister Admin--Administratorname--+-----+----->
                                     '-Kennwort-'

>+-----+-----+-----+----->
| (1)          | '-CONTACT---Text-'
|-----PASSExp---Tage-|
. -FORCEPwreset---No-----
>+-----+-----+-----+----->
| '-FORCEPwreset---+No--+-'
|                   '-Yes-'

>+-----+-----+-----+----->
| '-EMAILAddress---Benutzer-ID@Knoten-'

      (2)
. -----AUTHentication---Local-.
>+-----+-----+-----+----->
| '-AUTHentication---+Local+---'
|                   '-LDap--'

      (3)
. -SSLrequired---Default-----
>+-----+-----+-----+----->
| '-SSLrequired---+Yes-----+-'
|                   +-No-----+
|                   '-Default-'

. -SESSIONSECurity---TRANSitional----
>+-----+-----+-----+----->
| '-SESSIONSECurity---+STRict-----+-'
|                   '-TRANSitional-'

. -ALert---No-----
>+-----+-----+-----+----->
| '-ALert---+Yes--+-'
|                   '-No--'
```

Anmerkungen:

1. Der Befehl PASSEXP gilt nicht für Administratoren, die sich mit einem LDAP-Verzeichnisserver authentifizieren.
2. Der Standardwert kann sich ändern, wenn Sie den Befehl SET DEFAULTAUTHENTICATION ausgegeben und LDAP angegeben haben.
3. Der Parameter SSLREQUIRED ist veraltet.

## Parameter

---

### Administratorname (Erforderlich)

Gibt den Namen des zu registrierenden Administrators an. Die maximale Länge des Namens beträgt 64 Zeichen.

Der Administratorname NONE darf nicht angegeben werden.

Soll die Administrator-ID mit einem LDAP-Server authentifiziert werden, stellen Sie sicher, dass die Administrator-ID nicht mit dem Namen eines Knotens übereinstimmt, der sich mit einem LDAP-Server authentifiziert.

### Kennwort

Gibt das Kennwort des zu registrierenden Administrators an. Das Kennwort darf maximal 64 Zeichen lang sein.

Wenn Sie Kennwörter lokal mit dem IBM Spectrum Protect-Server authentifizieren, müssen Sie ein Kennwort angeben. Bei dem Kennwort muss die Groß-/Kleinschreibung nicht beachtet werden.

Wenn Sie Kennwörter mit einem Lightweight Directory Access Protocol-Server (LDAP-Server) authentifizieren, geben Sie kein Kennwort im Befehl REGISTER ADMIN an.

### PASSExp

Gibt die Anzahl der Tage an, die das Kennwort gültig ist. Für die Kennwortablaufdauer kann ein Wert von 0 bis 9999 Tage definiert werden. Der Wert 0 bedeutet, dass das Kennwort niemals abläuft. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, wird das Kennwort mit der globalen Verfallsperiode von 90 Tagen definiert. Dieser Parameter hat keine Auswirkungen auf Kennwörter, die sich mit einem LDAP-Verzeichnisserver authentifizieren.

### CONtact

Liefert Informationen zum Administrator, der registriert wird. Dieser Parameter ist wahlfrei. Diese Zeichenfolge kann maximal 255 Zeichen lang sein. Die Kontaktinformationen müssen in Anführungszeichen eingeschlossen sein, falls Leerzeichen enthalten sind.

### FORCEPwreset

Gibt an, ob der Administrator das Kennwort ändern oder zurücksetzen muss. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

#### No

Gibt an, dass der Administrator bei dem Versuch, sich beim Server anzumelden, das Kennwort nicht ändern bzw. zurücksetzen muss.

#### Yes

Gibt an, dass das Kennwort des Administrators bei der nächsten Anmeldung abläuft. Der Client bzw. Administrator muss das Kennwort dann ändern oder zurücksetzen. Wird kein Kennwort angegeben, wird eine Fehlernachricht empfangen. Einschränkung: Für Benutzer-IDs mit Administratorberechtigung, die mit einem LDAP-Server authentifiziert werden, wird der Kennwortablauf mithilfe von LDAP-Serverdienstprogrammen definiert. Geben Sie daher nicht FORCEPWRESET=YES an, wenn Sie AUTHENTICATION=LDAP angeben.

### EMAILADdress

Gibt die E-Mail-Adresse für diesen Administrator an.

### AUTHentication

Dieser Parameter gibt die Authentifizierungsmethode für die Administrator-ID an. Geben Sie einen der folgenden Werte an: LDAP oder LOCAL. Der Parameter ist wahlfrei und nimmt standardmäßig den Wert LOCAL an. Der Standardwert kann sich in LDAP ändern, wenn Sie den Befehl SET DEFAULTAUTHENTICATION verwenden und LDAP angeben.

#### Local

Gibt an, dass die lokale IBM Spectrum Protect-Serverdatenbank verwendet wird.

#### LDap

Gibt an, dass die Administrator-ID Kennwörter mit einem LDAP-Verzeichnisserver authentifiziert. Bei Kennwörtern, die mit einem LDAP-Verzeichnisserver authentifiziert werden, muss die Groß-/Kleinschreibung beachtet werden.

Tipp: Ein Kennwort ist nicht erforderlich, wenn Sie einen Administrator registrieren und AUTHENTICATION=LDAP auswählen. Bei der Anmeldung werden Sie zur Eingabe eines Kennworts aufgefordert.

### SSLrequired (veraltet)

Gibt an, ob die Administrator-ID das Protokoll Secure Sockets Layer (SSL) für die Kommunikation zwischen dem IBM Spectrum Protect-Server und dem Client für Sichern/Archivieren verwenden muss. Wenn Sie Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren, müssen Sie die Sitzungen mit SSL oder einer anderen Netzsicherheitsmethode schützen.

Wichtig: Ab IBM Spectrum Protect Version 8.1.2 und Tivoli Storage Manager Version 7.1.8 wird dieser Parameter nicht mehr verwendet. Die durch diesen Parameter aktivierte Validierung wird durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter

SESSIONSECURITY durchgesetzt wird. Der Parameter SSLREQUIRED wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

#### SESSIONSECURITY

Gibt an, ob der Administrator die sichersten Einstellungen verwenden muss, um mit einem IBM Spectrum Protect-Server zu kommunizieren. Dieser Parameter ist wahlfrei.

Sie können einen der folgenden Werte angeben:

#### STRICT

Gibt an, dass die striktesten Sicherheitseinstellungen für den Administrator durchgesetzt werden. Der Wert STRICT verwendet das sicherste Kommunikationsprotokoll, das verfügbar ist. Dies ist derzeit TLS 1.2. Das TLS 1.2-Protokoll wird für SSL-Sitzungen zwischen dem Server und dem Administrator verwendet. Um anzugeben, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, lesen Sie die Informationen zur Clientoption SSL. Für die Verwendung des Werts STRICT müssen die folgenden Anforderungen erfüllt werden, um sicherzustellen, dass sich der Administrator mit dem Server authentifizieren kann:

- Der Administrator und der Server müssen IBM Spectrum Protect-Software verwenden, die den Parameter SESSIONSECURITY unterstützt.
- Der Administrator muss für die Verwendung des TLS 1.2-Protokolls für SSL-Sitzungen zwischen dem Server und dem Administrator konfiguriert werden.

Administratoren, für die der Wert STRICT definiert ist und die diese Anforderungen nicht erfüllen, können sich nicht mit dem Server authentifizieren.

#### TRANSITIONAL

Gibt an, dass die vorhandenen Sicherheitseinstellungen für den Administrator durchgesetzt werden. Dies ist der Standardwert. Dieser Wert ist für die temporäre Verwendung bestimmt, während Sie Ihre Sicherheitseinstellungen aktualisieren, um die Anforderungen für den Wert STRICT zu erfüllen.

Ist SESSIONSECURITY=TRANSITIONAL definiert und hat der Administrator nie die Anforderungen für den Wert STRICT erfüllt, authentifiziert sich der Administrator weiterhin mithilfe des Werts TRANSITIONAL. Wenn ein Administrator jedoch die Anforderungen für den Wert STRICT erfüllt, wird der Wert des Parameters SESSIONSECURITY automatisch von TRANSITIONAL in STRICT aktualisiert. Der Administrator kann sich dann nicht mehr mit einer Version des Clients oder mit einem SSL/TLS-Protokoll authentifizieren, die bzw. das die Anforderungen für STRICT nicht erfüllt. Nachdem sich ein Administrator erfolgreich mit einem Kommunikationsprotokoll authentifiziert hat, das mehr Sicherheit bietet, kann sich der Administrator nicht mehr mit einem weniger sicheren Protokoll authentifizieren. Beispiel: Wenn ein Administrator, der nicht SSL verwendet, aktualisiert wird und sich mithilfe von TLS 1.2 erfolgreich authentifiziert, kann sich der Administrator nicht mehr ohne SSL-Protokoll oder mithilfe von TLS 1.1 authentifizieren. Diese Einschränkung gilt auch bei Verwendung von Funktionen wie z. B. Befehlsweiterleitung oder Export zwischen Servern, wenn sich der Administrator beim IBM Spectrum Protect-Server als Administrator von einem anderen Server authentifiziert.

#### Alert

Gibt an, ob Alerts an die E-Mail-Adresse eines Administrators gesendet werden.

#### Yes

Gibt an, dass Alerts an die E-Mail-Adresse des angegebenen Administrators gesendet werden.

#### No

Gibt an, dass Alerts nicht an die E-Mail-Adresse des angegebenen Administrators gesendet werden. Dies ist der Standardwert.

Tipp: Die Alertüberwachung muss aktiviert sein und die E-Mail-Einstellungen müssen korrekt definiert sein, damit Alerts erfolgreich als E-Mail empfangen werden können. Um die aktuellen Einstellungen anzuzeigen, geben Sie den Befehl QUERY MONITORSETTINGS aus.

## Beispiel: Einen Administrator registrieren

---

Den Administrator LARRY mit dem Kennwort PASSONE definieren. LARRY kann als Mitarbeiter der zweiten Schicht gekennzeichnet werden, indem diese Information im Parameter CONTACT angegeben wird. Den folgenden Befehl ausgeben:

```
register admin larry passone contact='zweite schicht'
```

## Beispiel: Eine Administrator-ID registrieren und die Authentifizierungsmethode definieren

---

Eine Administrator-ID für Harry definieren, damit sich Harry mit einem LDAP-Server authentifizieren kann. Den folgenden Befehl ausgeben:

```
register admin harry authentication=ldap
```



## Beispiel: Einen Administrator registrieren und die Sitzungssicherheit 'strict' durchsetzen

Einen Administrator mit dem Namen Harry registrieren und von Harry verlangen, dass er die striktesten Sicherheitseinstellungen verwendet, um sich mit dem Server zu authentifizieren. Den folgenden Befehl ausgeben:

```
register admin harry sessionsecurity=strict
```

## Zugehörige Befehle


Tabelle 1. Zugehörige Befehle für REGISTER ADMIN

| Befehl   | Beschreibung  |
|--|---|
| GRANT AUTHORITY  | Ordnet einem Administrator Berechtigungsklassen zu.   |
| LOCK ADMIN   | Verweigert einem Administrator den Zugriff auf IBM Spectrum Protect.                                      |
| QUERY ADMIN  | Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.                    |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen) | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.          |
| REGISTER NODE  | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.                   |
| REMOVE ADMIN   | Löscht einen Administrator aus der Liste der registrierten Administratoren.                               |
| RENAME ADMIN   | Ändert den Namen eines IBM Spectrum Protect-Administrators.   |
| SET DEFAULTAUTHENTICATION  | Gibt die Standardkennwortauthentifizierungsmethode für alle Befehle REGISTER NODE oder REGISTER ADMIN an. |
| SET PASSEXP  | Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.                        |
| UNLOCK ADMIN   | Ermöglicht einem gesperrten Administrator den Zugriff auf IBM Spectrum Protect.                           |
| UPDATE ADMIN   | Ändert das Kennwort eines Administrators bzw. die zu einem Administrator gehörigen Kontaktinformationen.  |
| UPDATE NODE  | Ändert die Attribute, die einem Clientknoten zugeordnet sind.   |

### Zugehörige Tasks:

Tivoli Storage Manager-Objekte benennen

### Zugehörige Verweise:

 Ssl (Clientoption)

## REGISTER LICENSE (Neue Lizenz registrieren)

Verwenden Sie diesen Befehl, um neue Lizenzen für Serverkomponenten zu registrieren, einschließlich IBM Spectrum Protect (Basis), IBM Spectrum Protect Extended Edition und IBM Spectrum Protect for Data Retention.

Lizenzen werden in Registrierungszertifikatsdateien gespeichert. Die Registrierungszertifikatsdateien enthalten Lizenzinformationen für das Serverprodukt. In der NODELOCK-Datei werden die Lizenzinformationen für Ihre Installation aufbewahrt. Ihre Lizenzvereinbarung bestimmt, welche Komponenten Sie verwenden dürfen, auch wenn Sie den Befehl REGISTER LICENSE nicht verwenden können, um alle Komponenten zu registrieren. Es wird erwartet, dass Sie die Lizenzvereinbarung einhalten und nur die Komponenten verwenden, die Sie gekauft haben. Die Verwendung des Befehls REGISTER LICENSE impliziert, dass Sie den Lizenzbedingungen zustimmen und Sie die Lizenzbedingungen akzeptieren, die in Ihrer Lizenzvereinbarung angegeben sind.

Wichtig:

- Bevor Sie ein Upgrade von einer vorherigen Version von IBM Spectrum Protect durchführen, müssen Sie die NODELOCK-Datei löschen oder umbenennen.
- Um die Registrierung von Lizenzen zurückzunehmen, müssen Sie die NODELOCK-Datei im Serverinstanzverzeichnis Ihrer Installation löschen und alle zuvor registrierten Lizenzen erneut registrieren.
- Sie können keine Lizenzen für IBM Spectrum Protect for Mail, IBM Spectrum Protect for Databases, IBM Spectrum Protect for ERP und IBM Spectrum Protect for Space Management registrieren.

Um einen Bericht zu erstellen, der Ihnen hilft, die Lizenzvoraussetzungen für Ihr System zu bestimmen, führen Sie den Befehl QUERY PVUESTIMATE aus. Der Bericht enthält Schätzungen der Anzahl von Clienteinheiten und PVU-Summen für Servereinheiten. Die Schätzungen sind rechtlich nicht bindend.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-REGister LICense--FILE-----+tsmbasic.lic+-----><
                                     +-tsmee.lic----+
                                     +-dataret.lic--+
                                     '-*.lic-----'
```

## Parameter

### FILE

Gibt den Namen der Registrierungszertifikatsdatei an, die die zu registrierende Lizenz enthält. Die Angabe kann ein Platzhalterzeichen (\*) enthalten. Geben Sie den vollständigen Dateinamen oder anstelle des Dateinamens ein Platzhalterzeichen ein. Bei den Dateinamen muß die Groß-/Kleinschreibung berücksichtigt werden. Die folgenden Werte können verwendet werden:

tsmbasic.lic

Zum Lizenzieren von IBM Spectrum Protect (Basis).

tsmee.lic

Zum Lizenzieren von IBM Spectrum Protect Extended Edition. Dazu gehören Disaster Recovery Manager, große Kassettenarchive und NDMP.

dataret.lic

Zum Lizenzieren von IBM Spectrum Protect for Data Retention. Diese Lizenz ist erforderlich, um den Aufbewahrungsschutz für Daten (Data Retention Protection) sowie die Aussetzung der Verfallsverarbeitung und des Löschens (Status "Löschen unzulässig") zu aktivieren.

\*.lic

Zum Lizenzieren aller IBM Spectrum Protect-Lizenzen für Serverkomponenten.

## Beispiel: Eine Lizenz registrieren

Die IBM Spectrum Protect-Basislizenz registrieren.

```
register license file=tsmbasic.lic
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für REGISTER LICENSE

| Befehl                 | Beschreibung   |
|------------------------|--|
| AUDIT LICENSES         | Prüft die Einhaltung der definierten Lizenzen.   |
| QUERY LICENSE          | Zeigt Informationen über Lizenzen und Prüfvorgänge an.   |
| QUERY PVUESTIMATE      | Zeigt Prozessor-Value-Unit-Schätzungen an.   |
| QUERY STATUS           | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| SET LICENSEAUDITPERIOD | Gibt die Anzahl Tage zwischen den automatischen Lizenzprüfungen an.  |

## REGISTER NODE (Knoten registrieren)

Verwenden Sie diesen Befehl, um einen Knoten für den Server zu registrieren.

Dieser Befehl kann eine Benutzer-ID mit Administratorberechtigung erstellen, die über Clienteignerberechtigung für den Knoten verfügt. Mit dieser Benutzer-ID mit Administratorberechtigung kann von fernen Standorten über einen Web-Browser auf den Web-Client für Sichern/Archivieren zugegriffen werden.

Tipp:

- In früheren Produktreleases erstellte der Befehl REGISTER NODE automatisch eine Benutzer-ID mit Administratorberechtigung, deren Name mit dem Knotennamen übereinstimmte. Ab IBM Spectrum Protect Version 8.1 erstellt der Befehl REGISTER NODE nicht automatisch eine Benutzer-ID mit Administratorberechtigung, deren Name mit dem Knotennamen übereinstimmt.
- Wenn Sie die Verwendung der LAN-unabhängigen Option mit diesem Knoten planen, müssen Sie eine Administrator-ID registrieren, die mit dem Knotennamen übereinstimmt. Um die Administrator-ID zu registrieren, verwenden Sie den Parameter USERID oder registrieren Sie manuell den Administrator und erteilen Sie dem Knoten die Eigenerberechtigung.

Benötigt ein Client eine andere als die Maßnahmendomäne STANDARD, muss der Clientknoten mit diesem Befehl registriert oder der registrierte Knoten aktualisiert werden.

Voraussetzung: Wenn Sie `sslrequired=serveronly` in einem Befehl REGISTER NODE definieren, wird die Einstellung für SSLREQUIRED für den Administrator auf YES zurückgesetzt. Soll eine Nicht-SSL-Sitzung mit einem Speicheragenten verwendet werden, benennen Sie den Administrator mit dem identischen Namen um, indem Sie den Befehl RENAME ADMIN ausgeben.

Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol): Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.

Wenn Sie einen Knoten registrieren oder aktualisieren, können Sie angeben, ob beschädigte Dateien auf dem Knoten von einem Replikationsserver wiederhergestellt werden können. Dateien können nur wiederhergestellt werden, wenn alle folgenden Bedingungen erfüllt sind:

- Version 7.1.1 oder höher ist auf dem Quellen- und Zielreplikationsserver installiert.
- Der Systemparameter REPLRECOVERDAMAGED ist auf ON gesetzt. Der Systemparameter kann mit dem Befehl SET REPLRECOVERDAMAGED definiert werden.
- Der Quellenserver schließt mindestens eine Datei ein, die auf dem Knoten, der repliziert wird, als beschädigt markiert ist.
- Die Knotendaten wurden repliziert, bevor die Beschädigung aufgetreten ist.

In der folgenden Tabelle wird beschrieben, wie sich Parametereinstellungen auf die Wiederherstellung beschädigter, replizierter Dateien auswirken.

Tabelle 1. Einstellungen, die sich auf die Wiederherstellung beschädigter Dateien auswirken

| Einstellung für den Systemparameter REPLRECOVERDAMAGED | Wert des Parameters RECOVERDAMAGED im Befehl REPLICATE NODE | Wert des Parameters RECOVERDAMAGED in den Befehlen REGISTER NODE und UPDATE NODE | Ergebnis  |
|--|---|--|---|
| OFF  | YES, NO oder nicht angegeben                                | YES oder NO  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.    |
| OFF  | ONLY  | YES oder NO  | Eine Fehlernachricht wird angezeigt, weil Dateien nicht wiederhergestellt werden können, wenn der Systemparameter REPLRECOVERDAMAGED auf OFF gesetzt ist. |
| ON   | YES   | YES oder NO  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.          |
| ON   | NO  | YES oder NO  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.    |
| ON   | ONLY  | YES oder NO  | Beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt, aber es findet keine Standardknotenreplikation statt.                            |
| ON   | Nicht angegeben   | YES  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.          |
| ON   | Nicht angegeben   | NO   | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.    |







übereinstimmen. Kennwörter, die von Knoten und Administratoren mit denselben Namen gemeinsam genutzt werden, bleiben bei einer Authentifizierungsänderung synchronisiert.

Wenn Sie die Verwendung der LAN-unabhängigen Option mit diesem Knoten planen, verwenden Sie den Parameter USERID, um eine Administrator-ID zu registrieren, die mit dem Knotennamen übereinstimmt.

Für Benutzer von LDAP-Servern: Soll der Knoten mit einem LDAP-Server authentifiziert werden, behalten Sie die Standardeinstellung (USERID=NONE) bei oder geben Sie eine Benutzer-ID mit Administratorberechtigung an, die sich vom Knotennamen unterscheidet. Wenn die Benutzer-ID mit Administratorberechtigung mit dem Knotennamen übereinstimmt, stellen Sie möglicherweise ein nicht erwartetes Verhalten fest, weil automatische Kennwortänderungen dasselbe Kennwort zweimal aktualisieren. Dies hat zur Folge, dass das Kennwort für die Benutzer-ID mit Administratorberechtigung unbekannt ist. Es kann aber auch vorkommen, dass die Kennwortaktualisierungsoperation fehlschlägt.

#### CONtact

Gibt eine Informationszeichenfolge an, die den Knoten identifiziert. Der Parameter ist wahlfrei. Die maximale Länge der Zeichenfolge beträgt 255 Zeichen. Die Kontaktinformationen müssen in Anführungszeichen eingeschlossen sein, falls Leerzeichen enthalten sind.

#### DOmain

Gibt den Namen der Maßnahmendomäne an, der der Knoten zugeordnet ist. Der Parameter ist wahlfrei. Wird kein Maßnahmendomänenname angegeben, wird der Knoten der Standardmaßnahmendomäne (STANDARD) zugeordnet.

Wenn ein Quellenserver als Knoten registriert wird, wird er einer Maßnahmendomäne zugeordnet. Daten vom Quellenserver werden in dem Speicherpool gespeichert, der in der Archivierungskopiengruppe der Standardverwaltungsklasse dieser Domäne angegeben ist.

#### COMPression

Gibt an, ob der Clientknoten seine Dateien komprimiert, bevor diese Dateien zum Sichern und Archivieren an den Server gesendet werden. Der Parameter ist wahlfrei. Der Standardwert ist CLIENT.

Einschränkung: Dieser Parameter gilt nicht für Knoten mit dem Typ NAS oder SERVER.

Sie können einen der folgenden Werte angeben:

##### Client

Gibt an, dass der Client festlegt, ob Dateien komprimiert werden.

##### Yes

Gibt an, dass der Clientknoten seine Dateien komprimiert, bevor diese Dateien zum Sichern und Archivieren an den Server gesendet werden.

##### No

Gibt an, dass der Clientknoten seine Dateien nicht komprimiert, bevor diese Dateien zum Sichern und Archivieren an den Server gesendet werden.

#### ARCHDElete

Gibt an, ob der Clientknoten seine eigenen Archivierungsdateien aus dem Server löschen darf. Der Parameter ist wahlfrei. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

##### Yes

Gibt an, dass der Clientknoten seine eigenen Archivierungsdateien aus dem Server löschen darf.

##### No

Gibt an, dass der Clientknoten seine eigenen Archivierungsdateien nicht aus dem Server löschen darf.

#### BACKDElete

Gibt an, ob der Clientknoten seine eigenen Sicherungsdateien aus dem Server löschen darf. Der Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

##### No

Gibt an, dass der Clientknoten seine eigenen Sicherungsdateien nicht aus dem Server löschen darf.

##### Yes

Gibt an, dass der Clientknoten seine eigenen Sicherungsdateien aus dem Server löschen darf.

#### CLOptset

Gibt den Namen der Optionsgruppe an, die der Client verwenden soll. Der Parameter ist wahlfrei.

#### FORCEPwreset

Gibt an, ob ein Client zum Ändern oder Zurücksetzen des Kennworts gezwungen werden soll. Der Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

##### No

Gibt an, dass die Kennwortablaufdauer über den Befehl SET PASSEXP definiert wird. Der Client muss das Kennwort nicht ändern oder zurücksetzen, während er sich beim Server anmeldet.

##### Yes

Gibt an, dass das Kennwort des Clientknotens bei der nächsten Anmeldung abläuft. Der Client muss das Kennwort dann ändern oder zurücksetzen. Wird kein Kennwort angegeben, wird eine Fehlernachricht empfangen.

Einschränkung: Für Knoten, die mit einem LDAP-Server authentifiziert werden, wird der Kennwortablauf mithilfe von LDAP-Serverdienstprogrammen definiert. Geben Sie daher nicht FORCEPWRESET=YES an, wenn Sie AUTHENTICATION=LDAP angeben.

#### Type

Gibt den Typ des Knotens an, der registriert wird. Der Parameter ist wahlfrei. Der Standardwert ist CLIENT. Sie können einen der folgenden Werte angeben:

##### Client

Gibt an, dass der Clientknoten ein Client für Sichern/Archivieren, ein IBM Spectrum Protect for Space Management-Client oder ein Anwendungsclient ist.

##### NAS

Gibt an, dass der Knoten ein NAS-Dateiserver ist, dessen Daten durch NDMP-Operationen geschützt werden. Der Knotenname darf nicht SERVER lauten.

Anmerkung: Der Name des NAS-Knotens muss mit dem Namen der Einheit zum Versetzen von Daten übereinstimmen. Aus diesem Grund kann der Name nicht geändert werden, nachdem eine entsprechende Einheit zum Versetzen von Daten definiert wurde.

##### Server

Gibt an, dass der Clientknoten ein Quellenserver ist, der auf dem Zielsystem registriert wird.

#### URL

Gibt die URL des IBM Spectrum Protect-Web-Clients an, die auf dem Clientsystem konfiguriert ist. Sie können die URL in einem Web-Browser und im Operations Center verwenden, um den Clientknoten über Fernzugriff zu verwalten.

Dieser Parameter ist wahlfrei. Die URL muss den DNS-Namen oder die IP-Adresse des Clientsystems und die Anschlussnummer enthalten, die auf dem Clientsystem für den IBM Spectrum Protect-Web-Client definiert ist. Beispiel:

`http://client.mycorp.com:1581`

#### UTILITYUrl

Gibt die Adresse der IBM Spectrum Protect-Clientverwaltungsservices an, die auf dem Clientsystem konfiguriert sind. Diese URL wird vom Operations Center verwendet, um auf Clientprotokolldateien zuzugreifen, sodass Sie im Operations Center Clientprobleme über Fernzugriff diagnostizieren können.

Dieser Parameter ist wahlfrei. Sie können eine URL mit maximal 200 Zeichen angeben. Die URL muss mit `https` beginnen. Sie enthält den DNS-Namen oder die IP-Adresse des Clientsystems und die Anschlussnummer, die auf dem Clientsystem für die IBM Spectrum Protect-Clientverwaltungsservices definiert ist. Beispiel: `https://client.mycorp.com:9028`

Wird keine Anschlussnummer angegeben, verwendet das Operations Center die Anschlussnummer 9028. Dies ist die Standardanschlussnummer, wenn Sie die Clientverwaltungsservices auf dem Clientsystem installieren.

#### MAXNUMMP

Gibt die maximale Anzahl der Mountpunkte an, die ein Knoten nur für Operationen, wie beispielsweise Sicherung, Archivierung und IBM Spectrum Protect for Space Management-Umlagerung, auf dem Server oder dem Speicheragenten verwenden darf. Der Parameter ist optional und gilt nicht für Knoten mit dem Typ NAS oder SERVER. Der Standardwert ist 1. Sie können eine ganze Zahl im Bereich von 0 bis 999 angeben. Der Wert 0 gibt an, dass ein Knoten keinen Mountpunkt für eine Operation zum Speichern von Clientdaten anfordern kann. Der MAXNUMMP-Wert wird während der Operationen zum Lesen von Clientdaten, wie beispielsweise Zurückschreiben, Abrufen und Zurückrufen durch IBM Spectrum Protect for Space Management, nicht ausgewertet oder umgesetzt. Mountpunkte, die für Operationen zum Lesen von Daten verwendet werden, werden jedoch in Bezug auf versuchte gleichzeitig ablaufende Datenspeicherungsoperationen für denselben Clientknoten ausgewertet und können verhindern, dass die Datenspeicherungsoperationen Mountpunkte anfordern können.

Für Datenträger in einem Speicherpool, dem der Einheitentyp FILE oder CENTERA zugeordnet ist, kann der Server über mehrere Sitzungen verfügen, um gleichzeitig denselben Datenträger zu lesen, und über eine Sitzung verfügen, um auf diesen Datenträger zu schreiben. Um den gemeinsamen Zugriff zu erweitern und einen effizienten Zugriff für Knoten mit Daten in Speicherpools des Typs FILE oder CENTERA zur Verfügung zu stellen, erhöhen Sie den Wert des Parameters MAXNUMMP.

Für Knoten, die mit aktivierter Funktion für simultanes Schreiben Daten in primären Speicherpools speichern, müssen Sie den Wert des Parameters MAXNUMMP anpassen, um die korrekte Anzahl der Mountpunkte für jede Clientsitzung anzugeben. Eine Clientsitzung erfordert einen Mountpunkt für den primären Speicherpool und einen Mountpunkt für jeden Kopierspeicherpool und jeden Pool für aktive Daten.

Hat ein Server bei der serverübergreifenden Sicherung eine andere Version als der andere Server, setzen Sie die Anzahl der Mountpunkte auf dem Zielsystem auf einen höheren Wert als 1. Andernfalls wird eine Fehlernachricht ausgegeben.

Ein Speicheragent verfolgt unabhängig die Anzahl der Mountpunkte, die während einer Clientsitzung verwendet werden. Ist auf einem Knoten ein Speicheragent installiert, kann der Wert für MAXNUMMP überschritten werden. Der Wert für MAXNUMMP kann



auch unter Bedingungen überschritten werden, bei denen der Knoten nicht auf einen Mountpunkt warten muss.

Anmerkung: Der Server kann der Operation eines Clients eine Operation mit höherer Priorität vorziehen, und der Client kann einen Mountpunkt verlieren, wenn keine anderen Mountpunkte verfügbar sind.

#### KEEPMP

Gibt an, ob der Clientknoten den Mountpunkt für die gesamte Sitzung beibehält. Der Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

##### Yes

Gibt an, dass der Clientknoten den Mountpunkt während der gesamten Sitzung beibehalten muss. Haben Maßnahmendefinitionen zur Folge, dass Daten in einem Plattenspeicherpool gespeichert werden, nachdem die Daten in einem Speicherpool mit sequenziellem Zugriff gespeichert wurden, werden alle von der Sitzung belegten Mountpunkte nicht freigegeben.

##### No

Gibt an, dass der Clientknoten den Mountpunkt während der Sitzung freigibt. Haben Maßnahmendefinitionen zur Folge, dass Daten in einem Plattenspeicherpool gespeichert werden, nachdem die Daten in einem Speicherpool mit sequenziellem Zugriff gespeichert wurden, werden alle von der Sitzung belegten Mountpunkte freigegeben.

#### AUTOFSRename

Geben Sie an, ob Dateibereiche automatisch umbenannt werden, wenn ein Upgrade des Clientsystems zur Unterstützung von Unicode durchgeführt wird, oder geben Sie an, ob Dateibereiche bei Bedarf vom Client umbenannt werden. Der Parameter ist wahlfrei. Der Standardwert ist NO. Wird der Parameter auf YES gesetzt, wird das automatische Umbenennen aktiviert. Das automatische Umbenennen findet statt, wenn der Client eine der folgenden Operationen ausführt: Archivierung, selektive Sicherung, vollständige Teilsicherung oder partielle Teilsicherung. Beim automatischen Umbenennen werden die Namen von bestehenden gesicherten Dateibereichen, die nicht in Unicode sind, im Serverspeicher geändert. Anschließend werden die Dateibereiche in Unicode gesichert. Sie können diesen Parameter für Unicode-fähige IBM Spectrum Protect-Clients mit den Betriebssystemen Windows, Macintosh OS X und NetWare verwenden.

Nachdem der Client mit Unterstützung für Unicode installiert wurde, werden alle neuen Dateibereiche, die der Client sichert, im Serverspeicher mit der Zeichenumsetztabelle UTF-8 gespeichert. UTF-8 ist eine byte-orientierte Verschlüsselungsform, die durch den Unicode Standard angegeben wird.

Sie können einen der folgenden Werte angeben:

##### Yes

Vorhandene Dateibereiche werden automatisch umbenannt, wenn ein Upgrade auf einen Client durchgeführt wird, der Unicode unterstützt, und der Client eine der folgenden Operationen ausführt: Archivierung, selektive Sicherung, vollständige Teilsicherung oder partielle Teilsicherung. Das Umbenennen findet statt, wenn der Client die grafische Benutzerschnittstelle, die Befehlszeile oder den Client-Scheduler verwendet. Beispielsweise wird ein Laufwerk vom Server wie folgt umbenannt:

```
Ursprünglicher Name: D_DRIVE  
Neuer Name: D_DRIVE_OLD
```

Der neue Name gibt an, dass der Dateibereich auf dem Server in einem Format gespeichert wird, das kein Unicode ist.

##### No

Vorhandene Dateibereiche werden nicht automatisch umbenannt, wenn für das Clientsystem ein Upgrade auf einen Client erfolgt, der Unicode unterstützt, und der Client eine der folgenden Operationen ausführt: Archivieren, selektive Sicherung, vollständige Teilsicherung oder partielle Teilsicherung.

##### Client

Die Option AUTOFSRENAME in der Optionsdatei des Clients bestimmt, ob Dateibereiche umbenannt werden.

Standardmäßig ist die Clientoption auf PROMPT gesetzt. Wenn für das Clientsystem ein Upgrade auf einen Client erfolgt, der Unicode unterstützt, und der Client eine IBM Spectrum Protect-Operation mit der grafischen Benutzerschnittstelle oder der Befehlszeile ausführt, zeigt das Programm dem Benutzer einmalig eine Bedienungsführung an und fordert den Benutzer zur Angabe auf, ob Dateibereiche umbenannt werden sollen.

Wenn der Client-Scheduler eine Operation ausführt, fordert das Programm nicht zur Angabe einer Auswahl für das Umbenennen auf, und es werden keine Dateibereiche umbenannt. Sicherungen von vorhandenen Dateibereichen werden wie zuvor gesendet (nicht in Unicode).

#### VALIDateprotocol (veraltet)

Gibt an, ob IBM Spectrum Protect eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) ausführt, um die Daten zu validieren, die zwischen dem Client und dem Server gesendet werden. Der Parameter ist wahlfrei. Der Standardwert ist NO. Wichtig: Ab IBM Spectrum Protect Version 8.1.2 und Tivoli Storage Manager Version 7.1.8 wird dieser Parameter nicht mehr verwendet. Die durch diesen Parameter aktivierte Validierung wird durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter SESSIONSECURITY durchgesetzt wird. Der Parameter VALIDATEPROTOCOL wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

## TXNGroupmax

Gibt die Anzahl der Dateien pro Transaktions-COMMIT an, die zwischen einem Client und einem Server übertragen werden. Der Parameter ist wahlfrei. Die Clientleistung kann verbessert werden, indem ein höherer Wert für diese Option verwendet wird.

Der Standardwert ist 0. Der Wert 0 gibt an, dass der Knoten den globalen Serverwert verwendet, der in der Serveroptionsdatei definiert ist. Soll ein anderer Wert als der globale Serverwert verwendet werden, geben Sie einen Wert von 4 bis 65.000 für diesen Parameter an. Der Knotenwert hat Vorrang vor dem Serverwert.

Achtung: Die Vergrößerung des Werts für TXNGROUPMAX führt zu einer Erhöhung der Auslastung des Wiederherstellungsprotokolls. Eine höhere Auslastung des Wiederherstellungsprotokolls kann das Risiko erhöhen, dass der Protokollspeicherbereich nicht mehr ausreicht. Werten Sie die Leistung jedes Knotens aus, bevor Sie den Parameter ändern.

## DATAWritepath

Gibt den Übertragungspfad an, der verwendet wird, wenn der Client während Speicheroperationen (Sicherung oder Archivierung) Daten an den Server und/oder den Speicheragenten sendet. Der Parameter ist wahlfrei. Der Standardwert ist ANY.

Anmerkung: Ist kein Pfad verfügbar, kann der Knoten keine Daten senden. Wenn Sie z. B. die LAN-unabhängige Option auswählen, aber kein LAN-unabhängiger Pfad definiert ist, schlägt die Operation fehl.

Sie können einen der folgenden Werte angeben:

### ANY

Gibt an, dass Daten über einen beliebigen verfügbaren Pfad an den Server und/oder Speicheragenten gesendet werden. Ein LAN-unabhängiger Pfad wird verwendet, wenn einer verfügbar ist. Ist kein LAN-unabhängiger Pfad verfügbar, werden die Daten über das LAN übertragen.

### LAN

Gibt an, dass Daten über das LAN gesendet werden.

### LANFree

Gibt an, dass Daten über einen LAN-unabhängigen Pfad gesendet werden.

## DATAReadpath

Gibt den Übertragungspfad an, der verwendet wird, wenn der Server und/oder Speicheragent während Operationen wie Zurückschreiben oder Abrufen Daten für einen Client lesen. Der Parameter ist wahlfrei. Der Standardwert ist ANY.

Anmerkung: Ist kein Pfad verfügbar, können keine Daten gelesen werden. Wenn Sie z. B. die LAN-unabhängige Option auswählen, aber kein LAN-unabhängiger Pfad definiert ist, schlägt die Operation fehl. Der Wert für den Übertragungspfad gilt auch für Übernahmeverbindungen. Wird der Wert auf LANFree gesetzt, kann für den Knoten auf dem sekundären Server keine Übernahme erfolgen.

Sie können einen der folgenden Werte angeben:

### ANY

Gibt an, dass der Server und/oder Speicheragent einen beliebigen verfügbaren Pfad verwenden, um Daten zu lesen. Ein LAN-unabhängiger Pfad wird verwendet, wenn einer verfügbar ist. Ist kein LAN-unabhängiger Pfad verfügbar, werden die Daten über das LAN gelesen.

### LAN

Gibt an, dass Daten über das LAN gelesen werden.

### LANFree

Gibt an, dass Daten über einen LAN-unabhängigen Pfad gelesen werden.

## TARGETLevel

Gibt das Clientimplementierungspaket für diesen Knoten an. Für V.R.M.F (Version.Release.Modifikation.Fix-Level) kann ein gültiges Releasepaket angegeben werden. Beispiel: `TARGETLevel=6.2.0.0`.

Sie müssen jedes Segment mit einer Zahl angeben, die für ein Implementierungspaket zutreffend ist. Sie können keinen Stern in einem Feld als Ersetzung für eine gültige Zahl verwenden. Der Parameter ist wahlfrei.

Einschränkung: Der Parameter TARGETLEVEL gilt nicht für Knoten mit dem Typ NAS oder SERVER.

## SESSIONInitiation

Steuert, ob der Server oder der Client Sitzungen einleitet. Der Standardwert gibt an, dass der Client Sitzungen einleitet. Der Parameter ist wahlfrei.

### Clientorserver

Gibt an, dass der Client Sitzungen mit dem Server einleiten kann, indem über den TCP/IP-Anschluss kommuniziert wird, der mit der Serveroption TCPPOINT definiert wird. Die Zeitplanung über Serversystemanfrage kann ebenfalls verwendet werden, um den Client aufzufordern, eine Verbindung zum Server herzustellen.

### SERVEROnly

Gibt an, dass der Server keine Clientanforderungen für Sitzungen akzeptiert. Alle Sitzungen müssen durch die Zeitplanung über Serversystemanfrage an dem Anschluss eingeleitet werden, der mit dem Befehl REGISTER oder UPDATE NODE für

den Client definiert wird. Sie können den Clientakzeptor (dsmcad) nicht verwenden, um den Scheduler zu starten, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist.

#### HLAddress

Gibt die Client-IP-Adresse an, die der Server anspricht, um geplante Ereignisse einzuleiten. Dieser Parameter muss verwendet werden, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist, unabhängig von den Adressen, die zuvor vom Client verwendet wurden, um den Server anzusprechen.

Die Adresse kann entweder im numerischen Format oder im Hostnamenformat angegeben werden. Wird eine numerische Adresse verwendet, wird sie ohne Prüfung durch einen Domänennamensserver gesichert. Ist die Adresse nicht korrekt, kann dies zu Fehlern führen, wenn der Server versucht, den Client anzusprechen. Adressen im Hostnamenformat werden mit einem Domänennamensserver geprüft. Geprüfte Namen werden mit Domänennamensservices (Domain Name Services) gesichert und aufgelöst, wenn der Server den Client anspricht.

#### LLAddress

Gibt die Clientanschlussnummer an, an der der Client für Sitzungen von dem Server empfangsbereit ist. Dieser Parameter muss verwendet werden, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist, unabhängig von den Adressen, die zuvor vom Client verwendet wurden, um den Server anzusprechen.

Der Wert für diesen Parameter muss mit dem Wert der Clientoption TCPCLIENTPORT übereinstimmen. Der Standardwert ist 1501.

#### EMAILAddress

Dieser Parameter wird für weitere Kontaktinformationen verwendet. Der Parameter ist wahlfrei. Die mit diesem Parameter angegebenen Informationen werden von IBM Spectrum Protect nicht verwendet.

#### DEDUPLICATION

Gibt an, wo die Dateneduplizierung für diesen Knoten stattfinden kann. Der Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

##### Clientorserver

Gibt an, dass von diesem Knoten gespeicherte Daten entweder auf dem Client oder auf dem Server dedupliziert werden können. Dieser Wert ist der Standardwert. Um die Dateneduplizierung auf dem Client auszuführen, müssen Sie auch den Wert YES für die Clientoption DEDUPLICATION angeben. Sie können diese Option in der Clientoptionsdatei oder in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server angeben.

##### SERVEROnly

Gibt an, dass von diesem Knoten gespeicherte Daten nur auf dem Server dedupliziert werden können.

#### BACKUPINITiation

Gibt an, ob die ID eines Benutzers ohne Rootberechtigung auf dem Clientknoten Dateien auf dem Server sichern kann. Der Parameter ist wahlfrei. Der Standardwert ALL gibt an, dass IDs der Benutzer ohne Rootberechtigung Daten auf dem Server sichern können. Sie können einen der folgenden Werte auswählen:

##### All

Gibt an, dass die IDs der Benutzer ohne Rootberechtigung Dateien auf dem Server sichern können. ALL ist der Standardwert, wenn BACKUPINITIATION nicht angegeben wird.

##### ROOT

Gibt an, dass die Rootbenutzer-ID Dateien auf dem Server sichern kann. Wenn Sie den Client für Sichern/Archivieren der Version 6.4 oder höher verwenden, haben berechtigte Benutzer dieselben Berechtigungen wie die Rootbenutzer-ID. Einschränkung: Das Attribut wird vom Server ignoriert, wenn der Client für Sichern/Archivieren eine Verbindung von einem anderen Betriebssystem als AIX, Linux, Solaris oder Mac OS herstellt. Hinweis: Die Anwendungsprogrammierschnittstelle (API) ist von dem Parameter BACKUPINITIATION auf dem Server betroffen. Standardmäßig dürfen alle API-Benutzer Daten sichern. Es wird nicht empfohlen, den Parameter auf einem API-Knoten auf ROOT zu setzen.

#### REPLState

Gibt an, ob Daten, die zu dem Clientknoten gehören, für die Replikation bereit sind. Dieser Parameter ist wahlfrei. Geben Sie diesen Parameter nur an, wenn Sie den Befehl REGISTER NODE auf einem Server ausgeben, der für die Replikation von Daten auf einen Zielreplikationsserver konfiguriert ist. Wenn Sie einen Clientknoten auf einem Quellenreplikationsserver registrieren und die Replikation für den Knoten definieren, registrieren Sie den Knoten nicht auf dem Zielreplikationsserver. Der Clientknoten wird automatisch auf dem Zielsever erstellt, wenn zum ersten Mal die Replikation erfolgt. Sie können einen der folgenden Werte auswählen:

##### Enabled

Gibt an, dass der Clientknoten für die Replikation konfiguriert und für die Replikation bereit ist. Wenn Sie diesen Parameter angeben, wird der Replikationsmodus in der Clientknotendefinition auf dem Quellenreplikationsserver automatisch auf

SEND gesetzt. Diese Einstellung gibt an, dass Daten, die zu dem Clientknoten gehören, während der Replikation an einen Zielservers gesendet werden.

Wenn die Replikation zum ersten Mal für den Clientknoten erfolgt, wird der Replikationsstatus des Knotens auf dem Zielreplikationsserver automatisch auf ENABLED gesetzt. Der Replikationsmodus auf dem Zielreplikationsserver wird auf RECEIVE gesetzt. Diese Einstellung gibt an, dass Daten, die zu dem Clientknoten gehören, von einem Quellenreplikationsserver empfangen werden. Um den Replikationsstatus und -modus zu bestimmen, geben Sie den Befehl QUERY NODE auf einem Quellen- oder Zielreplikationsserver aus.

DISabled

Gibt an, dass der Knoten für die Replikation konfiguriert ist, aber die Replikation erst erfolgt, wenn sie aktiviert wurde.

BKREPLRuledefault, ARREPLRuledefault und SPREPLRuledefault

Gibt die Replikationsregel an, die für einen Datentyp gilt, wenn die Dateibereichsregeln für den Datentyp auf DEFAULT gesetzt sind.

Einschränkung: Der Parameter BKREPLRULEDEFAULT, ARREPLRULEDEFAULT oder SPREPLRULEDEFAULT kann nur angegeben werden, wenn Sie den Parameter REPLSTATE angeben.

BKREPLRuledefault

Gibt die Replikationsregel für Sicherungsdaten an.

ARREPLRuledefault

Gibt die Replikationsregel für Archivierungsdaten an.

SPREPLRuledefault

Gibt die Replikationsregel für speicher verwaltete Daten an.

Sind die Dateibereichsregeln für den Datentyp auf DEFAULT gesetzt und geben Sie keine Regel für den Parameter BKREPLRULEDEFAULT, ARREPLRULEDEFAULT oder SPREPLRULEDEFAULT an, werden Daten gemäß der Serverregel für den Datentyp repliziert.

Sie können Replikationsregeln für normale Priorität oder Replikationsregeln für hohe Priorität angeben. In einem Replikationsprozess, der sowohl Daten mit normaler Priorität als auch Daten mit hoher Priorität einschließt, werden Daten mit hoher Priorität zuerst repliziert. Bevor Sie eine Regel angeben, beachten Sie die Reihenfolge, in der die Daten repliziert werden sollen.

Sie können die folgenden Regeln angeben:

ALL\_DATA

Repliziert aktive und inaktive Sicherungsdaten, Archivierungsdaten oder speicher verwaltete Daten. Die Daten werden mit einer normalen Priorität repliziert.

ACTIVE\_DATA

Repliziert nur aktive Sicherungsdaten. Die Daten werden mit einer normalen Priorität repliziert. Diese Regel ist nur für BKREPLRULEDEFAULT gültig.

Achtung:

Wenn Sie ACTIVE\_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

- Wenn eine Releaseversion vor Version 7.1.1 entweder auf dem Quellenreplikationsserver oder auf dem Zielreplikationsserver installiert ist.
- Wenn Sie den Befehl REPLICATE NODE mit dem Parameter `FORCERECONCILE=YES` verwenden.
- Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Releaseversion vor Version 7.1.1 ausführen.

Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

ALL\_DATA\_HIGH\_PRIORITY

Repliziert aktive und inaktive Sicherungsdaten, Archivierungsdaten oder speicher verwaltete Daten. Daten werden mit einer hohen Priorität repliziert.

ACTIVE\_DATA\_HIGH\_PRIORITY

Diese Regel entspricht der Replikationsregel ACTIVE\_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden. Diese Regel ist nur für BKREPLRULEDEFAULT gültig.

DEFAULT

Repliziert Daten gemäß der Serverreplikationsregel für Sicherungsdaten.

Beispiel: Angenommen, Sie möchten die Archivierungsdaten in allen Dateibereichen replizieren, die zu einem Clientknoten gehören. Die Replikation der Archivierungsdaten hat eine hohe Priorität. Eine Methode zur Ausführung dieser Task ist die Angabe von `ARREPLRULEDEFAULT=DEFAULT`. Stellen Sie sicher, dass die Dateibereichsregeln für Archivierungsdaten ebenfalls auf `DEFAULT` gesetzt sind und die Serverregel für Archivierungsdaten auf `ALL_DATA_HIGH_PRIORITY` gesetzt ist.

Einschränkung: Wenn ein Knoten für die Replikation konfiguriert ist, werden die Dateibereichsregeln auf `DEFAULT` gesetzt, nachdem der Knoten Daten auf dem Quellenreplikationsserver gespeichert hat.

#### NONE

Daten des angegebenen Typs werden nicht repliziert.

Sollen beispielsweise speicher verwaltete Daten, die zu einem Clientknoten gehören, nicht repliziert werden, geben Sie `SPREPLRULEDEFAULT=NONE` an.

#### RECOVERDamaged

Gibt an, ob beschädigte Dateien für diesen Knoten von einem Zielreplikationsserver wiederhergestellt werden können. Der Parameter ist wahlfrei. Der Standardwert ist `YES`. Sie können einen der folgenden Werte angeben:

##### Yes

Gibt an, dass die Wiederherstellung beschädigter Dateien durch einen Zielreplikationsserver für diesen Knoten aktiviert ist.

##### No

Gibt an, dass die Wiederherstellung beschädigter Dateien durch einen Zielreplikationsserver für diesen Knoten nicht aktiviert ist.

Tipp: Der Wert des Parameters `RECOVERDAMAGED` ist nur eine von mehreren Einstellungen, die bestimmen, ob beschädigte Dateien wiederhergestellt werden. Informationen zur Angabe der Einstellungen finden Sie in Einstellungen, die sich auf die Wiederherstellung beschädigter Dateien auswirken.

#### ROLEOVERRIDE

Gibt an, ob die zurückgemeldete Rolle des Clients für die Zurückmeldung der PVU-Schätzung (PVU - Prozessor-Value-Unit) überschrieben werden soll. Der Standardwert ist `USERREPORTED`. Der Parameter ist wahlfrei.

Die vom Client zurückgemeldete Rolle ist entweder 'Clienteinheit' (z. B. eine Workstation) oder 'Servereinheit' (z. B. Datei-/Druckserver, Anwendungsserver, Datenbank). Standardmäßig meldet der Client seine Rolle auf der Basis des Clienttyps und des Betriebssystems zurück. Alle Clients melden anfänglich ihre Rolle als 'Servereinheit' zurück, mit Ausnahme von Clients für Sichern/Archivieren, auf denen Microsoft Windows-Workstationverteilungen (Windows Vista) und Macintosh OS X ausgeführt werden.

Geben Sie einen der folgenden Werte an:

##### Client

Gibt eine Clienteinheit an.

##### Server

Gibt eine Servereinheit an.

##### Other

Gibt an, dass dieser Knoten nicht für die Zurückmeldung der PVU-Schätzung verwendet werden soll. Dieser Wert kann nützlich sein, wenn mehrere Knoten für ein physisches System implementiert sind (z. B. virtuelle Umgebungen, Testknoten, Knoten im Ruhezustand und Knoten, die nicht in der Produktion oder im Clustering sind).

##### Userreported

Die zurückgemeldete Rolle verwenden, die vom Client bereitgestellt wird.

#### AUTHentication

Dieser Parameter gibt die Kennwortauthentifizierungsmethode für den Knoten an. Geben Sie einen der folgenden Werte an: `LDAP` oder `LOCAL`. Der Parameter ist wahlfrei und nimmt standardmäßig den Wert `LOCAL` an. Der Standardwert kann sich in `LDAP` ändern, wenn Sie den Befehl `SET DEFAULTAUTHENTICATION` verwenden und `LDAP` angeben.

##### Local

Gibt an, dass die lokale IBM Spectrum Protect-Serverdatenbank verwendet wird.

##### LDap

Gibt an, dass der Knoten einen LDAP-Server für die Kennwortauthentifizierung verwendet.

#### SSLrequired (veraltet)

Gibt an, ob der Knoten das Protokoll Secure Sockets Layer (SSL) für die Kommunikation mit dem IBM Spectrum Protect-Server verwenden muss. Der Parameter ist wahlfrei. Wenn Sie Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren, müssen Sie die Sitzungen mit SSL oder einer anderen Netzsicherheitsmethode schützen.

Wichtig: Ab IBM Spectrum Protect Version 8.1.2 und Tivoli Storage Manager Version 7.1.8 wird dieser Parameter nicht mehr verwendet. Die durch diesen Parameter aktivierte Validierung wird durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter

SESSIONSECURITY durchgesetzt wird. Der Parameter SSLREQUIRED wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

#### SESSIONSECURITY

Gibt an, ob der Knoten die sichersten Einstellungen verwenden muss, um mit einem IBM Spectrum Protect-Server zu kommunizieren. Dieser Parameter ist wahlfrei.

Sie können einen der folgenden Werte angeben:

#### STRICT

Gibt an, dass die striktesten Sicherheitseinstellungen für den Knoten durchgesetzt werden. Der Wert STRICT verwendet das sicherste Kommunikationsprotokoll, das verfügbar ist. Dies ist derzeit TLS 1.2. Das TLS 1.2-Protokoll wird für SSL-Sitzungen zwischen dem Server und dem Knoten verwendet. Um anzugeben, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, lesen Sie die Informationen zur Clientoption SSL.

Für die Verwendung des Werts STRICT müssen die folgenden Anforderungen erfüllt werden, um sicherzustellen, dass sich der Knoten mit dem Server authentifizieren kann:

- Der Knoten und der Server müssen IBM Spectrum Protect-Software verwenden, die den Parameter SESSIONSECURITY unterstützt.
- Der Knoten muss für die Verwendung des TLS 1.2-Protokolls für SSL-Sitzungen zwischen dem Server und dem Knoten konfiguriert werden.

Knoten, für die der Wert STRICT definiert ist und die diese Anforderungen nicht erfüllen, können sich nicht mit dem Server authentifizieren.

#### TRANSITIONAL

Gibt an, dass die vorhandenen Sicherheitseinstellungen für den Knoten durchgesetzt werden. Dies ist der Standardwert. Dieser Wert ist für die temporäre Verwendung bestimmt, während Sie Ihre Sicherheitseinstellungen aktualisieren, um die Anforderungen für den Wert STRICT zu erfüllen.

Ist SESSIONSECURITY=TRANSITIONAL definiert und hat der Knoten nie die Anforderungen für den Wert STRICT erfüllt, authentifiziert sich der Knoten weiterhin mithilfe des Werts TRANSITIONAL. Wenn ein Knoten jedoch die Anforderungen für den Wert STRICT erfüllt, wird der Wert des Parameters SESSIONSECURITY automatisch von TRANSITIONAL in STRICT aktualisiert. Der Knoten kann sich dann nicht mehr mit einer Version des Clients oder mit einem SSL/TLS-Protokoll authentifizieren, die bzw. das die Anforderungen für STRICT nicht erfüllt. Nachdem sich ein Knoten erfolgreich mit einem Kommunikationsprotokoll authentifiziert hat, das mehr Sicherheit bietet, kann sich der Knoten nicht mehr mit einem weniger sicheren Protokoll authentifizieren. Beispiel: Wenn ein Knoten, der nicht SSL verwendet, aktualisiert wird und sich mithilfe von TLS 1.2 erfolgreich authentifiziert, kann sich der Knoten nicht mehr ohne SSL-Protokoll oder mithilfe von TLS 1.1 authentifizieren. Diese Einschränkung gilt auch bei Verwendung von Funktionen wie z. B. virtuelle Datenträger, wenn sich der Knoten beim IBM Spectrum Protect-Server als Knoten von einem anderen Server authentifiziert.

#### SPLITLARGEObjects

Gibt an, ob große Objekte, die von diesem Knoten gespeichert werden, automatisch vom Server in kleinere Teile aufgeteilt werden, um die Serververarbeitung zu optimieren. Der Parameter ist wahlfrei. Die Angabe von 'Yes' hat zur Folge, dass der Server große Objekte (über 10 GB) in kleinere Teile aufteilt, wenn sie von einem Clientknoten gespeichert werden. Bei Angabe von 'No' wird dieser Prozess übergangen. Geben Sie 'No' nur an, wenn Ihr primäres Ziel die Maximierung des Durchsatzes von Sicherungen direkt auf Band ist. Der Standardwert ist 'Yes'.

## Beispiel: Einen Clientknoten registrieren, der nur vom Rootbenutzer gesichert werden kann

---

Den Clientknoten `mete0rite` mit dem Kennwort `KingK0ng` registrieren, um nur dem Rootbenutzer das Sichern von Dateien auf dem Server zu erlauben.

```
register node mete0rite KingK0ng
backupinit=root
```

## Beispiel: Einen Clientknoten und ein Kennwort registrieren und die Komprimierung aktivieren

---

Den Clientknoten `JOEOS2` mit dem Kennwort `SECRETCODE` registrieren und diesen Knoten der Maßnahmendomäne `DOM1` zuordnen. Dieser Knoten kann seine eigenen Sicherungs- und Archivierungsdateien aus dem Server löschen. Der Clientknoten komprimiert alle Dateien, bevor sie an den Server gesendet werden. Dieser Befehl erstellt automatisch die Benutzer-ID mit Administratorberechtigung `JOEOS2` mit dem Kennwort `SECRETCODE`. Außerdem verfügt der Administrator jetzt über die Clienteignerberechtigung für den Knoten `JOEOS2`.

```
register node joeos2 secretcode domain=dom1
archdelete=yes backdelete=yes
compression=yes
```

## Beispiel: Einem vorhandenen Benutzer mit Verwaltungsaufgaben die Clienteignerberechtigung erteilen

---

Der vorhandenen Benutzer-ID mit Administratorberechtigung *HELPAADMIN* die Clienteignerberechtigung erteilen, wenn der Clientknoten *JAN* registriert wird. Dieser Schritt würde nicht automatisch die Administrator-ID *JAN* erstellen, sondern dem Administrator *HELPAADMIN* die Clienteignerberechtigung für diesen Knoten erteilen.

```
register node jan pwdsafe userid=helpadmin
```

## Beispiel: Einen NAS-Dateiserverknoten registrieren, der NDMP-Operationen verwendet

---

Den Knotennamen *NAS1* für einen NAS-Dateiserver registrieren, der NDMP-Operationen verwendet. Diesen Knoten einer speziellen NAS-Domäne zuordnen.

```
register node nas1 pw4pw domain=nasdom type=nas
```

## Beispiel: Einen Knoten registrieren und die maximale Anzahl der Dateien pro Transaktionsfestschreibung angeben

---

Einen Knoten mit dem Namen *ED* registrieren und *TXNGROUPMAX* auf 1.000 setzen.

```
register node ed pw45twx txngroupmax=1000
```

## Beispiel: Einen Knoten registrieren und die Datendeduplizierung auf dem Clientsystem zulassen

---

Einen Knoten mit dem Namen *JIM* registrieren und die Datendeduplizierung auf dem Clientsystem zulassen.

```
register node jim jim deduplication=clientorserver
```

## Beispiel: Den Knoten mit dem Namen ED registrieren und die Rolle als 'Servereinheit' für die Zurückmeldung der PVU-Schätzung definieren

---

Den Knoten mit dem Namen *ED* registrieren und die Rolle als 'Servereinheit' für die Zurückmeldung der PVU-Schätzung definieren.

```
register node ed pw45twx roleoverride=server
```

## Beispiel: Einen Knoten auf einem Quellenreplikationsserver registrieren

---

*NODE1* für einen Quellenreplikationsserver definieren. Eine Replikationsregel für die Sicherungsdaten angeben, die zu *NODE1* gehören, sodass aktive Sicherungsdaten mit einer hohen Priorität repliziert werden. Die Replikation für den Knoten aktivieren.

```
register node node1 bkreplruledefault=active_data_high_priority replstate=enabled
```

## Beispiel: Einen Knoten registrieren, der mit einem LDAP-Server authentifiziert wird

---

Registrieren Sie einen Knoten mit dem Namen *NODE17*, der sich mit einem LDAP-Server authentifizieren muss.

```
register node node17 authentication=ldap
```

Tipp: Wenn Sie einen Knoten auf diese Weise registrieren, wird keine Benutzer-ID mit Administratorberechtigung erstellt.

## Beispiel: Knoten für die Kommunikation mit einem Server unter Verwendung der Sitzungssicherheit 'strict' registrieren

---

Einen Knoten mit dem Namen *NODE4* registrieren, um die striktesten Sicherheitseinstellungen für die Authentifizierung mit dem Server zu verwenden.

```
register node node4 sessionsecurity=strict
```

## Beispiel: Einen Knoten registrieren und die Wiederherstellung beschädigter Dateien aktivieren

---

Den Knotennamen *PAYROLL* registrieren. Für den Knoten *PAYROLL* die Wiederherstellung beschädigter Dateien durch einen Zielreplikationsserver aktivieren.

```
register node payroll recoverdamaged=yes
```

Tabelle 2. Zugehörige Befehle für REGISTER NODE

| Befehl                     | Beschreibung   |
|----------------------------|--|
| DEFINE ASSOCIATION         | Ordnet Clients einem Zeitplan zu.  |
| DEFINE DATAMOVER           | Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server.  |
| DEFINE MACHNODEASSOCIATION | Ordnet einen IBM Spectrum Protect-Knoten einer Maschine zu.  |
| DELETE FILESPACE           | Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt. |
| LOCK NODE                  | Verhindert, dass ein Client auf den Server zugreift.   |
| QUERY FILESPACE            | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.  |
| QUERY NODE                 | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.  |
| QUERY PVUESTIMATE          | Zeigt eine Schätzung der Clienteinheiten und Servereinheiten an, die verwaltet werden.   |
| QUERY REPLNODE             | Zeigt Informationen zum Replikationsstatus eines Clientknotens an.   |
| REGISTER ADMIN             | Definiert einen neuen Administrator, ohne Administratorberechtigung zu erteilen.   |
| REMOVE NODE                | Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.   |
| REMOVE REPLNODE            | Entfernt einen Knoten aus der Replikation.   |
| RENAME NODE                | Ändert den Namen eines Clientknotens.  |
| REPLICATE NODE             | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |
| RESET PASSEXP              | Setzt die Kennwortablaufdauer für Knoten oder Administratoren zurück.  |
| SET DEFAULTAUTHENTICATION  | Gibt die Standardkennwortauthentifizierungsmethode für alle Befehle REGISTER NODE oder REGISTER ADMIN an.  |
| SET PASSEXP                | Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.   |
| SET CPUINFOREFRESH         | Gibt die Anzahl der Tage zwischen Clientsuchläufen nach Workstationinformationen an, die für PVU-Schätzungen verwendet werden.   |
| SET DEDUPVERIFICATIONLEVEL | Gibt den Prozentsatz der Bereiche an, die vom Server während der clientseitigen Deduplizierung geprüft werden sollen.  |
| SET REPLRECOVERDAMAGED     | Gibt an, ob die Knotenreplikation aktiviert ist, um beschädigte Dateien durch einen Zielreplikationsserver wiederherzustellen.   |
| UNLOCK NODE                | Ermöglicht einem gesperrten Benutzer in einer bestimmten Maßnahmendomäne wieder den Zugriff auf den Server.  |
| UPDATE ADMIN               | Ändert das Kennwort eines Administrators bzw. die zu einem Administrator gehörigen Kontaktinformationen.   |
| UPDATE FILESPACE           | Ändert Knotenreplikationsregeln für Dateibereiche.   |
| UPDATE NODE                | Ändert die Attribute, die einem Clientknoten zugeordnet sind.  |

### Zugehörige Konzepte:

Tasks für Rootbenutzer und berechtigte Benutzer des UNIX- und Linux-Clients

### Zugehörige Verweise:




Ssl (Clientoption)



## REMOVE-Befehle

---

Mit den REMOVE-Befehlen kann ein Objekt aus IBM Spectrum Protect entfernt werden.

- REMOVE ADMIN (Benutzer-ID mit Administratorberechtigung löschen)
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme REMOVE DAMAGED (Beschädigte Daten aus einem Quellspeicherpool entfernen)
- REMOVE NODE (Knoten oder zugehörigen Maschinenknoten löschen)
- REMOVE REPLNODE (Clientknoten aus Replikation entfernen)
- REMOVE REPLSERVER (Replikationsserver entfernen)

## REMOVE ADMIN (Benutzer-ID mit Administratorberechtigung löschen)

---

Verwenden Sie diesen Befehl, um eine Benutzer-ID mit Administratorberechtigung aus dem System zu entfernen.

Die letzte Benutzer-ID mit Systemadministratorberechtigung oder die Verwaltungs-ID SERVER\_CONSOLE kann nicht aus dem System entfernt werden.

Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol): Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.

### Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

---

```
>>-REMOve Admin--Administratorname----->
. -SYNClapdelete---No-----
>+-----+----->
'-SYNClapdelete---No---+'
      '-Yes-'
```

### Parameter

---

Administratorname (Erforderlich)

Gibt die Benutzer-ID mit Administratorberechtigung, die entfernt werden soll.

SYNClapdelete

Gibt an, ob die Administrator-ID auf dem LDAP-Server (LDAP = Lightweight Directory Access Protocol) gelöscht werden soll.

Yes

Die Administrator-ID wird auf dem LDAP-Server gelöscht.

Einschränkung: Sie dürfen nicht den Wert YES angeben. (Der Wert YES ist nur für die Benutzer der vorherigen LDAP-Authentifizierungsmethode gültig, die in Kennwörter und Anmeldeverfahren verwalten beschrieben wird.)

No

Die Administrator-ID wird auf dem LDAP-Server nicht gelöscht. Dies ist der Standardwert.

### Beispiel: Eine Benutzer-ID mit Administratorberechtigung entfernen

---

Entfernen Sie die Benutzer-ID larry mit Administratorberechtigung, die nicht auf einem LDAP-Server definiert ist. Geben Sie den folgenden Befehl aus:

```
remove admin larry
```




### Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für REMOVE ADMIN

| Befehl | Beschreibung |
|--------|--------------|
|--------|--------------|

| Befehl         | Beschreibung   |
|----------------|--|
| LOCK ADMIN     | Verweigert einem Administrator den Zugriff auf IBM Spectrum Protect.                   |
| QUERY ADMIN    | Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an. |
| REGISTER ADMIN | Definiert einen neuen Administrator, ohne Administratorberechtigung zu erteilen.       |
| RENAME ADMIN   | Ändert den Namen eines IBM Spectrum Protect-Administrators.                            |

## REMOVE DAMAGED (Beschädigte Daten aus einem Quellenspeicherpool entfernen)

Mit diesem Befehl können Sie nach der Speicherpoolkonvertierung beschädigte Daten aus einem Speicherpool entfernen, der eine Einheitenklasse FILE, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet.

Mit dem Befehl REMOVE DAMAGED werden beschädigte Daten permanent aus dem Speicherpool entfernt.

Tipp: Bevor Sie beschädigte Daten aus dem Speicherpool entfernen, versuchen Sie, eine unbeschädigte Version der Daten aus einem Kopierspeicherpool oder Speicherpool für aktive Daten wiederherzustellen, indem Sie den Befehl RESTORE STGPOOL ausgeben. Sie können eine unbeschädigte Version der Daten von einem Zielreplikationsserver wiederherstellen, indem Sie den Befehl REPLICATE NODE ausgeben und den Parameter RECOVERDAMAGED=YES angeben.

### Berechtigungsklasse

Für diesen Befehl ist die eingeschränkte Speicherberechtigung erforderlich.

### Syntax

```

>>-REMOve DAMaged--Poolname-+-----+----->
| .-*,-----|
| V           |
|---Knotenname-+-'
. -Wait----No-----
>+-----+-----<
'-Wait-----No-+-'
'-Yes-'

```

### Parameter

#### Poolname (Erforderlich)

Geben Sie einen primären Speicherpool an, der eine Einheitenklasse FILE, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet. Der Speicherpool enthält die beschädigten Daten. Dieser Parameter ist erforderlich.

#### Knotenname

Gibt den Namen des Clientknotens an. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Sie können ein Platzhalterzeichen anstelle eines Knotennamens verwenden, wenn beschädigte Daten auf allen Knoten in dem Speicherpool entfernt werden sollen.

#### Wait

Gibt an, ob darauf gewartet werden soll, dass der Server beschädigte Daten aus dem Speicherpool entfernt. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können diesen Parameter nur in einer Verwaltungsbefehlszeile angeben. Sie können einen der folgenden Werte angeben:

#### No

Gibt an, dass die Befehlsprozesse im Hintergrund ausgeführt werden.

#### Yes

Gibt an, dass die Befehlsprozesse im Vordergrund ausgeführt werden. Nachrichten werden erst angezeigt, wenn die Verarbeitung des Befehls beendet ist.

## Beispiel: Beschädigte Daten aus einem Speicherpool entfernen und darauf warten, dass der Server die Verarbeitung beendet

Beschädigte Daten aus einem Speicherpool mit dem Namen POOL1 entfernen und darauf warten, dass der Server die Verarbeitung im Vordergrund beendet.

```
remove damaged pool1 wait=yes
```

Tabelle 1. Zugehörige Befehle für REMOVE DAMAGED

| Befehl          | Beschreibung  |
|-----------------|---|
| CONVERT STGPOOL | Konvertiert einen Speicherpool in einen Verzeichniscontainerspeicherpool. |
| PROTECT STGPOOL | Schützt einen Verzeichniscontainerspeicherpool.                           |
| REPAIR STGPOOL  | Repariert einen Verzeichniscontainerspeicherpool.                         |

## REMOVE NODE (Knoten oder zugehörigen Maschinenknoten löschen)

Verwenden Sie diesen Befehl, um einen Knoten von dem Server zu entfernen. Wenn Sie Disaster Recovery Manager verwenden und der zu löschende Knoten einer Maschine zugeordnet ist, wird auch die Zuordnung zwischen dem Knoten und der Maschine gelöscht.

Ist ein Knoten Teil einer Kollokationsgruppe und wird der Knoten von dem Server entfernt, wird der Knoten aus der Kollokationsgruppe entfernt. Wird ein Knoten entfernt und enthielt der Knoten Dateibereiche in einer Dateibereichskollokationsgruppe, werden diese Dateibereiche aus der Liste der Gruppenmitglieder entfernt.

Wenn Sie einen Knoten entfernen, der Daten in einem deduplizierten Speicherpool gespeichert hat, wird der Knotenname DELETED in der Ausgabe des Befehls QUERY OCCUPANCY angezeigt, bis alle Dateneduplizierungsabhängigkeiten entfernt wurden.

Wenn ein Knoten entfernt wird, wird die entsprechende Verwaltungs-ID nur entfernt, wenn die folgenden Bedingungen zutreffen:

- Der Administratorname stimmt mit dem Knotennamen überein.
- Der Administrator hat Clienteigner- oder Clientzugriffsberechtigung *nur* für den Knoten, der entfernt wird.
- Der Administrator ist kein verwaltetes Objekt.

Bevor ein Knoten entfernt werden kann, müssen alle zu diesem Knoten gehörigen Bereiche für Archivierungs- und Sicherungsdateien gelöscht werden.

Bevor ein NAS-Knoten entfernt werden kann, der über eine entsprechende Einheit zum Versetzen von Daten verfügt, müssen Sie die folgenden Tasks in dieser Reihenfolge ausführen:

1. Alle Pfade von der Einheit zum Versetzen von Daten löschen
2. Die Einheit zum Versetzen von Daten löschen
3. Alle Definitionen des virtuellen Dateibereichs für den Knoten löschen
4. Den NAS-Knoten entfernen

Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol): Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, der der Clientknoten zugeordnet ist.

## Syntax

```
>>-REMove Node--Knotenname-----.-SYNCldapdelete-----No-----<<
                                     '-SYNCldapdelete-----+No---+'
                                     '-Yes-'
```

## Parameter

Knotenname (Erforderlich)

Gibt den Namen des zu löschenden Knotens an.

SYNCLdapdelete

Gibt an, ob der Knoten auf dem LDAP-Server (LDAP = Lightweight Directory Access Protocol) entfernt werden soll.

Yes

Gibt an, dass der Knoten entfernt wird.

Einschränkung: Sie dürfen nicht den Wert YES angeben. (Der Wert YES ist nur für die Benutzer der vorherigen LDAP-Authentifizierungsmethode gültig, die in Kennwörter und Anmeldeverfahren verwaltet beschrieben wird.)

No

Gibt an, dass der Knoten nicht entfernt wird. Dies ist der Standardwert.


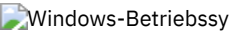

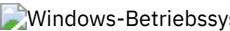

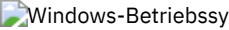

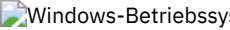
## Beispiel: Einen Clientknoten entfernen

Den Clientknoten LARRY entfernen.

```
remove node larry
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für REMOVE NODE

| Befehl   | Beschreibung  |
|--|---|
|   DELETE MACHNODEASSOCIATION |   Löscht die Zuordnung zwischen einer Maschine und einem Knoten. |
| DELETE DATAMOVER   | Löscht eine Einheit zum Versetzen von Daten.  |
| DELETE FILESPACE   | Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.            |
| DELETE PATH  | Löscht einen Pfad von einer Quelle zu einem Ziel.   |
| DELETE VIRTUALFSMAPPING  | Zuordnung eines virtuellen Dateibereichs löschen.   |
| LOCK NODE  | Verhindert, dass ein Client auf den Server zugreift.  |
| QUERY COLLOGROUP   | Zeigt Informationen zu Kollokationsgruppen an.  |
|   QUERY MACHINE          |   Zeigt Informationen über Maschinen an.                     |
| QUERY NODE   | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.   |
| QUERY SESSION  | Zeigt Informationen zu allen aktiven Administrator- und Clientsitzungen mit IBM Spectrum Protect an.  |
| REGISTER NODE  | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.   |
| RENAME NODE  | Ändert den Namen eines Clientknotens.   |

## REMOVE REPLNODE (Clientknoten aus Replikation entfernen)

Verwenden Sie diesen Befehl, um einen Knoten aus der Replikation zu entfernen, wenn die Daten, die zu dem Knoten gehören, nicht mehr repliziert werden sollen.

Sie können keine Clientknotendaten löschen, indem Sie den Befehl REMOVE REPLNODE ausgeben. Sie können den Befehl auf einem Quellen- oder einem Zielreplikationsserver ausgeben. Sie können diesen Befehl nur über einen Verwaltungsbefehlszeilenclient ausgeben. Dieser Befehl kann nicht über die Server-Konsole ausgegeben werden.

Wird der Befehl REMOVE REPLNODE für einen Clientknoten ausgegeben, dessen Replikationsmodus auf SEND oder RECEIVE gesetzt ist, wird der Modus auf NONE gesetzt. Der Replikationsstatus wird ebenfalls auf NONE gesetzt. Nach dem Entfernen eines Clientknotens aus der Replikation kann der Zielreplikationsserver Sicherungsdaten, Archivierungsdaten und speicher verwaltete Daten direkt vom Knoten akzeptieren.

Wenn ein Clientknoten aus der Replikation entfernt wird, werden Informationen in der Datenbank zur Replikation für den Knoten gelöscht. Wenn der Clientknoten später für die Replikation aktiviert wird, repliziert der Replikationsprozess alle Daten, die durch

Replikationsregeln und Einstellungen angegeben sind.

Wenn Sie den Befehl REMOVE REPLNODE ausgeben, werden die Daten, die zu einem Clientknoten gehören, nicht gelöscht. Sollen Dateibereichsdaten gelöscht werden, die zu dem Clientknoten gehören, geben Sie den Befehl DELETE FILESPACE für jeden Dateibereich aus, der zu dem Knoten gehört. Soll die Clientknotendefinition nicht aufbewahrt werden, geben Sie den Befehl REMOVE NODE aus. Sollen Dateibereichsdaten und die Clientknotendefinition gelöscht werden, geben Sie DELETE FILESPACE und REMOVE NODE auf dem Zielreplikationsserver aus.

Einschränkung: Wenn ein Knotenreplikationsprozess für einen mit diesem Befehl angegebenen Clientknoten aktiv ist, schlägt der Befehl fehl und die Replikationsinformationen für den Knoten werden nicht entfernt.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, der der Clientknoten zugeordnet ist.

## Syntax

```
>>-REMOve REPLNode-----+-----Knotenname-----+-----<<
      |
      v
      '-Knotengruppenname-'
```

## Parameter

Knotenname oder Knotengruppenname (Erforderlich)

Gibt den Namen des Clientknotens oder der definierten Gruppe von Clientknoten an, der bzw. die aus der Replikation entfernt werden soll. Sollen mehrere Clientknotennamen und Clientknotengruppenamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Sie können Platzhalterzeichen verwenden, um Clientknotennamen anzugeben, aber Sie können keine Platzhalterzeichen verwenden, um Clientknotengruppenamen anzugeben. Sie können Knoten- oder Knotengruppenamen nicht mit dem Domännennamen kombinieren.

## Beispiel: Drei Clientknoten und eine Clientknotengruppe aus der Replikation entfernen

Die Namen der Clientknoten sind NODE1, NODE2 und NODE3. Der Name der Clientknotengruppe lautet PAYROLL. Geben Sie den folgenden Befehl auf dem Quellen- und Zielreplikationsserver aus:

```
remove replnode node*,payroll
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für REMOVE REPLNODE

| Befehl            | Beschreibung  |
|-------------------|---|
| QUERY NODE        | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an. |
| QUERY REPLICATION | Zeigt Informationen zu Knotenreplikationsprozessen an.                            |

## REMOVE REPLSERVER (Replikationsserver entfernen)

Verwenden Sie diesen Befehl, um einen Replikationsserver aus der Liste der Replikationsserver zu entfernen oder zu einem Replikationsserver in der Liste der Replikationsserver zu wechseln. Mit diesem Befehl werden alle Informationen zum Replikationsstatus für alle Knoten gelöscht, die auf diesen Server repliziert wurden.

Sie können den Befehl auf einem Quellen- oder einem Zielreplikationsserver ausgeben.

Einschränkung: Sie können keine Clientknotendaten mit dem Befehl REMOVE REPLSERVER löschen.

Verwenden Sie den Befehl, um zwischen Replikationsservern zu wechseln und Replikationsinformationen für einen alten Server zu entfernen. Der Befehl hat keine Auswirkungen auf den aktuellen Replikationsmodus oder -status von Knotendefinitionen. Geben Sie den Befehl sowohl auf dem Quellenserver als auch auf dem Zielservers aus, damit die Informationen zum Replikationsstatus für beide Server konsistent bleiben.

Einschränkung: Wenn Sie den Standardreplikationsserver für den Befehl REMOVE REPLSERVER angeben und ein Knotenreplikationsprozess aktiv ist, schlägt der Befehl fehl und es werden keine Replikationsinformationen entfernt.

Dieser Befehl wird als Hintergrundoperation ausgeführt und kann nicht abgebrochen werden. IBM Spectrum Protect löscht Replikationsinformationen, die dem angegebenen Server zugeordnet sind, als Serie von Stapeldatenbanktransaktionen. Wenn ein Systemfehler auftritt, kann ein partielles Löschen erfolgen.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-REMOve REPLServer--GUID-----><
```

## Parameter

---

Replikations-GUID (Erforderlich)

Die eindeutige ID für den Replikationsserver, der entfernt wird. Sie können Platzhalterzeichen verwenden, um die global eindeutige ID (GUID) für die Replikation anzugeben, es kann jedoch nur eine einzige GUID mit dem Platzhalterzeichen übereinstimmen. Wenn die Platzhalterzeichenfolge mehreren GUIDs entspricht, schlägt der Befehl fehl. Sie müssen die Platzhalterzeichenfolge qualifizieren, damit nur die zu löschende GUID gefunden wird.

## Beispiel: Ein Platzhalterzeichen verwenden, um einen Replikationsserver zu entfernen

---

Entfernen Sie einen Replikationsserver, indem Sie ein Platzhalterzeichen zur Angabe der GUID verwenden.

```
remove replserver e*
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für REMOVE REPLSERVER

| Befehl   | Beschreibung                                   |
|--|--|
| REMOVE REPLNODE (Clientknoten aus Replikation entfernen) | Entfernt einen Knoten aus der Replikation.     |
| QUERY REPLSERVER (Replikationsserver abfragen)           | Zeigt Informationen zu Replikationsservern an. |

## RENAME-Befehle

---

Mit den RENAME-Befehlen kann der Name eines vorhandenen Objekts geändert werden.

- RENAME ADMIN (Administrator umbenennen)
- RENAME FILESPACE (Clientdateibereich auf dem Server umbenennen)
- RENAME NODE (Knoten umbenennen)
- RENAME SCRIPT (IBM Spectrum Protect-Prozedur umbenennen)
- RENAME SERVERGROUP (Servergruppe umbenennen)
- RENAME STGPOOL (Den Namen eines Speicherpools ändern)

## RENAME ADMIN (Administrator umbenennen)

---

Verwenden Sie diesen Befehl, um eine Benutzer-ID mit Administratorberechtigung zu ändern. Bestehende Informationen zu diesem Administrator, zum Beispiel Kennwort, Kontaktinformationen und Berechtigungsklassen, werden nicht geändert.

Wenn Sie eine bestehende Administrator-ID einer anderen Person zuordnen, verwenden Sie den Befehl UPDATE ADMIN, um das Kennwort zu ändern.

Wenn ein Administrator und ein Knoten einen Namen gemeinsam nutzen und die Authentifizierungsmethode des Administrators geändert wird, ändert sich auch die Knotenauthentifizierungsmethode. Wenn Sie einen Administrator in den Namen eines vorhandenen Knotens umbenennen, können sich die Authentifizierungsmethode und die Einstellung für SSLREQUIRED für den Knoten ändern. Sind diese Einstellungen unterschiedlich, haben der Administrator und der Knoten nach dem Umbenennen dieselbe Authentifizierungsmethode und dieselbe Einstellung für SSLREQUIRED.

Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol):

- Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.
- Benennen Sie keine Benutzer-ID mit Administratorberechtigung so um, dass sie mit einem Knotennamen identisch ist. Wenn die Namen übereinstimmen, stellen Sie möglicherweise ein nicht erwartetes Verhalten fest, weil automatische Kennwortänderungen dasselbe Kennwort zweimal aktualisieren. Dies hat zur Folge, dass das Kennwort für die Benutzer-ID mit Administratorberechtigung unbekannt ist. Es kann aber auch vorkommen, dass die Kennwortaktualisierung fehlschlägt.

Die Verwaltungs-ID SERVER\_CONSOLE kann nicht umbenannt werden.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-REName Admin--aktueller_Administratorname--neuer_Administratorname-->
. -SYNCldapdelete----No-----
>-----+-----+-----+-----+-----+-----+-----+-----+-----+-----><
' -SYNCldapdelete----+No--+-'
                               '-Yes-'
```

## Parameter

---

- aktueller\_Administratorname (Erforderlich)  
Gibt die Benutzer-ID mit Administratorberechtigung, die umbenannt werden soll.
- neuer\_Administratorname (Erforderlich)  
Gibt die neue Benutzer-ID mit Administratorberechtigung an. Die maximale Länge des Namens beträgt 64 Zeichen.
- SYNCldapdelete  
Gibt an, ob die Administrator-ID auf dem LDAP-Server (LDAP = Lightweight Directory Access Protocol) gelöscht und die ID durch eine neue ID ersetzt werden soll.
- Yes  
Die Administrator-ID wird auf dem LDAP-Server gelöscht und durch eine neue ID ersetzt.  
Einschränkung: Sie dürfen nicht den Wert YES angeben. (Der Wert YES ist nur für die Benutzer der vorherigen LDAP-Authentifizierungsmethode gültig, die in Kennwörter und Anmeldeverfahren verwalten beschrieben wird.)
- No  
Die Administrator-ID wird auf dem LDAP-Server nicht gelöscht und ersetzt. Dies ist der Standardwert.

## Beispiel: Einen Administrator umbenennen

---

Den IBM Spectrum Protect-Administrator CLAUDIA in BILL umbenennen.

```
rename admin claudia bill
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für RENAME ADMIN

| Befehl       | Beschreibung   |
|--------------|--|
| QUERY ADMIN  | Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.                   |
| UPDATE ADMIN | Ändert das Kennwort eines Administrators bzw. die zu einem Administrator gehörigen Kontaktinformationen. |

## RENAME FILESPACE (Clientdateibereich auf dem Server umbenennen)

---

Mit diesem Befehl können vorhandene Clientdateibereiche auf dem Server oder importierte Dateibereiche umbenannt werden.

Möglicherweise möchten Sie einen Dateibereich umbenennen, der importiert wurde, oder die Erstellung neuer Unicode-fähiger Dateibereiche für Unicode-fähige Clients veranlassen.

Einschränkung: Benennen Sie keine NAS- oder VMware-Dateibereiche um. Wenn Sie einen NAS- oder VMware-Dateibereich umbenennen, ist er nicht mehr sichtbar und kann nicht zurückgeschrieben werden. Um einen umbenannten NAS- oder VMware-Dateibereich zurückzuschreiben, müssen Sie den Dateibereich in seinen ursprünglichen Namen umbenennen und den Parameter 'force' wie folgt definieren: force=yes

## Berechtigungsklasse

Jeder Administrator mit uneingeschränkter Maßnahmenberechtigung oder eingeschränkter Maßnahmenberechtigung für die Maßnahmendomäne des Clients kann diesen Befehl ausgeben.

## Syntax

```
>>-REName Filespace--Knotenname----->>  
>--aktueller_Dateibereichsname--neuer_Dateibereichsname----->  
  .-NAMEType-----SERVER-----  
>+-----+-----+-----+-----+----->  
  '-NAMEType-----+-SERVER--+-'  
      +-Unicode-+  
      '-FSID----'  
  .-NEWNAMEType-----SERVER-----.  
>+-----+-----+-----+-----+-----+----->  
  |                                          (1) | '-force---yes-'  
  '-NEWNAMEType-----+-Unicode-----+'  
      '-HEXadecimal-'
```

Anmerkungen:

1. Dieser Parameter ist der Standardwert, wenn NAMEType=Unicode angegeben wird.

## Parameter

Knotenname (Erforderlich)

Gibt den Namen des Clientknotens an, zu dem der umzubenehende Dateibereich gehört.

aktueller\_Dateibereichsname (Erforderlich)

Gibt den Namen des Dateibereichs an, der umbenannt werden soll. Bei einem Dateibereichsnamen muss die Groß-/Kleinschreibung berücksichtigt werden, und der Name muss genau so angegeben werden, wie er für den Server definiert ist. Namen für die Zuordnung virtueller Dateibereiche sind zulässig.

neuer\_Dateibereichsname (Erforderlich)

Gibt den neuen Namen für den Dateibereich an. Bei einem Clientdateibereichsnamen muss die Groß-/Kleinschreibung berücksichtigt werden, und der Name muss genau so angegeben werden, wie er für den Server definiert werden soll. Bei diesem Parameter kann es sich nicht um einen vorhandenen Namen für die Zuordnung eines virtuellen Dateibereichs handeln. Ist der aktuelle\_Dateibereichsname ein virtueller Dateibereich, muss der neue\_Dateibereichsname allen Regeln zum Definieren eines virtuellen Dateibereichsnamens entsprechen. Für weitere Informationen siehe Befehl DEFINE VIRTUALFSMAPPING. Wichtig: Ist der Typ des neuen Namens ein hexadezimaler Typ, geben Sie gültige UTF-8-Hexadezimalwerte an, damit die Zeichenumsetzungstabelle des Servers den Dateibereichsnamen wie gewünscht anzeigt. Geben Sie beispielsweise keinen Wert an, der als Rücksetzzeichen interpretiert werden kann.

Wenn Sie einen Dateibereich umbenennen, der Teil einer Dateibereichskollokationsgruppe ist, wird die Kollokationsgruppe mit dem neuen Namen aktualisiert.

NAMEType

Geben Sie an, wie der Server den aktuellen Dateibereichsnamen interpretieren soll, den Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unterstützung für Unicode verfügt. Sie können diesen Parameter für Unicode-fähige IBM Spectrum Protect-Clients mit den Betriebssystemen Windows, Macintosh OS X und NetWare verwenden.

Der Standardwert lautet SERVER. Wird ein Name für die Zuordnung eines virtuellen Dateibereichs angegeben, müssen Sie SERVER verwenden. Gültige Werte:

**SERVER**

Der Server verwendet die Zeichenumsetzungstabelle des Servers, um den Dateibereichsnamen zu interpretieren.

**Unicode**

Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetzungstabelle in die Zeichenumsetzungstabelle UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetzungstabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in



der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

#### FSID

Der Server interpretiert den Dateibereichsnamen als Dateibereichs-ID (FSID).

#### NEWNAMETYPE

Angeben, wie der Server den neuen Dateibereichsnamen interpretieren soll, den Sie eingeben. Der Standardwert lautet SERVER, wenn Sie für NAMETYPE SERVER angegeben haben oder wenn der Dateibereich, der umbenannt werden soll, nicht Unicode ist. Der Standardwert lautet UNICODE, wenn Sie für NAMETYPE UNICODE angegeben haben oder wenn der Dateibereich, der umbenannt werden soll, Unicode ist. Wird ein Name für die Zuordnung eines virtuellen Dateibereichs angegeben, müssen Sie SERVER verwenden. Gültige Werte:

#### SERVER

Der Server verwendet die Zeichenumsetztabelle des Servers, um den Dateibereichsnamen zu interpretieren.

#### UNICODE

Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Ist die Konvertierung nicht erfolgreich, möchten Sie möglicherweise den Parameter HEXADECIMAL angeben.

#### HEXadecimal

Der Server interpretiert den Dateibereichsnamen, den Sie eingeben, als hexadezimale Darstellung eines Namens in Unicode. Durch die Verwendung der hexadezimalen Darstellung wird sichergestellt, dass der Server den Dateibereich unabhängig von der Zeichenumsetztabelle des Servers korrekt umbenennen kann.

Soll die hexadezimale Darstellung eines Dateibereichsnamens angezeigt werden, können Sie den Befehl QUERY FILESPACE mit FORMAT=DETAILED verwenden.

Einschränkung: Sie können nicht einen neuen Namen mit einer Art, die von der Art des ursprünglichen Namens abweicht, angeben. Sie können den Namen eines Dateibereichs, der in Unicode ist, in einen anderen Namen in Unicode umbenennen. Sie können einen Dateibereich, der nicht in Unicode ist, umbenennen und einen neuen Namen in der Zeichenumsetztabelle des Servers verwenden. Die beiden Arten können jedoch nicht gemischt werden.

#### force

Um einen NAS- oder VMware-Dateibereich umzubenennen, müssen Sie diesen Parameter wie folgt definieren: force=yes

## Einen importierten Dateibereich umbenennen, um ein Überschreiben zu verhindern

Der AIX-Clientknoten LARRY hat den Dateibereich /r033 auf dem IBM Spectrum Protect-Server gesichert. Der Dateibereich wurde auf Band exportiert und später wieder auf den Server importiert. Beim Importieren dieses Dateibereichs wurde der vom System generierte Name /r031 für den importierten Dateibereich erstellt, da der Name /r033 für den Clientknoten LARRY vorhanden war.

Der Clientknoten LARRY verfügte jedoch bereits über einen Dateibereich mit dem Namen /r031, der nicht gesichert wurde und daher dem Server unbekannt war. Wird der importierte Dateibereich nicht umbenannt, überschreibt er den Dateibereich /r031, da der von der Funktion IMPORT generierte Dateibereichsname mit dem Namen eines Dateibereichs auf Clientknoten LARRY übereinstimmt, der dem Server nicht bekannt ist.

Verwenden Sie den folgenden Befehl, um den importierten Dateibereich /r031 umzubenennen. Der neue Name /imported-r033 gibt an, dass der neue Dateibereich ein importiertes Abbild des Dateibereichs /r033 ist.

```
rename filestorage larry /r031 /imported-r033
```

## Dateibereich umbenennen, um einen Unicode-fähigen Dateibereich zu erstellen

Client JOE verwendet einen deutschen Unicode-aktivierten IBM Spectrum Protect-Client. JOE hat mehrere große Dateibereiche, die nicht Unicode-fähig sind, im Serverspeicher gesichert. Dateibereich \\joe\c\$ enthält einige Dateien mit japanischen Dateinamen, die nicht in einem Dateibereich gesichert werden können, der nicht Unicode-fähig ist. Da die Dateibereiche groß sind, möchte der Administrator jetzt nicht alle Dateibereiche von JOE in Unicode-fähige Dateibereiche konvertieren. Der Administrator möchte nur den Nicht-Unicode-Dateibereich \\joe\c\$ umbenennen, so dass bei der nächsten Sicherung des Dateibereichs ein neuer Unicode-fähiger Dateibereich erstellt wird. Der neue Unicode-fähige Dateibereich ermöglicht die erfolgreiche Sicherung der japanischen Dateien.

Verwenden Sie den folgenden Befehl, um \\joe\c\$ umzubenennen:

```
rename filestorage joe \\joe\c$ \\joe\c$_old
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RENAME FILESPACE

| Befehl | Beschreibung |
|--------|--------------|
|--------|--------------|

| Befehl                  | Beschreibung   |
|-------------------------|--|
| DEFINE VIRTUALFSMAPPING | Zuordnung eines virtuellen Dateibereichs definieren.   |
| DELETE FILESPACE        | Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt. |
| EXPORT NODE             | Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.  |
| QUERY FILESPACE         | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.  |
| QUERY OCCUPANCY         | Zeigt Dateibereichsdaten anhand des Speicherpools an.  |

## RENAME NODE (Knoten umbenennen)

Verwenden Sie diesen Befehl, um einen Knoten umzubenennen.

Wenn Sie eine bestehende Knoten-ID einer anderen Person zuordnen, verwenden Sie den Befehl UPDATE NODE, um das Kennwort zu ändern.

Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol):

- Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.
- Benennen Sie einen Knoten nicht so um, dass er mit einer vorhandenen Benutzer-ID mit Administratorberechtigung übereinstimmt. Wenn Sie einen Knoten umbenennen und der Knotenname mit einer Benutzer-ID mit Administratorberechtigung übereinstimmt, stellen Sie möglicherweise ein nicht erwartetes Verhalten fest, weil automatische Kennwortänderungen dasselbe Kennwort zweimal aktualisieren. Dies hat zur Folge, dass das Kennwort für die Benutzer-ID mit Administratorberechtigung unbekannt ist. Es kann aber auch vorkommen, dass die Kennwortaktualisierung fehlschlägt.

Einschränkungen:

- Ein NAS-Knoten, für den eine entsprechende Einheit zum Versetzen von Daten definiert ist, kann nicht umbenannt werden. Verfügt die Einheit zum Versetzen von Daten über definierte Pfade, müssen die Pfade zuerst gelöscht werden.
- Wenn ein Knoten für die Replikation konfiguriert ist, kann er nicht umbenannt werden.

Wenn Sie einen Knoten in den Namen eines vorhandenen Administrators umbenennen, werden die Authentifizierungsmethode des Administrators und die Einstellung für SSLREQUIRED aktualisiert, damit sie mit dem Knoten übereinstimmen. Wenn ein Knoten und ein Administrator einen Namen gemeinsam nutzen und die Knotenauthentifizierungsmethode oder die Einstellung für SSLREQUIRED des Knotens geändert wird, werden die Administratoreinstellungen ebenfalls geändert. Sie müssen über die Berechtigung auf Systemebene verfügen, um die Knotenauthentifizierungsmethode oder die Einstellung für SSLREQUIRED des Knotens und einen Administrator mit demselben Namen zu aktualisieren.

## Berechtigungsklasse

Sie müssen über Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne verfügen, der der Clientknoten zugeordnet ist.

## Syntax

```
>>-REName Node--aktueller_Knotenname--neuer_Knotenname----->
. -SYNClapdelete---No----- .
>-----+-----+-----><
' -SYNClapdelete---+No--+- '
      '-Yes-'
```

## Parameter

aktueller\_Knotenname (Erforderlich)  
Gibt den Namen des Knotens an, der umbenannt werden soll.

neuer\_Knotenname (Erforderlich)

Gibt den neuen Namen des Knotens an. Die maximale Länge beträgt 64 Zeichen.

SYNCDapdelete

Gibt an, ob der Knotenname auf dem LDAP-Server (LDAP = Lightweight Directory Access Protocol) gelöscht und ersetzt wird.

Yes

Gibt an, dass der Knotenname gelöscht und ersetzt wird.

Einschränkung: Sie dürfen nicht den Wert YES angeben. (Der Wert YES ist nur für die Benutzer der vorherigen LDAP-Authentifizierungsmethode gültig, die in Kennwörter und Anmeldeverfahren verwaltet beschrieben wird.)

No

Gibt an, dass der Knotenname nicht gelöscht und ersetzt wird. Dies ist der Standardwert.

## Beispiel: Einen Knoten umbenennen

---

Den Knoten JOE in JOYCE umbenennen.

```
rename node joe joyce
```

## Beispiel: Einen Knoten umbenennen, der einen Namensbereich mit anderen Servern gemeinsam nutzt

---

Benennen Sie den Knoten JOYCE in JOE um und löschen Sie den vorherigen Namen auf den entsprechenden LDAP-Servern nicht.

```
rename node joyce joe
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für RENAME NODE

| Befehl      | Beschreibung  |
|-------------|---|
| QUERY NODE  | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an. |
| UPDATE NODE | Ändert die Attribute, die einem Clientknoten zugeordnet sind.                     |

### Zugehörige Tasks:

NAS-Dateiserverknoten verwalten

## RENAME SCRIPT (IBM Spectrum Protect-Prozedur umbenennen)

---

Mit diesem Befehl kann eine IBM Spectrum Protect-Prozedur umbenannt werden.

## Berechtigungsklasse

---

Für diesen Befehl ist die Bediener-, Maßnahmen-, System- oder Speicherberechtigung erforderlich.

## Syntax

---

```
>>-REName SCRIpt--aktueller_Prozedurname--neuer_Prozedurname---<
```

## Parameter

---

aktueller\_Prozedurname (Erforderlich)

Gibt den Namen der Prozedur an, die umbenannt werden soll.

neuer\_Prozedurname (Erforderlich)

Gibt den neuen Namen für die Prozedur an. Der Name kann bis zu 30 Zeichen umfassen.

## Beispiel: Ein Script umbenennen

---

SCRIPT1 in die neue Prozedur SCRIPT2 umbenennen.

```
rename script script1 script2
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für RENAME SCRIPT

| Befehl        | Beschreibung  |
|---------------|---|
| COPY SCRIPT   | Erstellt eine Kopie einer Prozedur.                           |
| DEFINE SCRIPT | Definiert eine Prozedur für den IBM Spectrum Protect-Server.  |
| DELETE SCRIPT | Löscht eine Prozedur oder einzelne Zeilen aus einer Prozedur. |
| QUERY SCRIPT  | Zeigt Informationen über Prozeduren an.                       |
| RUN           | Führt ein Script aus.   |
| UPDATE SCRIPT | Ändert Zeilen oder fügt Zeilen in einer Prozedur hinzu.       |

## RENAME SERVERGROUP (Servergruppe umbenennen)

Mit diesem Befehl kann eine Server-Gruppe umbenannt werden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-REName SERVERGroup--aktueller_Gruppenname--neuer_Gruppenname-><
```

### Parameter

aktueller\_Gruppenname (Erforderlich)

Gibt die Server-Gruppe an, die umbenannt werden soll.

neuer\_Gruppenname (Erforderlich)

Gibt den neuen Namen der Server-Gruppe an. Die maximale Länge des Namens beträgt 64 Zeichen.

### Beispiel: Eine Servergruppe umbenennen

Die Server-Gruppe WEST\_COMPLEX in BIG\_WEST umbenennen.

```
rename servergroup west_complex big_west
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RENAME SERVERGROUP

| Befehl             | Beschreibung                               |
|--------------------|--|
| COPY SERVERGROUP   | Erstellt eine Kopie einer Servergruppe.    |
| DEFINE SERVERGROUP | Definiert eine neue Servergruppe.          |
| DELETE SERVERGROUP | Löscht eine Servergruppe.                  |
| QUERY SERVERGROUP  | Zeigt Informationen über Servergruppen an. |
| UPDATE SERVERGROUP | Aktualisiert eine Servergruppe.            |

## RENAME STGPOOL (Den Namen eines Speicherpools ändern)

Mit diesem Befehl kann der Name eines Speicherpools geändert werden. Sie können Speicherpoolnamen ändern, um dieselben Namen auf einem Konfigurationsmanager und seinen verwalteten Servern zu verwenden.

Wenn Sie einen Speicherpool umbenennen, behalten alle Administratoren mit eingeschränkter Speicherberechtigung für den alten Speicherpool automatisch die eingeschränkte Speicherberechtigung für den umbenannten Speicherpool. Befindet sich der umbenannte Speicherpool in einer Speicherpoolhierarchie, wird die Hierarchie beibehalten. Sie müssen die Verwaltungsklasse oder Kopiengruppe aktualisieren, um den neuen Speicherpoolnamen als Ziel für Dateien anzugeben.

Sind Prozesse aktiv, wenn ein Speicherpool umbenannt wird, wird der alte Name möglicherweise noch in Nachrichten oder Abfragen für diese Prozesse angezeigt.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-REName STGpool--aktueller_Poolname--neuer_Poolname-----><
```

## Parameter

aktueller\_Poolname (Erforderlich)

Gibt den Speicherpool an, der umbenannt werden soll.

neuer\_Poolname (Erforderlich)

Gibt den neuen Namen des Speicherpools an. Die maximale Länge des Namens beträgt 30 Zeichen.

## Beispiel: Den Namen eines Speicherpools ändern

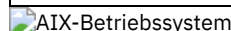
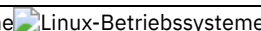
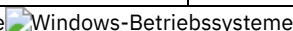
Speicherpool STGPOOLA umbenennen in STGPOOLB:

```
rename stgpool stgpoola stgpoolb
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RENAME STGPOOL

| Befehl          | Beschreibung   |
|-----------------|--|
| BACKUP STGPOOL  | Sichert einen primären Speicherpool in einem Kopierspeicherpool.                   |
| DEFINE STGPOOL  | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern. |
| DELETE STGPOOL  | Löscht einen Speicherpool aus dem Serverspeicher.                                  |
| QUERY STGPOOL   | Zeigt Informationen zu Speicherpools an.   |
| RESTORE STGPOOL | Schreibt Dateien aus Kopierspeicherpools in einen primären Speicherpool zurück.    |
| UPDATE STGPOOL  | Ändert die Attribute eines Speicherpools.  |

## REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)

Mit diesem Befehl können deduplizierte Speicherbereiche in einem Verzeichniscontainerspeicherpool repariert werden. Beschädigte deduplizierte Speicherbereiche werden mit Bereichen repariert, die auf dem Zielreplikationsserver oder in Containerkopierspeicherpools auf demselben Server gesichert werden.

Einschränkungen:

- Sie können den Befehl REPAIR STGPOOL nur ausgeben, wenn Sie bereits den Befehl PROTECT STGPOOL ausgegeben haben, um Daten in einem anderen Speicherpool auf einem Zielreplikationsserver oder auf demselben Server zu sichern.
- Wenn Sie einen Verzeichniscontainerspeicherpool mithilfe des Replikationsservers reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:
  - Der Zielspeicherpool ist nicht verfügbar.
  - Der Zielspeicherpool ist beschädigt.
  - Ein Netzausfall tritt auf.
- Wenn Sie einen Verzeichniscontainerspeicherpool mithilfe von Containerkopierspeicherpools reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:
  - Der Containerkopierspeicherpool ist nicht verfügbar.
  - Der Containerkopierspeicherpool ist beschädigt.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax, wenn die Quelle der Replikationsserver ist

```
                .-SRCLOCation-----Replserver-.
>>-REPAir STGPool--Poolname--+-----+----->
                '-SRCLOCation-----Replserver-'

                .-MAXSESSions-----1-----
>--+-----+-----+----->
                '-MAXSESSions-----Anzahl Sitzungen--'

                .-Preview-----No----- .-Wait-----No-----
>--+-----+-----+-----<
                '-Preview-----+No--+-' '-Wait-----+No--+-'
                    '-Yes-'                '-Yes-'
```

### Syntax, wenn die Quelle ein Speicherpool auf demselben Server ist

```
                .-Preview-----No----- .-Wait-----No-----
>>-REPAir STGPool--Poolname--SRCLOCation-----Local----->
                '-Preview-----+No--+-' '-Wait-----+No--+-'
                    '-Yes-'                '-Yes-'
```

## Parameter

### Poolname (Erforderlich)

Gibt den Namen des Verzeichniscontainerspeicherpools an, der die Daten enthält, die repariert werden müssen.

### SRCLOCation

Gibt die Quellenposition an, die verwendet wird, um die Daten zu reparieren. Der Standardwert ist REPLSERVER. Dieser Parameter ist nur erforderlich, wenn sich die Quellenposition auf demselben Server befindet. Sie können einen der folgenden Werte angeben:

#### Local

Gibt an, dass die Daten mithilfe von Containerkopierspeicherpools auf demselben Server repariert werden.

#### Replserver

Gibt an, dass die Daten mithilfe eines Verzeichniscontainerspeicherpools auf dem Zielreplikationsserver repariert werden.

### MAXSESSions

Gibt die maximale Anzahl der Datensitzungen an, die Daten an einen Zielsender senden können. Dieser Parameter ist wahlfrei, wenn Sie Daten mithilfe eines Replikationssservers reparieren.

Der angegebene Wert kann im Bereich 1 - 20 liegen. Der Standardwert ist 1. Wenn Sie die Anzahl der Sitzungen erhöhen, können Sie den Speicherpool schneller reparieren.

Wenn Sie einen Wert für den Parameter MAXSESSIONS definieren, stellen Sie sicher, dass die verfügbare Bandbreite und die Prozessorkapazität des Quellen- und Zielservers ausreichend sind.

#### Tipps:

- Wird ein Befehl QUERY SESSION ausgegeben, kann die Gesamtzahl der Sitzungen die Anzahl der Datensitzungen überschreiten.
- Die Anzahl der Sitzungen, die für die Reparatur von Speicherpools verwendet werden, hängt vom Datenvolumen ab, das repariert wird. Wird nur ein geringes Datenvolumen repariert, wird durch die Erhöhung der Anzahl Sitzungen kein Vorteil erzielt.

### Preview

Gibt an, ob eine Voranzeige der Daten aufgerufen werden soll oder ob die Daten repariert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

#### No

Gibt an, dass die Daten in dem Speicherpool repariert, aber nicht vorangezeigt werden.

#### Yes

Gibt an, dass die Daten vorangezeigt, aber nicht repariert werden.

Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Reparaturverarbeitung für den Speicherpool beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können diesen Parameter nur in einer Verwaltungsbefehlszeile angeben. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass die Befehlsprozesse im Hintergrund ausgeführt werden. Um die Hintergrundverarbeitung des Befehls REPAIR STGPOOL zu überwachen, geben Sie den Befehl QUERY PROCESS aus.

Yes

Gibt an, dass die Befehlsprozesse im Vordergrund ausgeführt werden. Nachrichten werden erst angezeigt, wenn die Verarbeitung des Befehls beendet ist.

## Beispiel: Einen Speicherpool reparieren und die Daten voranzeigen

Einen Speicherpool mit dem Namen POOL1 reparieren und die Daten voranzeigen.

```
repair stgpool pool1 preview=yes
```

## Beispiel: Einen Speicherpool reparieren und eine maximale Anzahl Sitzungen angeben

Einen Speicherpool mit dem Namen POOL1 reparieren und ein Maximum von 10 Sitzungen angeben.

```
repair stgpool pool1 maxsessions=10
```

## Beispiel: Einen Speicherpool mit Band reparieren

Einen Speicherpool mit dem Namen POOL1 reparieren und 'Local' für die Quellenposition angeben.

```
repair stgpool pool1 SRCLOCATION=local
```

Tabelle 1. Zugehörige Befehle für REPAIR STGPOOL

| Befehl                                | Beschreibung  |
|---------------------------------------|---|
| DEFINE STGPOOL (Verzeichniscontainer) | Definiert einen Verzeichniscontainerspeicherpool.   |
| DEFINE STGPOOL (Containerkopie)       | Definiert einen Containerkopierspeicherpool, in dem Kopien von Daten aus einem Verzeichniscontainerspeicherpool gespeichert werden. |
| DEFINE STGPOOLDIRECTORY               | Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool.                             |
| PROTECT STGPOOL                       | Schützt einen Verzeichniscontainerspeicherpool.   |

## REPLICATE NODE (Daten in Dateibereichen replizieren, die zu einem Clientknoten gehören)

Verwenden Sie diesen Befehl, um Daten in Dateibereichen zu replizieren, die zu einem oder mehreren Clientknoten oder zu definierten Gruppen von Clientknoten gehören.

Wenn Sie diesen Befehl ausgeben, wird ein Prozess gestartet, in dem Daten, die zu den angegebenen Clientknoten gehören, gemäß Replikationsregeln repliziert werden. Dateien, die nicht mehr auf dem Quellenreplikationsserver gespeichert werden, aber auf dem Zielreplikationsserver vorhanden sind, werden während dieses Prozesses gelöscht.

Tipp: Vermeiden Sie Konflikte bei der Verwaltung von Administrator-IDs und Clientoptionsgruppen, indem Sie die IDs und Optionsgruppen, die auf den Zielsver repliziert werden, und die IDs und Optionsgruppen angeben, die in einer unternehmensweiten Konfiguration verwaltet werden. Sie können keine Benutzer-ID mit Administratorberechtigung für einen registrierten Knoten definieren, wenn eine Administrator-ID für denselben Knoten vorhanden ist.

Wenn ein Knotenreplikationsprozess bereits für einen mit diesem Befehl angegebenen Clientknoten ausgeführt wird, wird der Knoten übersprungen und die Replikation für andere Knoten gestartet, die für die Replikation aktiviert sind.

Nach der Beendigung des Knotenreplikationsprozesses kann ein Wiederherstellungsprozess auf dem Zielreplikationsserver gestartet werden. Dateien werden nur wiederhergestellt, wenn alle folgenden Bedingungen erfüllt sind:

- Version 7.1.1 oder höher ist auf dem Quellen- und Zielreplikationsserver installiert.
- Der Systemparameter REPLRECOVERDAMAGED ist auf ON gesetzt. Der Systemparameter kann mit dem Befehl SET REPLRECOVERDAMAGED definiert werden.

- Der Quellenserver schließt mindestens eine Datei ein, die auf dem Knoten, der repliziert wird, als beschädigt markiert ist.
- Die Knotendaten wurden repliziert, bevor die Beschädigung aufgetreten ist.

In der folgenden Tabelle wird beschrieben, wie sich Einstellungen auf die Wiederherstellung beschädigter, replizierter Dateien auswirken.

Einschränkung: Sie können den Parameter REPLRECOVERDAMAGED nicht für Verzeichniscontainer- oder Cloudspeicherpools verwenden.

Tabelle 1. Einstellungen, die sich auf die Wiederherstellung beschädigter Dateien auswirken

| Einstellung für den Systemparameter REPLRECOVERDAMAGED | Wert des Parameters RECOVERDAMAGED im Befehl REPLICATE NODE | Wert des Parameters RECOVERDAMAGED in den Befehlen REGISTER NODE und UPDATE NODE | Ergebnis  |
|--|---|--|---|
| OFF  | YES, NO oder nicht angegeben                                | YES oder NO  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.    |
| OFF  | ONLY  | YES oder NO  | Eine Fehlernachricht wird angezeigt, weil Dateien nicht wiederhergestellt werden können, wenn der Systemparameter REPLRECOVERDAMAGED auf OFF gesetzt ist. |
| ON   | YES   | YES oder NO  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.          |
| ON   | NO  | YES oder NO  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.    |
| ON   | ONLY  | YES oder NO  | Beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt, aber es findet keine Standardknotenreplikation statt.                            |
| ON   | Nicht angegeben   | YES  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.          |
| ON   | Nicht angegeben   | NO   | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.    |

Tipp: Wenn der Befehl QUERY PROCESS während der Knotenreplikation ausgegeben wird, kann die Ausgabe nicht erwartete Ergebnisse für die Anzahl der abgeschlossenen Replikationen anzeigen. Der Grund liegt darin, dass zu Knotenreplikationszwecken für jeden Dateibereich angenommen wird, dass er drei logische Dateibereiche enthält:

- Einen Bereich für Sicherungsobjekte
- Einen Bereich für Archivierungsobjekte
- Einen Bereich für speicherverwaltete Objekte

Standardmäßig generiert der Befehl QUERY PROCESS Ergebnisse für jeden logischen Dateibereich. Andere Faktoren haben ebenfalls Auswirkungen auf die Ausgabe des Befehls QUERY PROCESS:

- Verfügt ein Dateibereich über eine Replikationsregel, die auf NONE gesetzt ist, wird der Dateibereich nicht in der Anzahl der Dateibereiche berücksichtigt, die verarbeitet werden.
- Wenn Sie im Befehl REPLICATE NODE Datentypen angeben, werden nur diese Datentypen in der Anzahl der Dateibereiche berücksichtigt, die verarbeitet werden, abzüglich aller Dateibereiche, die ausgeschlossen sind.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.


## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax





2. Geben Sie nicht die FSID an, wenn Sie Platzhalterzeichen für den Clientknotenamen verwenden.
3.  Linux-Betriebssysteme Der Parameter TRANSFERMETHOD ist nur auf Betriebssystemen Linux x86\_64 verfügbar.

## Parameter

---

### Knotenname oder Knotengruppenname (Erforderlich)

Gibt den Namen des Clientknotens oder der definierten Gruppe von Clientknoten an, dessen bzw. deren Daten repliziert werden sollen. Sie können auch eine Kombination von Clientknotenamen und Clientknotengruppenamen angeben. Sollen mehrere Clientknotenamen oder Clientknotengruppenamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Sie können Platzhalterzeichen für Clientknotenamen, aber nicht für Clientknotengruppenamen verwenden. Die Replikationsregeln für alle Dateibereiche in den angegebenen Clientknoten werden überprüft.

### Dateibereichsname oder FSID

Gibt den Namen des Dateibereichs oder die ID des Dateibereichs (FSID) an, der repliziert werden soll. Ein Name oder eine FSID ist optional. Wenn Sie keinen Namen oder keine FSID angeben, können alle Daten in allen Dateibereichen für die angegebenen Clientknoten für die Replikation ausgewählt werden.

### Dateibereichsname

Gibt den Namen des Dateibereichs an, der zu replizierende Daten enthält. Bei Dateibereichsnamen muss die Groß-/Kleinschreibung berücksichtigt werden. Um die korrekte Schreibweise für den Dateibereich zu bestimmen, geben Sie den Befehl `QUERY FILESPACE` aus. Mehrere Namen sind ohne Leerzeichen durch Kommas voneinander zu trennen. Wenn Sie einen Namen angeben, können Sie Platzhalterzeichen verwenden.

Ein Server, der über Clients mit Dateibereichen verfügt, die für Unicode aktiviert sind, muss möglicherweise den Dateibereichsnamen konvertieren. Beispielsweise muss der Server gegebenenfalls einen Namen aus der Zeichenumsetzungstabelle des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich in der Beschreibung des Parameters `NAMETYPE`. Geben Sie keinen Dateibereichsnamen an oder geben Sie ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter `CODETYPE` verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

### FSID

Gibt die Dateibereichs-ID für den zu replizierenden Dateibereich an. Der Server verwendet FSIDs zum Lokalisieren der Dateibereiche, die repliziert werden sollen. Um die FSID für einen Dateibereich zu bestimmen, geben Sie den Befehl `QUERY FILESPACE` aus. Mehrere FSIDs sind ohne Leerzeichen durch Kommas voneinander zu trennen. Wenn Sie eine FSID angeben, muss der Wert des Parameters `NAMETYPE` `FSID` lauten.

### `NAMETYPE`

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Sie können diesen Parameter für IBM Spectrum Protect-Clients verwenden, die für Unicode aktiviert sind und die über die Betriebssysteme Windows, Macintosh OS X und NetWare verfügen.

Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen eingeben. Der Standardwert lautet `SERVER`. Sie können einen der folgenden Werte angeben:

#### `SERVER`

Der Server verwendet die Zeichenumsetzungstabelle des Servers, um Dateibereichsnamen zu interpretieren.

#### `UNICODE`

Der Server konvertiert Dateibereichsnamen aus der Serverzeichenumsetzungstabelle in die Zeichenumsetzungstabelle UTF-8. Der Erfolg der Konvertierung hängt von den Zeichen in dem Namen und der Zeichenumsetzungstabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetzungstabelle nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

#### `FSID`

Der Server interpretiert Dateibereichsnamen unter Verwendung ihrer Dateibereichs-IDs.

### `CODETYPE`

Gibt den Typ der Dateibereiche an, die bei der Knotenreplikationsverarbeitung berücksichtigt werden sollen. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben. Der Standardwert lautet `BOTH`. Dieser Standardwert gibt an, dass Dateibereiche unabhängig vom Typ der Codepage eingeschlossen werden. Sie können einen der folgenden Werte angeben:

#### `UNICODE`

Gibt Dateibereiche an, die nur in Unicode sind.

#### `NONUNICODE`

Gibt Dateibereiche an, die nicht in Unicode sind.

#### `BOTH`

Gibt alle Dateibereiche unabhängig von der Art der Zeichenumsetzungstabelle an.

### `DATATYPE`

Gibt den Typ der Daten an, die repliziert werden sollen. Daten werden gemäß der Replikationsregel repliziert, die für den Datentyp gilt. Dieser Parameter ist wahlfrei. Sie können einen oder mehrere Datentypen angeben. Wenn Sie keinen Datentyp angeben, werden alle Sicherungsdaten, Archivierungsdaten und speicherverwaltete Daten repliziert. Mehrere Datentypen sind ohne Leerzeichen durch Kommas voneinander zu trennen. Sie können keine Platzhalterzeichen verwenden. Sie können einen der folgenden Werte angeben:

#### ALL

Repliziert alle Sicherungsdaten, Archivierungsdaten und speicherverwaltete Daten in einem Dateibereich gemäß der Regel, die dem Datentyp zugeordnet ist. Beispiel: Angenommen, NODE1 hat einen einzelnen Dateibereich. Es gelten die folgenden Replikationsregeln:

- Die Dateibereichsregeln für Sicherungs- und Archivierungsdaten in dem Dateibereich sind auf ALL\_DATA gesetzt.
- Die Dateibereichsregel für speicherverwaltete Daten ist auf DEFAULT gesetzt.
- Die Clientknotenregel für speicherverwaltete Daten ist auf NONE gesetzt.

Wenn Sie den Befehl `REPLICATE NODE NODE1 DATATYPE=ALL` ausgeben, werden nur Sicherungs- und Archivierungsdaten repliziert.

#### BACKUP

Repliziert aktive und inaktive Sicherungsdaten in einem Dateibereich, wenn die steuernde Replikationsregel ALL\_DATA, ACTIVE\_DATA, ALL\_DATA\_HIGH\_PRIORITY oder ACTIVE\_DATA\_HIGH\_PRIORITY lautet.

#### BACKUPActive

Repliziert nur aktive Sicherungsdaten in einem Dateibereich, wenn die steuernde Replikationsregel ACTIVE\_DATA oder ACTIVE\_DATA\_HIGH\_PRIORITY lautet.

#### ARCHive

Repliziert nur Archivierungsdaten in einem Dateibereich, wenn die steuernde Replikationsregel ALL\_DATA oder ALL\_DATA\_HIGH\_PRIORITY lautet.

#### SPACEManaged

Repliziert nur speicherverwaltete Daten in einem Dateibereich, wenn die steuernde Replikationsregel ALL\_DATA oder ALL\_DATA\_HIGH\_PRIORITY lautet.

#### PRIority

Gibt die zu replizierenden Daten auf der Basis der Priorität der Replikationsregel an. Sie können einen der folgenden Werte angeben:

##### All

Repliziert alle Daten in einem Dateibereich, wenn die steuernde Replikationsregel ALL\_DATA, ACTIVE\_DATA, ALL\_DATA\_HIGH\_PRIORITY oder ACTIVE\_DATA\_HIGH\_PRIORITY lautet.

##### High

Repliziert nur Daten in einem Dateibereich, die die steuernde Replikationsregel ALL\_DATA\_HIGH\_PRIORITY oder ACTIVE\_DATA\_HIGH\_PRIORITY haben.

##### Normal

Repliziert nur Daten in einem Dateibereich, die die steuernde Replikationsregel ALL\_DATA oder ACTIVE\_DATA haben.

#### MAXSESSions

Gibt die maximal zulässige Anzahl der Datensitzungen an, die zum Senden von Daten an einen Zielreplikationsserver verwendet werden sollen. Dieser Parameter ist wahlfrei. Der Wert kann zwischen 1 und 99 liegen. Der Standardwert ist 10.

Wird die Anzahl der Sitzungen erhöht, kann der Durchsatz bei der Knotenreplikation verbessert werden.

Berücksichtigen Sie bei der Festlegung dieses Werts die Anzahl der logischen und physischen Laufwerke, die dem Replikationsprozess zugeordnet werden können. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl der verfügbaren Mountpunkte und Laufwerke hängt von den folgenden Faktoren ab:

- Andere IBM Spectrum Protect-Aktivitäten und Systemaktivitäten
- Die Grenzwerte für Ladeanforderungen der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff, die betroffen sind

Stellen Sie sicher, dass genügend Mountpunkte und Laufwerke verfügbar sind, damit die Knotenreplikationsprozesse ausgeführt werden können. Jede Replikationssitzung benötigt möglicherweise für Speicherpooldatenträger einen Mountpunkt auf dem Quellen- und Zielreplikationsserver. Lautet der Einheitentyp nicht FILE, benötigt jede Sitzung möglicherweise auch ein Laufwerk auf dem Quellen- und Zielreplikationsserver.

Berücksichtigen Sie bei der Festlegung eines Werts für MAXSESSIONS auch die verfügbare Bandbreite und die Prozessorkapazität des Quellen- und Zielreplikationsservers.

Tipp:

- Der vom Parameter MAXSESSIONS angegebene Wert gilt nur für Datensitzungen. Datensitzungen sind Sitzungen, in denen Daten an einen Zielreplikationsserver gesendet werden. Wird jedoch ein Befehl QUERY SESSION ausgegeben, kann die Gesamtzahl der Sitzungen die Anzahl der Datensitzungen überschreiten. Die Differenz resultiert aus kurzen Steuersitzungen, die zum Abfragen und Definieren von Replikationsoperationen verwendet werden.
- Der Wert des Parameters MAXSESSIONS stellt die maximal zulässige Anzahl Sitzungen dar. Die Anzahl der Sitzungen, die für die Replikation verwendet werden, hängt vom Datenvolumen ab, das repliziert werden soll. Wird nur ein geringes Datenvolumen repliziert, wird durch die Erhöhung der Anzahl Sitzungen kein Vorteil erzielt. Die Gesamtzahl der Sitzungen kann kleiner als der Wert sein, der mit dem Parameter MAXSESSIONS angegeben wird.

#### Preview

Gibt an, ob eine Voranzeige der Daten aufgerufen werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass die Daten auf den Zielsever repliziert, aber nicht vorangezeigt werden.

Yes

Gibt an, dass die Daten vorangezeigt, aber nicht repliziert werden. Wenn Sie PREVIEW=YES angeben, werden nur Datenträger, die physisch geladen werden müssen, wie z. B. Banddatenträger, angezeigt. Datenträger, die Speicherpools zugeordnet sind, die die Einheitenklasse FILE haben, werden nicht angezeigt.

Die folgenden Informationen werden in der Ausgabe angezeigt:

- Die Namen der Clientknoten, deren Daten repliziert würden.
- Die Anzahl der Dateien, die repliziert oder gelöscht würden.
- Die geschätzte Zeit für die Ausführung des Knotenreplikationsprozesses.
- Eine Liste der Datenträger, die geladen würden.
- Eine Zusammenfassung der Informationen zu replizierten, beschädigten Daten. In der Zusammenfassung werden die Anzahl der Knoten, der Dateibereiche, der Dateien und der Byte aufgelistet, die während eines Replikationswiederherstellungsprozesses wiederhergestellt werden können. Die Zusammenfassung wird nur angezeigt, wenn RECOVERDAMAGED=YES oder RECOVERDAMAGED=ONLY angegeben ist.

Wenn die Daten des mit dem Befehl REPLICATE NODE angegebenen Clientknotens nie repliziert wurden und Sie PREVIEW=YES angeben, werden der Knoten und seine Dateibereiche automatisch auf dem Zielreplikationsserver definiert.

#### LISTfiles

Gibt an, ob die Namen der Dateien aufgelistet werden sollen, die repliziert würden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Die Angabe dieses Parameters bedeutet, dass der Parameter WAIT auf YES gesetzt ist und Sie den Parameter WAIT nicht an der Serverkonsole ausgeben können.

Sie können einen der folgenden Werte angeben:

No

Gibt an, dass die Namen der Dateien, die repliziert würden, nicht angezeigt werden.

Yes

Gibt an, dass die Namen der Dateien, die repliziert würden, angezeigt werden.

#### Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass der Befehl im Hintergrund verarbeitet wird. Um die Hintergrundverarbeitung des Befehls REPLICATE NODE zu überwachen, geben Sie den Befehl QUERY PROCESS aus.

Yes

Gibt an, dass der Befehl im Vordergrund verarbeitet wird. Nachrichten werden erst angezeigt, wenn die Verarbeitung des Befehls beendet ist. Sie können nicht WAIT=YES an der Serverkonsole angeben.

#### RECOVERDamaged

Gibt an, ob nach der Beendigung des Knotenreplikationsprozesses ein Wiederherstellungsprozess auf einem Zielreplikationsserver gestartet wird. Dieser Parameter ist optional und überschreibt den Wert, den Sie bei der Definition oder Aktualisierung eines Knotens für den Parameter RECOVERDamaged angegeben haben. Sie können einen der folgenden Werte angeben:

Yes

Gibt an, dass ein Replikationsprozess gestartet wird, um beschädigte Dateien wiederherzustellen. Dies gilt jedoch nur, wenn die Einstellung für den Systemparameter REPLRECOVERDAMAGED ON lautet. Lautet die Einstellung OFF, werden beschädigte Dateien nicht wiederhergestellt.

No

Gibt an, dass beschädigte Dateien nicht wiederhergestellt werden.

Only

Gibt an, dass ein Replikationsprozess nur zum Zweck der Wiederherstellung beschädigter Dateien gestartet wird. Dies gilt jedoch nur, wenn die Einstellung für den Systemparameter REPLRECOVERDAMAGED ON lautet. Lautet die Einstellung OFF, werden beschädigte Dateien nicht wiederhergestellt, und Sie erhalten eine Benachrichtigung, dass die Wiederherstellung nicht gestartet wurde.

Einschränkung: Wenn Sie eine ungültige Kombination von Werten und Einstellungen für die Dateiwiederherstellung angeben, wird die Replikation gestoppt und eine Fehlermeldung angezeigt.

#### FORCEREconcile

Gibt an, ob alle Dateien auf dem Quellenreplikationsserver mit den Dateien auf dem Zielreplikationsserver verglichen und die Unterschiede zwischen ihnen synchronisiert werden sollen. Vor Version 7.1.1 war dieses Verhalten der Standardwert für die Replikationsverarbeitung. Wenn IBM® Tivoli Storage Manager Version 7.1.1 oder höher auf dem Quellen- und Zielreplikationsserver installiert ist, wird während der Erstreplikation automatisch ein Abgleich ausgeführt. Nach der Erstreplikation können Sie diesen Parameter aus folgenden Gründen verwenden:

- Um Dateien auf dem Quellen- und dem Zielreplikationsserver zu synchronisieren, wenn sie unterschiedlich sind.
- Um inaktive Dateien, die übersprungen wurden, zu replizieren, wenn die Replikationsregeln von ACTIVE\_DATA in ALL\_DATA geändert werden.
- Um inaktive Dateien auf dem Zielreplikationsserver zu löschen, wenn die Replikationsregeln von ALL\_DATA in ACTIVE\_DATA geändert werden.
- Um sicherzustellen, dass nur aktive Daten repliziert werden, wenn Sie die Replikationsregel ACTIVE\_DATA verwenden, sodass der Zielreplikationsserver nur über aktive Dateien verfügt.
- Um die Dateien zu resynchronisieren, damit der Zielreplikationsserver dieselben Dateien wie der Quellenreplikationsserver hat, wenn Sie zuvor oder derzeit die Maßnahmen auf dem Zielreplikationsserver zum Verwalten replizierter Dateien verwendet haben bzw. verwenden.
- Um die Dateien auf dem Quellen- und dem Zielreplikationsserver zu resynchronisieren, wenn die Datenbank mit einer anderen Methode als dem Befehl DSMSEV RESTORE DB auf einen früheren Zeitpunkt zurückgesetzt wird.
- Um Dateien an die neue Verwaltungsklasse auf dem Zielreplikationsserver erneut zu binden, wenn diese Verwaltungsklasse nicht vorhanden war, als die Dateien repliziert wurden. Sie müssen die Maßnahmen verwenden, die auf dem Zielreplikationsserver definiert sind, um replizierte Dateien zu verwalten.

Hinweis: Wenn die Regel ACTIVE\_DATA zugeordnet ist, wird ein Abgleich nur für aktive Dateien auf dem Quellenreplikationsserver ausgeführt.

Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:


No

Gibt an, dass die Replikationsverarbeitung keinen Abgleich erzwingt, um alle Dateien auf dem Quellenreplikationsserver mit Dateien auf dem Zielreplikationsserver zu vergleichen. Stattdessen verfolgt die Replikationsverarbeitung Dateiänderungen auf dem Quellenreplikationsserver seit der letzten Replikation und synchronisiert diese Änderungen auf dem Zielreplikationsserver. NO ist der Standardwert.

Yes

Gibt an, dass die Replikationsverarbeitung einen Abgleich erzwingt, um alle Dateien auf dem Quellenreplikationsserver mit Dateien auf dem Zielreplikationsserver zu vergleichen, und die Dateien auf dem Zielreplikationsserver mit den Dateien auf dem Quellenreplikationsserver synchronisiert.

#### Linux-BetriebssystemeTRANSFERMethod

 Linux-BetriebssystemeGibt die Methode an, die für die Datenübertragung zwischen Servern verwendet wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

Tcpip

Gibt an, dass TCP/IP für die Übertragung von Daten verwendet wird. Dieser Wert ist der Standardwert.

Fasp

Gibt an, dass die Aspera FASP-Technologie (Fast Adaptive Secure Protocol) für die Übertragung von Daten verwendet wird. Mit der Aspera FASP-Technologie kann die Datenübertragung in einem Weitverkehrsnetz (WAN) optimiert werden. Wenn Sie TRANSFERMETHOD=FASP angeben, werden alle Parameter TRANSFERMETHOD überschrieben, die Sie im Befehl DEFINE SERVER oder UPDATE SERVER angegeben haben.

Einschränkungen:

- Mit der Aspera FASP-Technologie können nur Daten übertragen werden, die in einem Verzeichniscontainerspeicherpool gespeichert sind. Zur Übertragung von Daten, die nicht in einem Verzeichniscontainerspeicherpool gespeichert sind, wird TCP/IP verwendet.
- Bevor Sie die Aspera FASP-Technologie aktivieren, müssen Sie bestimmen, ob die Technologie für Ihre Systemumgebung geeignet ist, und die entsprechenden Lizenzen installieren. Anweisungen finden Sie unter

- Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann. Wenn die Lizenzen fehlen oder abgelaufen sind, schlägt die Knotenreplikation fehl.
- Wenn die WAN-Leistung Ihre Geschäftsanforderungen erfüllt, aktivieren Sie nicht die Aspera FASP-Technologie.

## Beispiel: Daten nach Datentyp und Priorität replizieren

Aktive Sicherungsdaten und Archivierungsdaten mit hoher Priorität replizieren, die zu allen Clientknoten in der Gruppe PAYROLL gehören.

```
replicate node payroll datatype=backupactive,archive priority=high
```

## Beispiel: Alle Daten, die zu einem Knoten gehören, gemäß den zugeordneten Replikationsregeln replizieren

NODE1 hat einen einzelnen Dateibereich. Es gelten die folgenden Replikationsregeln:

- Dateibereichsregeln:
  - Sicherungsdaten: ACTIVE\_DATA
  - Archivierungsdaten: DEFAULT
  - Speicherverwaltete Daten: DEFAULT
- Clientknotenregeln:
  - Sicherungsdaten: DEFAULT
  - Archivierungsdaten: ALL\_DATA\_HIGH\_PRIORITY
  - Speicherverwaltete Daten: DEFAULT
- Serverregeln:
  - Sicherungsdaten: ALL\_DATA
  - Archivierungsdaten: ALL\_DATA
  - Speicherverwaltete Daten: NONE

```
replicate node nodel priority=all
```

Aktive Sicherungsdaten in dem Dateibereich werden mit normaler Priorität repliziert. Archivierungsdaten werden mit hoher Priorität repliziert. Speicherverwaltete Daten werden nicht repliziert.

## Beispiel: Beschädigte Dateien ohne Starten des vollständigen Replikationsprozesses wiederherstellen



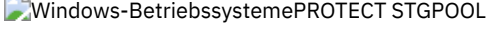
Alle beschädigten Dateien auf den Clientknoten der Group PAYROLL wiederherstellen, ohne den vollständigen Replikationsprozess zu starten. Sicherstellen, dass die Einstellung für den Systemparameter REPLRECOVERDAMAGED ON lautet. Anschließend den folgenden Befehl ausgeben:

```
replicate node payroll recoverdamaged=only
```

## Zugehörige Befehle

Tabelle 2. Zugehörige Befehle für REPLICATE NODE

| Befehl             | Beschreibung   |
|--------------------|--|
| CANCEL PROCESS     | Bricht einen Serverhintergrundprozess ab.  |
| CANCEL REPLICATION | Bricht Knotenreplikationsprozesse ab.  |
| QUERY FILESPACE    | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.                                      |
| QUERY NODE         | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.                                    |
| QUERY REPLICATION  | Zeigt Informationen zu Knotenreplikationsprozessen an.   |
| QUERY REPLNODE     | Zeigt Informationen zum Replikationsstatus eines Clientknotens an.   |
| QUERY REPLRULE     | Zeigt Informationen zu Knotenreplikationsregeln an.  |
| QUERY SERVER       | Zeigt Informationen über Server an.  |
| QUERY STATUS       | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

| Befehl   | Beschreibung   |
|--|--|
| REGISTER NODE  | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.  |
| REMOVE REPLNODE  | Entfernt einen Knoten aus der Replikation.   |
|  <br> PROTECT STGPOOL | Schützt einen Verzeichniscontainerspeicherpool.  |
| SET REPLRECOVERDAMAGED   | Gibt an, ob die Knotenreplikation aktiviert ist, um beschädigte Dateien durch einen Zielreplikationsserver wiederherzustellen. |
| UPDATE FILESPACE   | Ändert Knotenreplikationsregeln für Dateibereiche.   |
| UPDATE NODE  | Ändert die Attribute, die einem Clientknoten zugeordnet sind.  |
| UPDATE REPLRULE  | Aktiviert oder inaktiviert Replikationsregeln.   |
| VALIDATE REPLICATION   | Überprüft die Replikation für Dateibereiche und Datentypen.  |

## REPLY (Verarbeitung einer Anforderung fortsetzen)

Mit Hilfe dieses Befehls und einer Identifikationsnummer kann der Server darüber informiert werden, dass eine angeforderte Operation beendet wurde. Nicht alle Serveranforderungen erfordern eine Antwort. Dieser Befehl ist nur erforderlich, wenn die Anforderungsnachricht ausdrücklich angibt, dass eine Antwort benötigt wird.

### Berechtigungsklasse

Für diesen Befehl ist die System- oder die Bedienerberechtigung erforderlich.

### Syntax

```
>>-REPLY--Anforderungsnummer----->
>--+-----+-----<
  '-LABEL----Datenträgerkennsatz-'
```

### Parameter

#### Anforderungsnummer (**Erforderlich**)

Gibt die Identifikationsnummer der Anforderung an.

#### LABEL

Gibt den Kennsatz an, der auf einen Datenträger geschrieben werden soll, wenn Sie auf eine Nachricht von einem Prozess des Befehls LABEL LIBVOLUME antworten. Dieser Parameter ist wahlfrei.

### Beispiel: Auf eine Anforderung antworten

Eine Antwortanforderung mit 3 als Anforderungsnummer beantworten.

```
reply 3
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für REPLY

| Befehl         | Beschreibung  |
|----------------|---|
| CANCEL REQUEST | Bricht anstehende Datenträgerladeanforderungen ab.              |
| QUERY REQUEST  | Zeigt Informationen über alle anstehenden Ladeanforderungen an. |

## RESET PASSEXP (Kennwortablaufdauer zurücksetzen)

Verwenden Sie den Befehl RESET PASSEXP, um die Kennwortablaufdauer für Kennwörter von Administratoren und Clientknoten auf die allgemeine Kennwortablaufdauer zurückzusetzen. Der Befehl RESET PASSEXP gilt nicht für Kennwörter, die auf einem LDAP-Verzeichnisserver gespeichert werden.

Einschränkung: Sie können die Kennwortablaufdauer nicht mit dem Befehl SET PASSEXP auf eine allgemeine Kennwortablaufdauer zurücksetzen.

Verwenden Sie den Befehl QUERY STATUS, um die allgemeine Kennwortablaufdauer anzuzeigen.

Einschränkung: Wird der Parameter NODE oder ADMIN nicht angegeben, wird die Kennwortablaufdauer für alle Clientknoten und Administratoren zurückgesetzt.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-RESet PASSExp-----+-----+----->
|           .-,------. |
|           v             | |
| '-Node-----Knotenname-+-'
>-+-----+-----+-----><
|           .-,------. |
|           v             | |
| '-Admin-----Administratorname-+-'
```

## Parameter

### Node

Gibt den Namen des Knotens an, dessen Kennwortablaufdauer zurückgesetzt werden soll. Soll eine Liste mit Knoten angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Dieser Parameter ist wahlfrei.

### Admin

Gibt den Namen des Administrators an, dessen Kennwortablaufdauer zurückgesetzt werden soll. Soll eine Liste mit Administratoren angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Dieser Parameter ist wahlfrei.

## Beispiel: Die Kennwortablaufdauer für bestimmte Clientknoten zurücksetzen

Die Kennwortablaufdauer für die Clientknoten bj und katie zurücksetzen.

```
reset passexp node=bj,katie
```

## Beispiel: Die Kennwortablaufdauer für alle Benutzer zurücksetzen

Die Kennwortablaufdauer für alle Benutzer auf die allgemeine Kennwortablaufdauer zurücksetzen.

```
reset passexp
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RESET PASSEXP

| Befehl       | Beschreibung   |
|--------------|--|
| QUERY STATUS | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| SET PASSEXP  | Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.                                   |
| UPDATE ADMIN | Ändert das Kennwort eines Administrators bzw. die zu einem Administrator gehörigen Kontaktinformationen.             |
| UPDATE NODE  | Ändert die Attribute, die einem Clientknoten zugeordnet sind.  |

## RESTART EXPORT (Ausgesetzte Exportoperation erneut starten)

Mit diesem Befehl kann eine ausgesetzte Exportoperation erneut gestartet werden.



Eine Exportoperation wird ausgesetzt, wenn eine der folgenden Bedingungen festgestellt wird:

- Ein Befehl SUSPEND EXPORT wird für die aktive Exportoperation ausgegeben
- Segmentvorableerung - die Datei, die für den Export gelesen wird, wird von einem anderen Prozess gelöscht
- Übertragungsfehler bei einem Export zwischen Servern
- Keine verfügbaren Mountpunkte
- Erforderliche Datenträger sind nicht verfügbar
- E/A-Fehler wurden festgestellt

Wichtig: Knoten oder Dateibereiche (auf dem exportierenden Server) in der ursprünglichen Exportoperation, die später umbenannt werden, werden bei der wieder aufgenommenen Operation nicht berücksichtigt. Alle verbleibenden Daten für Knoten oder Dateibereiche auf dem Zielsystem, die vor der Wiederaufnahme gelöscht werden, werden verworfen.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung erforderlich.

## Syntax

```
>>-RESTART EXPORT .-*-----  
                    +-----+-----<<  
                    '---Export-ID---'
```

## Parameter

Export-ID

Dieser optionale Parameter ist die eindeutige ID für die ausgesetzte Exportoperation zwischen Servern. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben. Der Name der Export-ID kann mit dem Befehl QUERY EXPORT ermittelt werden, der alle momentan ausgesetzten Exportoperationen zwischen Servern auflistet.

## Beispiel: Einen ausgesetzten Export erneut starten

Die ausgesetzte Exportoperation erneut starten, die durch die Export-ID EXPORTALLACCTNODES angegeben ist.

```
restart export exportallacctnodes
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RESTART EXPORT

| Befehl         | Beschreibung  |
|----------------|---|
| CANCEL EXPORT  | Löscht eine ausgesetzte Exportoperation.  |
| EXPORT NODE    | Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.                       |
| EXPORT SERVER  | Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server. |
| QUERY EXPORT   | Zeigt die Exportoperationen an, die gerade aktiv oder ausgesetzt sind.  |
| SUSPEND EXPORT | Setzt eine aktive Exportoperation aus.  |

## RESTORE-Befehle

Mit den RESTORE-Befehlen können IBM Spectrum Protect-Speicherpools oder -Datenträger zurückgeschrieben werden.

- RESTORE NODE (NAS-Knoten zurückschreiben)
- RESTORE STGPOOL (Speicherpooldaten aus einem Kopienpool oder einem Pool für aktive Daten zurückschreiben)
- RESTORE VOLUME (Daten primärer Datenträger aus Kopienpool oder Pool für aktive Daten zurückschreiben)

## RESTORE NODE (NAS-Knoten zurückschreiben)



wird die Datei aus dem letzten Sicherungsbild vor der angegebenen Zeit zurückgeschrieben. Werden die Parameter PITDATE und PITTIME nicht angegeben, wird die Datei aus dem letzten Sicherungsbild des Dateisystems zurückgeschrieben.

Ist das Bild eine Differenzsicherung, werden Objekte zuerst aus der entsprechenden Gesamtsicherung und dann aus der Differenzsicherung zurückgeschrieben. Die Zurückschreibung wird ausgeführt, indem die entsprechenden Bilder nach den angegebenen Objekten durchsucht werden und alle gefundenen Objekte zurückgeschrieben werden. Auf die Inhaltsverzeichnisse für diese Bilder wird nicht zugegriffen, so dass der Server nicht überprüft, ob die Objekte tatsächlich in den Bildern enthalten sind.

Der Ordnerpfad und Dateiname müssen unter Verwendung von Schrägstrichsymbolen (/) eingegeben werden. Es ist kein abschließender Schrägstrich (/) am Ende des Dateinamens erforderlich. Alle Argumente, die ein Leerzeichen enthalten, müssen über Anführungszeichen verfügen ("Argument mit Leerzeichen"), die das gesamte Argument einschließen.

```
FILELIST="/path/to/filename1 with blanks",/path/to/filename2_no_blanks
```

Alle Dateinamen, die Kommas enthalten, müssen Anführungszeichen haben, die das gesamte Argument einschließen, und müssen in Hochkommas eingeschlossen sein ("Argument mit Kommas").

```
FILELIST="'/Pfad/zu/Dateiname1,mit,Kommas'",/Pfad/zu/Dateiname2_ohne_Kommas
```

Um ein vollständiges Verzeichnis zurückzuschreiben, geben Sie anstelle eines Dateinamens einen Verzeichnisnamen an. Alle Dateien in dem Verzeichnis und in seinen Unterverzeichnissen werden zurückgeschrieben. Es ist kein abschließender Schrägstrich (/) am Ende des Verzeichnisnamens erforderlich:

```
FILELIST=/path/to/mydir
```

#### Dateiname

Gibt einen oder mehrere Datei- oder Verzeichnisnamen an, die zurückgeschrieben werden sollen. Die angegebenen Namen dürfen keine Platzhalterzeichen enthalten. Mehrere Namen müssen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Bei Dateinamen muss die Groß-/Kleinschreibung berücksichtigt werden.

#### FILE:Dateiliste

Gibt den Namen einer Datei an, die eine Liste der Datei- oder Verzeichnisnamen enthält, die zurückgeschrieben werden sollen. In der angegebenen Datei muss jeder Datei- oder Verzeichnisname in einer separaten Zeile stehen. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert. Beispiel:

Um die Dateien FILE01, FILE02 und FILE03 zurückzuschreiben, erstellen Sie eine Datei mit dem Namen RESTORELIST, die eine Zeile für jede Datei enthält:

```
FILE01  
FILE02  
FILE03
```

Sie können die Dateien, die zurückgeschrieben werden sollen, mit dem folgenden Befehl angeben:

```
FILELIST=FILE:RESTORELIST
```

#### NAMETYPE

Gibt an, wie der Server die Namen, die als FILELIST=Dateiname angegeben werden, oder die Namen, die in der mit FILELIST=Dateiliste angegebenen Datei aufgelistet sind, interpretieren soll. Dieser Parameter ist nützlich, wenn die Namen Unicode-Zeichen enthalten. Er hat keine Auswirkungen, wenn der Parameter FILELIST nicht angegeben wird. Der Standardwert lautet SERVER. Gültige Werte:

#### SERVER

Der Server verwendet die Codepage des Servers, um die Namen zu interpretieren.

#### HEXadecimal

Der Server interpretiert die eingegebenen Namen als hexadezimale Darstellung eines Namens in Unicode. Soll die hexadezimale Darstellung eines Datei- oder Verzeichnisnamens angezeigt werden, können Sie den Befehl QUERY TOC mit FORMAT=DETAILED verwenden.

#### UNICODE

Der Server interpretiert die Namen als UTF-8-verschlüsselt. Diese Option ist nur gültig, wenn Sie eine Liste mit FILELIST=FILE:Dateiliste angegeben haben.

Einschränkung: Network Data Management Protocol (NDMP) verfügt über Einschränkungen, die verhindern, dass IBM Spectrum Protect das erfolgreiche Zurückschreiben einzelner Dateien und Verzeichnisse melden kann.

#### PITDate

Gibt das Datum des Zeitpunkts an. Bei Verwendung mit dem Parameter PITTIME gibt PITDATE den Zeitpunkt an, ab dem Daten zum Zurückschreiben ausgewählt werden sollen. Die letzten Daten, die an oder vor dem angegebenen Datum und der angegebenen Uhrzeit gesichert wurden, werden zurückgeschrieben. Dieser Parameter ist wahlfrei. Der Standardwert ist TODAY. Sie können das Datum mit einem der folgenden Werte angeben:

| Wert | Beschreibung | Beispiel |
|------|--------------|----------|
|------|--------------|----------|

| Wert                           | Beschreibung   | Beispiel  |
|--------------------------------|--|---|
| MM/TT/JJJJ                     | Ein bestimmtes Datum                                     | 06/25/2001  |
| TODAY                          | Das aktuelle Datum                                       | TODAY   |
| TODAY-Tage<br>oder<br>-Tage    | Das aktuelle Datum minus der Anzahl der angegebenen Tage | TODAY-7 oder -7.<br><br>Um Daten zurückzuschreiben, die vor einer Woche gesichert wurden, geben Sie PITDATE=TODAY-7 oder PITDATE=-7 an. |
| EOLM (Ende des letzten Monats) | Der letzte Tag des Vormonats.                            | EOLM  |
| EOLM-Tage                      | Der letzte Tag des Vormonats minus angegebene Tage.      | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.                                      |
| BOTM (Anfang dieses Monats)    | Der erste Tag des aktuellen Monats.                      | BOTM  |
| BOTM+Tage                      | Der erste Tag des aktuellen Monats plus angegebene Tage. | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.   |

#### PITTime

Gibt die Uhrzeit des Zeitpunkts an. Bei Verwendung mit dem Parameter PITDATE gibt PITTIME den Zeitpunkt an, ab dem Daten zum Zurückschreiben ausgewählt werden sollen. Die letzten Daten, die an oder vor dem angegebenen Datum und der angegebenen Uhrzeit gesichert wurden, werden zurückgeschrieben. Dieser Parameter ist wahlfrei. Standardwert ist die aktuelle Uhrzeit.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert                        | Beschreibung   | Beispiel   |
|-----------------------------|--|--|
| HH:MM:SS                    | Eine bestimmte Uhrzeit am angegebenen Datum                                    | 12:33:28   |
| NOW                         | Die aktuelle Uhrzeit am angegebenen Datum                                      | NOW  |
| NOW-HH:MM<br>oder<br>-HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Anfangsdatum | NOW-03:30 oder -03:30.<br><br>Wird dieser Befehl um 9:00 Uhr mit der Angabe PITTIME=NOW-03:30 oder PITTIME=-03:30 ausgegeben, schreibt der Server Sicherungssätze mit der Uhrzeit 5:30 Uhr oder später am Datum des Zeitpunkts zurück. |

#### Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Der Standardwert ist NO. Gültige Werte:

##### No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Mit dem Befehl QUERY PROCESS kann die Hintergrundverarbeitung dieses Befehls überwacht werden.

##### Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Der Befehl muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist.

Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

#### TYPE

Gibt den Typ des Images an, das zurückgeschrieben werden soll. Der Standardwert für diesen Parameter ist BACKUPIIMAGE, und er wird verwendet, um Daten aus standardmäßigen NDMP-Basis- oder -Differenzsicherungen zurückzuschreiben. Andere Imagetypen stellen Sicherungsmethoden dar, die für einen bestimmten Dateiserver spezifisch sein können. Gültige Werte:

##### BACKUPIImage

Gibt an, dass das Dateisystem aus den entsprechenden standardmäßigen NDMP-Sicherungsimages zurückgeschrieben werden soll. Dies ist die Standardmethode für die Ausführung einer NDMP-Zurückschreibungsoperation. Mit dem Typ BACKUPIIMAGE können Sie Daten aus Basis- und Differenzsicherungen sowie Daten auf Dateiebene zurückschreiben.

##### SNAPMirror

Gibt an, dass das Dateisystem aus einem NetApp SnapMirror-Image abgerufen werden soll. SnapMirror-Images sind Gesamtsicherungsimages auf Blockebene eines NetApp-Dateisystems. Ein SnapMirror-Image kann nur in ein Dateisystem zurückschrieben werden, das als SnapMirror-Zieldatenträger vorbereitet wurde. Ausführliche Informationen enthält die Dokumentation zu Ihrem NetApp-Dateiserver.

Nachdem ein SnapMirror-Image abgerufen und in ein Zieldateisystem kopiert wurde, unterbricht IBM Spectrum Protect die SnapMirror-Beziehung, die von dem Dateiserver während der Operation erstellt wurde. Nach Abschluss der Zurückschreibung kehrt das Zieldateisystem in denselben Status wie das ursprüngliche Dateisystem zum Zeitpunkt der Sicherung zurück.

Beachten Sie die folgenden Einschränkungen, wenn der Parameter TYPE auf SNAPMIRROR gesetzt wird:

Einschränkungen:

- Sie können nicht den Parameter FILELIST angeben.
- Weder der *Quelldateisystemname* noch der *Zieldateisystemname* kann der Name eines virtuellen Dateibereichs sein.
- Dieser Parameter ist nur für NetApp- und IBM® N-Series-Dateiserver gültig.

## Beispiel: Ein vollständiges Verzeichnis zurückschreiben

Alle Dateien und Unterverzeichnisse in dem Verzeichnis /mydir zurückschreiben.

```
restore node nasnode /myfs /dest filelist=/path/to/mydir
```

## Beispiel: Daten aus einem Dateisystem zurückschreiben

Die Daten aus dem Dateisystem /vol/vol10 auf NAS-Knoten NAS1 zurückschreiben.

```
restore node nas1 /vol/vol10
```

## Beispiel: Eine Sicherung auf Verzeichnisebene an dieselbe Position zurückschreiben

Die Sicherung auf Verzeichnisebene an die ursprüngliche Position zurückschreiben. Die Quelle ist der virtuelle Dateibereich /MIKESDIR, und es ist kein Zielort angegeben.

```
restore node nas1 /mikesdir
```

Für dieses und das nächste Beispiel wird angenommen, dass die folgenden Definitionen für virtuelle Dateibereiche auf dem Server für den Knoten NAS1 vorhanden sind.

| VFS-Name       | Dateisystem | Pfad   |
|----------------|-------------|--------|
| /mikesdir      | /vol/vol2   | /mikes |
| /TargetDirVol2 | /vol/vol2   | /tmp   |
| /TargetDirVol1 | /vol/vol1   | /tmp   |

## Beispiel: Eine Sicherung auf Verzeichnisebene in ein anderes Dateisystem zurückschreiben

Die Sicherung auf Verzeichnisebene in ein anderes Dateisystem zurückschreiben, aber den Pfad beibehalten.

```
restore node nas1 /mikesdir /vol/vol0
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RESTORE NODE

| Befehl                  | Beschreibung   |
|-------------------------|--|
| BACKUP NODE             | Sichert einen NAS-Knoten (NAS = Network Attached Storage).                   |
| CANCEL PROCESS          | Bricht einen Serverhintergrundprozess ab.                                    |
| DEFINE VIRTUALFSMAPPING | Zuordnung eines virtuellen Dateibereichs definieren.                         |
| QUERY NASBACKUP         | Zeigt Informationen zu NAS-Sicherungsimages an.                              |
| QUERY TOC               | Zeigt Details zum Inhaltsverzeichnis für ein angegebenes Sicherungsimage an. |

# RESTORE STGPOOL (Speicherpooldaten aus einem Kopienpool oder einem Pool für aktive Daten zurückschreiben)

Mit diesem Befehl können Dateien aus einem oder mehreren Kopienspeicherpools oder Pools für aktive Daten in einen primären Speicherpool zurückgeschrieben werden.

Von IBM Spectrum Protect werden alle Dateien im primären Speicherpool zurückgeschrieben, die

- als fehlerhaft identifiziert wurden.
- sich auf einem Datenträger mit dem Zugriffsmodus DESTROYED befinden.

Einschränkung: Sie können diesen Befehl nicht für Containerspeicherpools verwenden. Verwenden Sie den Befehl REPLICATE STGPOOL, um Daten für Containerspeicherpools zu schützen.

Mit diesem Befehl können auch Datenträger identifiziert werden, die zerstörte Primärdateien enthalten. Während der Zurückschreibungsverarbeitung wird für jeden Datenträger (im zurückgeschriebenen Speicherpool), der zerstörte, nicht zwischengespeicherte Dateien enthält, eine Nachricht ausgegeben. Mit dem Befehl QUERY CONTENT können zerstörte Primärdateien auf einem bestimmten Datenträger abgefragt werden.

Sie können keinen Speicherpool zurückschreiben, der mit der Einheitenklasse CENTERA definiert ist.

Neben dem Zurückschreiben von Daten in primäre Speicherpools mit dem Datenformat NATIVE oder NONBLOCK können Sie mit diesem Befehl auch Daten in primäre Speicherpools zurückschreiben, die NDMP-Datenformate haben (NETAPPDUMP, CELERRADUMP oder NDMPDUMP). Der primäre Speicherpool muss dasselbe Datenformat wie der Kopienspeicherpool haben, aus dem Daten zurückgeschrieben werden sollen. IBM Spectrum Protect unterstützt die Back-End-Datenversetzung für NDMP-Images.

**Tipp:** Um NAS-Clientknotendaten in NAS-Speicherpools zurückzuschreiben, müssen Sie manuell den Zugriffsmodus der Datenträger mit dem Befehl UPDATE VOLUME in DESTROYED ändern. Verwenden Sie jedoch Disaster Recovery Manager, enthält die Plandatei die Informationen, die der Server benötigt, um die Datenträger automatisch als DESTROYED zu markieren.

Die Zurückschreibung von Dateien kann unvollständig sein, wenn Sicherungsdateiekopien in Kopienspeicherpools oder Pools für aktive Daten von anderen IBM Spectrum Protect-Prozessen während der Zurückschreibungsverarbeitung versetzt oder gelöscht wurden. Um diesen Fehler zu verhindern, geben Sie nicht die folgenden Befehle für Datenträger in Kopienspeicherpools oder Pools für aktive Daten aus, während die Zurückschreibungsverarbeitung läuft:

- MOVE DATA
- DELETE VOLUME (DISCARDATA=YES)
- AUDIT VOLUME (FIX=YES)

Die Wiederherstellungsverarbeitung für Kopienspeicherpools kann verhindert werden, indem der Prozentsatz für RECLAIM im Befehl UPDATE STGPOOL auf 100 gesetzt wird.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den primären Speicherpool, für den Dateien zurückgeschrieben werden sollen, erforderlich. Wenn ein Administrator mit eingeschränkter Speicherberechtigung Dateien in einem neuen primären Speicherpool zurückschreiben möchte, muss er auch über die Berechtigung für diesen neuen Speicherpool verfügen.

## Syntax

```
>>RESTORE STGpool--Name_des_primären_Pools----->
>-----+-----+-----+-----+-----+-----+----->
  '-COPYstgpool----Kopienpoolname-'
  .-ACTIVEDATAOnly---No-----
>-----+-----+-----+-----+-----+-----+----->
  '-ACTIVEDATAOnly---+No-----+-'
                                '-Yes--| A |-'
>-----+-----+-----+-----+-----+-----+----->
  '-NEWstgpool----Name_des_neuen_primären_Pools-'
  .-MAXProcess-----1-----  .-Preview-----No-----
>-----+-----+-----+-----+-----+-----+----->
  '-MAXProcess----Anzahl-'  '-Preview-----+No--+-'
                                '-Yes-'
```

```

.-Wait---No-----
>-----<
'-Wait---+No---+'
      '-Yes-'

```

A (Yes)

```
|--ACTIVEDATAPool-----Name_des_Pools_für_aktive_Daten-----|
```

## Parameter

### Name\_des\_primären\_Pools (Erforderlich)

Gibt den Namen des primären Speicherpools an, der zurückgeschrieben wird.

### COPYstgpool

Gibt den Namen des Kopierspeicherpools an, aus dem die Dateien zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, werden Dateien aus jedem Kopierspeicherpool, in dem Kopien gefunden werden, zurückgeschrieben. Verwenden Sie diesen Parameter nicht mit den Parametern ACTIVEONLY oder ACTIVEPOOL.

### ACTIVEONLY

Gibt an, dass aktive Versionen von Sicherungsdateien nur aus Pools für aktive Daten zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird dieser Parameter nicht angegeben, werden Dateien aus Kopierspeicherpools zurückgeschrieben. Verwenden Sie diesen Parameter nicht mit dem Parameter COPYSTGPOOL. Gültige Werte:

No

Gibt an, dass der Speicherpool nicht aus Pools für aktive Daten zurückgeschrieben wird.

Yes

Gibt an, dass der Speicherpool aus Pools für aktive Daten zurückgeschrieben wird, die mit dem Parameter ACTIVEPOOL angegeben werden. Wird YES als Wert für ACTIVEONLY angegeben, aber wird kein Wert für ACTIVEPOOL angegeben, werden Dateien aus jedem Pool für aktive Daten zurückgeschrieben, in dem aktive Versionen von Sicherungsdateien lokalisiert werden können.

Achtung: Das Zurückschreiben eines primären Speicherpools aus einem Pool für aktive Daten kann zur Folge haben, dass einige oder alle inaktiven Dateien aus der Datenbank gelöscht werden, wenn der Server bestimmt, dass eine inaktive Datei ersetzt werden muss, aber der Server die Datei im Pool für aktive Daten nicht finden kann.

### ACTIVEDATAPool

Gibt den Namen des Pools für aktive Daten an, aus dem die aktiven Versionen von Sicherungsdateien zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, werden Dateien aus jedem Pool für aktive Daten zurückgeschrieben, in dem aktive Versionen von Sicherungsdateien lokalisiert werden können.

### NEWstgpool

Gibt den Namen des neuen Speicherpools an, in den die Dateien zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, werden Dateien in den ursprünglichen primären Speicherpool (den Pool, der wiederhergestellt wird) zurückgeschrieben.

### MAXProcess

Gibt die maximale Anzahl paralleler Prozesse an, die für das Zurückschreiben von Dateien verwendet werden. Die Verwendung mehrerer paralleler Prozesse kann den Durchsatz der Zurückschreibung verbessern. Dieser Parameter ist wahlfrei. Es kann ein Wert von 1 bis 999 angegeben werden. Der Standardwert ist 1.

Bei der Bestimmung dieses Werts ist die Anzahl Mountpunkte (logische Laufwerke) und physischer Laufwerke zu berücksichtigen, die dieser Operation zugeordnet werden können. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl verfügbarer Mountpunkte und Laufwerke ist von anderen IBM Spectrum Protect-Aktivitäten und Systemaktivitäten sowie von den Mountlimits der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die von der Zurückschreibung betroffen sind.

Jeder Prozess benötigt einen Mountpunkt für Datenträger aus dem Kopierspeicherpool und, falls der Einheitentyp nicht FILE lautet, außerdem ein Laufwerk. Werden Dateien in einen Speicherpool mit sequenziellem Zugriff zurückgeschrieben, benötigt jeder Prozess einen zusätzlichen Mountpunkt für Datenträger für primäre Speicherpools und, falls die Einheitenklasse nicht FILE lautet, ein zusätzliches Laufwerk. Beispiel: Angenommen, es werden maximal 3 Prozesse für die Zurückschreibung eines primären sequenziellen Speicherpools aus einem Kopierspeicherpool mit derselben Einheitenklasse angegeben. Jeder Prozess benötigt zwei Mountpunkte und zwei Laufwerke. Um alle drei Prozesse ausführen zu können, muss das Mountlimit für die Einheitenklasse mindestens 6 betragen und es müssen mindestens 6 Mountpunkte und 6 Laufwerke verfügbar sein.

Für die Voranzeige einer Zurückschreibung wird nur ein einziger Prozess verwendet und es werden keine Mountpunkte oder Laufwerke benötigt.

Preview

Gibt an, ob eine Voranzeige der Zurückschreibung, nicht aber ihre Ausführung gewünscht wird. Anhand der Voranzeige können die Datenträger identifiziert werden, die zum Zurückschreiben des Speicherpools erforderlich sind. Die Voranzeige zeigt Folgendes an:

- Eine Liste der Datenträger des primären Speicherpools, die beschädigte Dateien enthalten.
- Die Anzahl Dateien und die Anzahl Byte, die zurückgeschrieben werden sollen, wobei davon ausgegangen wird, daß der Zugriffsmodus der erforderlichen Datenträger aus dem Kopierspeicherpool READWRITE oder READONLY lautet, wenn die Operation zum Zurückschreiben ausgeführt wird.
- Eine Liste der Datenträger aus dem Kopierspeicherpool, die Dateien enthalten, die zurückgeschrieben werden sollen. Diese Datenträger müssen geladen werden, wenn die Zurückschreibung ausgeführt wird.
- Eine Liste aller Datenträger mit Dateien, die nicht zurückgeschrieben werden können.

Anmerkung: Soll nur eine Liste mit ausgelagerten Kopierspeicherpooldatenträgern angezeigt werden, die während einer Zurückschreibung geladen werden sollen, den Zugriffsmodus der Kopierspeicherpooldatenträger in UNAVAILABLE ändern. Damit wird die Wiederherstellungs- und Datenversetzungsverarbeitung der Datenträger verhindert, bis sie für die Zurückschreibung vor Ort versetzt werden.

Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, daß die Zurückschreibung ausgeführt wird.

Yes

Gibt an, daß eine Voranzeige der Zurückschreibung, aber nicht die Ausführung der Zurückschreibung gewünscht wird.

Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet.

Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

Bei dem Hintergrundprozess erstellte Nachrichten werden im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden. Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird dieser Prozess abgebrochen, wurden möglicherweise einige Dateien bereits vor dem Abbruch zurückgeschrieben.

Yes

Gibt an, dass der Server diese Operation im Vordergrund ausführt. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Der Server zeigt dann die Ausgabenachrichten dem Verwaltungsclient an, wenn die Operation beendet ist.

Anmerkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

## Beispiel: Dateien aus einem Kopierspeicherpool in den primären Speicherpool zurückschreiben

Dateien aus allen Kopierspeicherpools sollen in den primären Speicherpool PRIMARY\_POOL zurückgeschrieben werden.

```
restore stgpool primary_pool
```

## Beispiel: Dateien aus einem bestimmten Pool für aktive Daten in den primären Speicherpool zurückschreiben

Dateien aus dem Pool für aktive Daten ADP1 in den primären Speicherpool PRIMARY\_POOL zurückschreiben.

```
restore stgpool primary_pool activedataonly=yes activedatapool=adp1
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RESTORE STGPOOL

| Befehl            | Beschreibung   |
|-------------------|--|
| BACKUP STGPOOL    | Sichert einen primären Speicherpool in einem Kopierspeicherpool. |
| CANCEL PROCESS    | Bricht einen Serverhintergrundprozess ab.                        |
| COPY ACTIVATEDATA | Kopiert aktive Sicherungsdaten.                                  |



| Befehl         | Beschreibung  |
|----------------|---|
| QUERY CONTENT  | Zeigt Informationen über Dateien in einem Speicherpooldatenträger an.   |
| QUERY PROCESS  | Zeigt Informationen über Hintergrundprozesse an.  |
| RESTORE VOLUME | Schreibt Dateien, die auf angegebenen Datenträgern in einem primären Speicherpool gespeichert sind, aus Kopienspeicherpools zurück. |
| UPDATE STGPOOL | Ändert die Attribute eines Speicherpools.   |
| UPDATE VOLUME  | Aktualisiert die Attribute der Speicherpooldatenträger.   |

## RESTORE VOLUME (Daten primärer Datenträger aus Kopienpool oder Pool für aktive Daten zurückschreiben)

Mit diesem Befehl können alle Dateien auf beschädigten Datenträgern in einen primären Speicherpool zurückgeschrieben werden, der in einem Kopienspeicherpool gesichert oder in einen Pool für aktive Daten kopiert wurde. IBM Spectrum Protect schreibt keine Cache-Kopien von Dateien zurück, und entfernt diese Cache-Dateien während der Zurückschreibungsverarbeitung aus der Datenbank.

Neben dem Zurückschreiben von Daten auf Datenträger in Speicherpools mit dem Datenformat NATIVE oder NONBLOCK können Sie mit diesem Befehl auch Daten auf Datenträger in Speicherpools zurückschreiben, die NDMP-Datenformate haben (NETAPPDUMP, CELERRADUMP oder NDMPDUMP). Die Datenträger, die zurückgeschrieben werden sollen, müssen dasselbe Datenformat wie die Datenträger in dem Kopienspeicherpool haben. IBM Spectrum Protect unterstützt die Back-End-Datenversetzung für NDMP-Images.

Dieser Befehl ändert den Zugriffsmodus der angegebenen Datenträger in DESTROYED. Nachdem alle Dateien auf einem Datenträger in andere Standorte zurückgeschrieben wurden, wird der leere zerstörte Datenträger aus der Datenbank gelöscht.

Das Zurückschreiben kann aus folgenden Gründen unvollständig sein:

- Dateien wurden entweder nie gesichert oder die Sicherungskopien wurden als beschädigt markiert. Mit dem Befehl QUERY CONTENT können weitere Informationen zu den auf dem Datenträger verbleibenden Dateien abgerufen werden.
- Im Befehl RESTORE wurde zwar ein Kopienspeicherpool angegeben, aber die Dateien wurden in einem anderen Kopienspeicherpool gesichert. Wird der Befehl RESTORE nochmals ausgegeben, sollte der Parameter PREVIEW angegeben werden, um zu sehen, ob dies der Fall ist.
- Datenträger im Kopienspeicherpool, die für das Zurückschreiben benötigt werden, sind ausgelagert oder nicht verfügbar. Das Aktivitätenprotokoll auf Nachrichten prüfen, die während der Zurückschreibungsverarbeitung aufgetreten sind.
- Sicherungsdateikopien in Kopienspeicherpools wurden von anderen Prozessen während der Zurückschreibung versetzt oder gelöscht. Siehe 3.
- Ein Pool für aktive Daten wurde für die Zurückschreibung angegeben, und es waren keine inaktiven Dateien zum Kopieren verfügbar.

Wichtig:

1. Sie können keine Datenträger in Speicherpools zurückschreiben, die mit der Einheitenklasse CENTERA definiert sind.
2. Vor dem Zurückschreiben eines Datenträgers mit wahlfreiem Zugriff den Befehl VARY ausgeben, um den Datenträger abzuhängen.
3. Um zu verhindern, dass Kopienspeicherpooldateien von anderen Prozessen versetzt oder gelöscht werden, dürfen die folgenden Befehle während einer Zurückschreibung nicht für Kopienspeicherpooldatenträger ausgegeben werden:
  - MOVE DATA
  - DELETE VOLUME (DISCARDATA=YES)
  - AUDIT VOLUME (FIX=YES)

Um die Wiederherstellungsverarbeitung von Kopienspeicherpools zu verhindern, den Befehl UPDATE STGPOOL ausgeben und den Parameter RECLAIM in diesem Befehl auf 100 setzen.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den primären Speicherpool erforderlich. Wenn ein Administrator mit eingeschränkter Berechtigung Dateien in einen neuen primären Speicherpool zurückschreiben möchte, muss er auch über die Berechtigung für den neuen Speicherpool verfügen.

## Syntax

```
RESTORE VOLUME [OPTION] [VOLUME]
```

```

>>-RESTORE Volume----Datenträgername+----->
>--+-----+----->
' -COPYstgpool----Kopienpoolname-'
. -ACTIVEDATAOnly----No-----
>--+-----+----->
' -ACTIVEDATAOnly----+No-----+ '
          '-Yes--| A |- '
>--+-----+----->
' -NEWstgpool----Name_des_neuen_primären_Pools-'
. -MAXPRocess----1----- . -Preview----No-----
>--+-----+-----+----->
' -MAXPRocess----Anzahl-' ' -Preview----+No--+ '
          '-Yes-'
. -Wait----No-----
>--+-----+-----><
' -Wait----+No--+ '
          '-Yes-'

A (Yes)

|--ACTIVEDATAPool----Name_des_Pools_für_aktive_Daten-----|

```

## Parameter

### Datenträgername (Erforderlich)

Gibt den Namen des zurückzuschreibenden Datenträgers des primären Speicherpools an. Soll eine Liste mit Datenträgern angegeben werden, die zu demselben primären Speicherpool gehören, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

### COPYstgpool

Gibt den Namen des Kopierspeicherpools an, aus dem die Dateien zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, werden Dateien aus jedem Kopierspeicherpool, in dem Kopien gefunden werden, zurückgeschrieben. Verwenden Sie diesen Parameter nicht mit den Parametern ACTIVATEDATAONLY oder ACTIVEDATAPool.

### ACTIVEDATAOnly

Gibt an, dass aktive Versionen von Sicherungsdateien nur aus Pools für aktive Daten zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird dieser Parameter nicht angegeben, werden Dateien aus Kopierspeicherpools zurückgeschrieben. Verwenden Sie diesen Parameter nicht mit dem Parameter COPYSTGPOOL. Gültige Werte:

#### No

Gibt an, dass der Speicherpool nicht aus Pools für aktive Daten zurückgeschrieben wird.

#### Yes

Gibt an, dass der Speicherpool aus Pools für aktive Daten zurückgeschrieben wird, die mit dem Parameter ACTIVEDATAPool angegeben werden. Wird YES als Wert für ACTIVATEDATAONLY angegeben, aber wird kein Wert für ACTIVEDATAPool angegeben, werden Dateien aus jedem Pool für aktive Daten zurückgeschrieben, in dem aktive Versionen von Sicherungsdateien lokalisiert werden können.

**Achtung:** Das Zurückschreiben eines Datenträgers aus einem Pool für aktive Daten kann zur Folge haben, dass einige oder alle inaktiven Dateien aus der Datenbank gelöscht werden, wenn der Server bestimmt, dass eine inaktive Datei ersetzt werden muss, aber der Server die Datei im Pool für aktive Daten nicht finden kann.

### ACTIVEDATAPool

Gibt den Namen des Pools für aktive Daten an, aus dem die aktiven Versionen von Sicherungsdateien zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, werden Dateien aus jedem Pool für aktive Daten zurückgeschrieben, in dem aktive Versionen von Sicherungsdateien lokalisiert werden können.

### NEWstgpool

Gibt den Namen des neuen Speicherpools an, in den die Dateien zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, werden Dateien in den ursprünglichen primären Speicherpool zurückgeschrieben.

### MAXPRocess

Gibt die maximale Anzahl paralleler Prozesse für das Zurückschreiben von Dateien an. Mit Hilfe von parallelen Prozessen kann der Durchsatz verbessert werden. Dieser Parameter ist wahlfrei. Es kann ein Wert von 1 bis 999 angegeben werden. Der Standardwert ist 1.

Bei der Bestimmung dieses Werts ist die Anzahl Mountpunkte (logische Laufwerke) und physischer Laufwerke zu berücksichtigen, die dieser Operation zugeordnet werden können. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM

Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl verfügbarer Mountpunkte und Laufwerke ist von anderen IBM Spectrum Protect-Aktivitäten und Systemaktivitäten sowie von den Mountlimits der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die von der Zurückschreibung betroffen sind.

Jeder Prozess benötigt einen Mountpunkt für Datenträger aus dem Kopierspeicherpool. Lautet der Einheitentyp nicht FILE, benötigt jeder Prozess außerdem ein Laufwerk. Wird ein sequentieller Speicherpool zurückgeschrieben, benötigt jeder Prozess einen zusätzlichen Mountpunkt für Datenträger des primären Speicherpools und, falls der Einheitentyp nicht FILE lautet, ein zusätzliches Laufwerk. Beispiel: Angenommen, es werden maximal drei Prozesse für die Zurückschreibung eines primären sequentiellen Speicherpools aus einem Kopierspeicherpool mit derselben Einheitenklasse angegeben. Jeder Prozess benötigt zwei Mountpunkte und zwei Laufwerke. Um alle drei Prozesse ausführen zu können, muss das Mountlimit für die Einheitenklasse mindestens 6 betragen und es müssen mindestens 6 Mountpunkte und 6 Laufwerke verfügbar sein.

Für die Voranzeige einer Zurückschreibung wird nur ein einziger Prozess verwendet und es werden keine Mountpunkte oder Laufwerke benötigt.

#### Preview

Gibt an, ob eine Voranzeige der Zurückschreibung, nicht aber ihre Ausführung gewünscht wird. Mit dieser Option können die ausgelagerten Datenträger identifiziert werden, die zum Zurückschreiben eines Speicherpools erforderlich sind. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

#### No

Gibt an, dass die Operation zum Zurückschreiben ausgeführt werden soll.

#### Yes

Gibt an, daß die Operation zum Zurückschreiben vorab angezeigt werden soll, ohne die Daten zurückzuschreiben. Tipp: Wird eine Zurückschreibung vorab angezeigt, um eine Liste der ausgelagerten Kopienpooldatenträger anzuzeigen, die geladen werden müssen, sollte der Zugriffsmodus der identifizierten Datenträger in UNAVAILABLE geändert werden. Dies verhindert so lange die Wiederherstellungs- und Datenversetzungsverarbeitung (MOVE DATA) für diese Datenträger, bis sie zur Verwendung bei der Zurückschreibungsverarbeitung zum Standort vor Ort transportiert werden. Die Voranzeige zeigt folgendes an:

- Die Anzahl Dateien und Byte, die zurückgeschrieben werden sollen, wenn der Zugriffsmodus der Datenträger aus dem Kopierspeicherpool READWRITE oder READONLY lautet, wenn die Zurückschreibung ausgeführt wird.
- Eine Liste der Datenträger aus dem Kopierspeicherpool, die Dateien enthalten, die zurückgeschrieben werden sollen. Diese Datenträger müssen geladen werden, wenn die Zurückschreibung ausgeführt wird.
- Eine Liste der Datenträger mit Dateien, die nicht zurückgeschrieben werden können.

#### Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

#### No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet.

Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Bei dem Hintergrundprozess erstellte Nachrichten werden entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird dieser Prozess abgebrochen, wurden möglicherweise einige Dateien bereits vor dem Abbruch gesichert.

#### Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist.

Hinweis: Sie können nicht WAIT=YES an der Serverkonsole angeben.

## Beispiel: Datendateien auf einem Primärdatenträger zurückschreiben

---

Dateien auf dem Datenträger PVOL2 im primären Speicherpool PRIMARY\_POOL sollen zurückgeschrieben werden.

```
restore volume pvol2
```

## Beispiel: Datendateien auf einem Primärdatenträger aus einem Pool für aktive Daten zurückschreiben

---

Dateien auf dem Datenträger VOL001 im primären Pool PRIMARY\_POOL aus dem Pool für aktive Daten ADP1 zurückschreiben.

```
restore volume vol001 activedataonly=yes activedatapool=adp1
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RESTORE VOLUME

| Befehl            | Beschreibung  |
|-------------------|---|
| BACKUP STGPOOL    | Sichert einen primären Speicherpool in einem Kopierspeicherpool.                |
| COPY ACTIVATEDATA | Kopiert aktive Sicherungsdaten.   |
| CANCEL PROCESS    | Bricht einen Serverhintergrundprozess ab.                                       |
| QUERY PROCESS     | Zeigt Informationen über Hintergrundprozesse an.                                |
| RESTORE STGPOOL   | Schreibt Dateien aus Kopierspeicherpools in einen primären Speicherpool zurück. |

## REVOKE-Befehle

Mit den REVOKE-Befehlen können Sie Berechtigungen oder den Zugriff widerrufen.

- REVOKE AUTHORITY (Administratorberechtigung entziehen)
- REVOKE PROXYNODE (Proxyberechtigung für einen Clientknoten entziehen)

## REVOKE AUTHORITY (Administratorberechtigung entziehen)

Mit diesem Befehl können einem Administrator eine oder mehrere Berechtigungsklassen entzogen werden.

Sie können diesen Befehl auch verwenden, um die Anzahl der Maßnahmendomänen zu reduzieren, für die ein Administrator mit eingeschränkter Maßnahmenberechtigung berechtigt ist, und die Anzahl der Speicherpools zu reduzieren, für die ein Administrator mit eingeschränkter Speicherberechtigung berechtigt ist.

Wird der Befehl REVOKE AUTHORITY ohne die Parameter CLASSES, DOMAINS und STGPOOLS verwendet, werden dem angegebenen Administrator sämtliche Berechtigungen entzogen.

Mindestens ein Administrator muss über Systemberechtigung verfügen; diesem kann deshalb die Berechtigung nicht entzogen werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-REVoKe AUTHority--Administratorname----->
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|               .-,----- . |
|               V           | |
| (1)           | |         | |
|'-Classes-----+System-----+-----+'
|               +-Policy-----+
|               +-Storage-----+
|               +-Operator-----+
|               '-Node--| A |-+'
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|               .-,----- . |
|               V           | |
|'-Domains-----+Domänenname+-----+'
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+<
|               .-,----- . |
|               V           | |
| (1)           | |         | |
|'-STGpools-----+Poolname+-----+'
A
.-AUTHority----Access-----
|-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|'-AUTHority----+Access+-----+' '-Node-----+Knotenname-----+'
```

'-Owner--'

Anmerkungen:

1. Werden alle diese Parameter ausgelassen, werden diesem Administrator sämtliche Berechtigungen entzogen.

## Parameter

---

Administratorname (Erforderlich)

Gibt den Namen des Administrators an, dessen Administratorberechtigung entzogen oder reduziert werden soll.

Classes

Gibt eine oder mehrere Administratorberechtigungsklassen an, die entzogen werden sollen. Es können mehrere Klassen angegeben werden, indem die Klassen durch ein Komma voneinander getrennt werden.

System

Gibt an, dass diesem Administrator die Systemberechtigung entzogen werden soll. Bei Angabe von CLASSES=SYSTEM können keine anderen Klassen angegeben werden und auch die Parameter DOMAINS und STGPools können nicht angegeben werden.

Policy

Gibt an, dass diesem Administrator die Maßnahmenberechtigung entzogen werden soll. Sollen alle Maßnahmenberechtigungen entzogen werden, ist CLASSES=POLICY anzugeben. Der Parameter DOMAINS darf dann nicht angegeben werden.

STorage

Gibt an, dass diesem Administrator die Speicherberechtigung entzogen werden soll. Sollen alle Speicherberechtigungen entzogen werden, ist CLASSES=STORAGE anzugeben. Der Parameter STGPools darf dann nicht angegeben werden.

Operator

Gibt an, dass diesem Administrator die Bedienerberechtigung entzogen werden soll.

Node

Gibt an, dass die Knotenberechtigung für diesen Benutzer entzogen werden soll.

AUTHority

Gibt die Berechtigungsstufe an, die für einen Benutzer mit Knotenberechtigung entzogen werden soll. Dieser Parameter ist wahlfrei.

Hat ein Administrator bereits die System- oder Maßnahmenberechtigung für die Maßnahmendomäne, zu der der Knoten gehört, wird mit diesem Befehl die Berechtigung des Administrators nicht geändert.

Gültige Berechtigungsstufen sind:

Access

Gibt an, dass die Clientzugriffsberechtigung entzogen wird. Dies ist der Standardwert, wenn CLASSES=NODE angegeben wird.

Anmerkung: Ein Clientknoten kann die Option REVOKEREMOTEACCESS definieren, um den Zugriff eines Benutzers mit Knotenberechtigung und Clientzugriffsberechtigung zu verhindern. Hat ein Benutzer mit Knotenberechtigung die Client-Eignerberechtigung oder hat er die System- oder Maßnahmenberechtigung für die Maßnahmendomäne, zu der der Knoten gehört, kann dieser Administrator dennoch auf den Web-Client für Sichern/Archivieren zugreifen.

Owner

Gibt an, dass die Clienteignerberechtigung entzogen wird.

DOmains

Gibt an, dass die Clientzugriffsberechtigung oder Clienteignerberechtigung eines Administrators für alle Clients in der angegebenen Maßnahmendomäne entzogen werden soll. Dieser Parameter kann nicht zusammen mit dem Parameter NODE verwendet werden.

NOde

Gibt an, dass die Clientzugriffsberechtigung oder Clienteignerberechtigung eines Administrators für den Knoten entzogen werden soll. Dieser Parameter kann nicht zusammen mit dem Parameter DOMAIN verwendet werden.

DOmains

Gibt bei Verwendung mit CLASSES=POLICY eine Liste mit Maßnahmendomänen an, die von einem Administrator mit eingeschränkter Maßnahmenberechtigung nicht mehr verwaltet werden dürfen. (Der Administrator hatte die Berechtigung zum Verwalten dieser Domänen, bis der Befehl REVOKE ausgegeben wurde.) Dieser Parameter ist wahlfrei. Die Listeneinträge werden durch Kommas ohne Leerzeichen voneinander getrennt. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Für alle übereinstimmenden Domänen wird die Berechtigung entzogen. Bei Angabe von DOMAINS ist der Parameter CLASSES=POLICY wahlfrei.

STGpools

Gibt eine Liste mit Speicherpools an, die von einem Administrator mit eingeschränkter Speicherberechtigung nicht mehr verwaltet werden dürfen. (Der Administrator hatte die Berechtigung zum Verwalten dieser Speicherpools, bis der Befehl REVOKE ausgegeben wurde.) Dieser Parameter ist wahlfrei. Die Listeneinträge werden durch Kommas ohne Leerzeichen voneinander getrennt. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Für alle übereinstimmenden Speicherpools wird die Berechtigung entzogen. Bei Angabe von STGPOOLS ist der Parameter CLASSES=STORAGE wahlfrei.

## Hinweise

1. Soll die uneingeschränkte Speicherberechtigung für eine Administrator in die eingeschränkte Speicherberechtigung geändert werden, muss mit diesem Befehl zunächst die uneingeschränkte Berechtigung entzogen werden. Danach ist es möglich, dem Administrator mit dem Befehl GRANT AUTHORITY eingeschränkte Speicherberechtigung zu erteilen und die Speicherpools anzugeben, für die der Administrator berechtigt sein soll.

Soll einem Administrator die uneingeschränkte Speicherberechtigung entzogen werden, den Parameter CLASSES=STORAGE angeben. Der Parameter STGPOOLS kann nicht dazu verwendet werden, einem Administrator mit uneingeschränkter Speicherberechtigung die Berechtigung für ausgewählte Speicherpools zu entziehen.

2. Soll die uneingeschränkte Maßnahmenberechtigung für eine Administrator in die eingeschränkte Maßnahmenberechtigung geändert werden, muss mit diesem Befehl zunächst die uneingeschränkte Berechtigung entzogen werden. Danach ist es möglich, dem Administrator mit dem Befehl GRANT AUTHORITY eingeschränkte Maßnahmenberechtigung zu erteilen und die Maßnahmendomänen anzugeben, für die der Administrator berechtigt sein soll.

Soll einem Administrator die uneingeschränkte Maßnahmenberechtigung entzogen werden, den Parameter CLASSES=POLICY angeben. Der Parameter DOMAINS kann nicht verwendet werden, um einem Administrator mit uneingeschränkter Berechtigung die Berechtigung für ausgewählte Domänen zu entziehen.

## Beispiel: Bestimmte Administratorberechtigungen entziehen

Der Administratorin CLAUDIA soll ein Teil ihrer Berechtigungen entzogen werden. CLAUDIA hat eingeschränkte Maßnahmenberechtigung für die Maßnahmendomänen EMPLOYEE\_RECORDS und PROG1. Ihre Maßnahmenberechtigung soll nun auf die Maßnahmendomäne EMPLOYEE\_RECORDS beschränkt werden.

```
revoke authority claudia classes=policy
domains=employee_records
```

## Beispiel: Alle Administratorberechtigungen entziehen

Der Administrator LARRY verfügt derzeit über Bedienerberechtigung und eingeschränkte Maßnahmenberechtigung. Ihm sollen jedoch alle Administratorberechtigungen entzogen werden. Um alle Berechtigungen zu entziehen, muss der Name des Administrators angegeben werden; es darf jedoch weder CLASSES noch DOMAINS noch STGPOOLS angegeben werden. LARRY bleibt dann zwar Administrator, aber er kann nur solche Befehle ausführen, die jeder andere Administrator auch ausführen kann.

```
revoke authority larry
```

## Beispiel: Knotenberechtigung entziehen

Die Benutzerin CONNIE im Help Desk-Personal verfügt gegenwärtig über die Knotenberechtigung mit Client-Eigenerberechtigung für den Client-Knoten WARD3. Ihr soll die Knotenberechtigung mit Client-Eigenerberechtigung entzogen werden.

```
revoke authority connie classes=node
authority=owner node=ward3
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für REVOKE AUTHORITY

| Befehl          | Beschreibung   |
|-----------------|--|
| GRANT AUTHORITY | Ordnet einem Administrator Berechtigungsklassen zu.                                    |
| QUERY ADMIN     | Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an. |

## REVOKE PROXYNODE (Proxyberechtigung für einen Clientknoten entziehen)

Verwenden Sie diesen Befehl, um die Berechtigung für einen Agentenclientknoten zur Ausführung von Sicherungs- und Zurückschreibungsoperationen für einen Zielknoten auf dem IBM Spectrum Protect-Server zu entziehen.

## Berechtigungsklasse

---

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Systemberechtigung
- Uneingeschränkte Maßnahmenberechtigung

## Syntax

---

```
>>-REVOKE PROXynode TArget-----Zielknotenname----->  
>--AGent-----Agentenknotenname-----<<
```

## Parameter

---

TArget (Erforderlich)

Gibt den Zielknoten an, für den einem Agentenknoten die Proxyberechtigung erteilt wurde. Platzhalterzeichen und durch Kommas getrennte Listen mit Knotennamen sind zulässig.

AGent (Erforderlich)

Gibt den Knoten an, der die Berechtigung als Proxy für den Zielknoten hat. Platzhalterzeichen und durch Kommas getrennte Listen mit Knotennamen sind zulässig.

## Beispiel: Die Proxy-Berechtigung eines Knotens widerrufen

---

Um dem Zielknoten NASCLUSTER die Berechtigung als Proxy für alle Knoten zu entziehen, die mit dem Buchstaben M beginnen, geben Sie den folgenden Befehl aus.

```
revoke proxynode target=nascluster agent=m*
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für REVOKE PROXYNODE

| Befehl          | Beschreibung   |
|-----------------|--|
| GRANT PROXYNODE | Erteilt einem Agentenknoten die Proxyberechtigung.               |
| QUERY PROXYNODE | Zeigt die Knoten an, die die Berechtigung als Proxyknoten haben. |

## ROLLBACK (Nicht festgeschriebene Änderungen in einem Makro rückgängig machen)

---

Mit diesem Befehl können innerhalb eines Makros Änderungen rückgängig gemacht werden, die von Befehlen, die vom Server ausgeführt wurden, vorgenommen, jedoch noch nicht in der Datenbank festgeschrieben wurden. Eine festgeschriebene Änderung ist permanent und kann nicht rückgängig gemacht werden. Der Befehl ROLLBACK ist für das Testen von Makros nützlich.

Bei Verwendung dieses Befehls muß sichergestellt werden, daß die Verwaltungs-Client-Sitzung nicht mit der Option ITEMCOMMIT ausgeführt wird.

Wichtig: SETOPT-Befehle innerhalb eines Makros können nicht rückgängig gemacht werden.

## Berechtigungsklasse

---

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

---

```
>>-ROLLBACK-----<<
```

## Parameter

---

Keine.

## Beispiel: Änderungen in einem Makro rückgängig machen

Für das Makro REGN soll der Befehl ROLLBACK ausgeführt werden, um zu bestätigen, dass das Makro keine Änderungen festschreibt. Der Makroinhalt lautet:

```
/* Mit dem Makro werden Maßnahmen-
administratoren registriert und Berechtigungen erteilt */
REGister Admin sara hobby
GRant AUTHority sara CClasses=Policy
REGister Admin ken plane
GRant AUTHority ken CClasses=Policy
ROLLBACK      /* verhindert, daß Änderungen festgeschrieben werden */
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für ROLLBACK

| Befehl | Beschreibung                               |
|--------|--|
| COMMIT | Schreibt Änderungen in der Datenbank fest. |
| MACRO  | Führt eine angegebene Makrodatei aus.      |

### Zugehörige Konzepte:

Makros des Verwaltungsclients

## RUN (IBM Spectrum Protect-Prozedur ausführen)

Mit diesem Befehl kann eine IBM Spectrum Protect-Prozedur ausgeführt werden. Soll dieser Befehl auf einem anderen Server ausgegeben werden, muß die Prozedur, die ausgeführt wird, auf diesem Server definiert sein.

RUN-Befehle können in Prozeduren eingeschlossen werden, solange sie keine Schleifen erstellen. Beispielsweise sollten RUN-Befehle nicht eingeschlossen werden, wenn die Prozedur SCRIPT\_A die Prozedur SCRIPT\_B und die Prozedur SCRIPT\_B die Prozedur SCRIPT\_A ausführt.

Wichtig: IBM Spectrum Protect verfügt über keinen Befehl, mit dem ein Script nach dem Starten abgebrochen werden kann. Um ein Script zu stoppen, muss der Server angehalten werden.

## Berechtigungsklasse

Für diesen Befehl ist die Bediener-, Maßnahmen-, System- oder Speicherberechtigung erforderlich.

## Syntax

```
>>-RUN--Prozedurname--+-+-----+-+-----+-+-----+-+----->
      | .-,------. |
      | V              | |
      '---Substitutionswert---'

.-Preview----No-----.-Verbose----No-----
>+-----+-+-----+-+-----+-+-----<
'-Preview----+No--+-' '-Verbose----+No--+-'
      '-Yes-'          '-Yes-'
```

## Parameter

### Prozedurname (Erforderlich)

Gibt den Namen der Prozedur an, die verarbeitet werden soll. Der angegebene Name darf keine Substitutionsvariable wie beispielsweise \$1 sein.

### Substitutionswert

Gibt einen oder mehrere Substitutionswerte für Variablen an, wenn die Prozedur ausgeführt wird. In einer Prozedur besteht eine Substitutionsvariable aus dem Zeichen '\$' gefolgt von einer Zahl. Bei der Ausführung der Prozedur ersetzt IBM Spectrum Protect die in einer Prozedur definierten Substitutionsvariablen durch die Werte, die mit diesem Befehl angegeben werden. Für jede in der Prozedur definierte Substitutionsvariable müssen Werte angegeben werden. Andernfalls schlägt die Prozedur fehl. Dieser Parameter ist wahlfrei.

### Preview



Gibt an, ob die Befehlszeilen einer Prozedur vorab angezeigt werden sollen, ohne die Prozedur tatsächlich zu verarbeiten. Der Standardwert ist NO.

Gültige Werte:

Yes

Gibt an, daß die in einer Prozedur enthaltenen Befehlszeilen angezeigt werden, die Prozedur jedoch nicht verarbeitet wird.

No

Gibt an, daß die in einer Prozedur enthaltenen Befehlszeilen angezeigt werden und die Prozedur verarbeitet wird.

Verbose

Gibt an, ob die Befehlszeilen, die Variablensubstitution und die Tests der bedingten Logik, die in einer Prozedur verwendet werden, angezeigt werden, wenn die Prozedur verarbeitet wird. Dieser Parameter wird ignoriert, wenn PREVIEW=YES angegeben wird. Der Standardwert ist NO.

Gültige Werte:

Yes

Gibt an, daß die Befehlszeilen, die Variablensubstitution und die Tests der bedingten Logik angezeigt werden, wenn die Prozedur verarbeitet wird.

No

Gibt an, daß die Befehlszeilen, die Variablensubstitution und die Tests der bedingten Logik nicht angezeigt werden, wenn die Prozedur verarbeitet wird.

## Beispiel: Die Befehle anzeigen, die von einem Script mit einer Substitutionsvariablen für den Tabellennamen generiert werden

---

Um das folgende Beispielscript mit dem Namen QSAMPLE auszuführen, geben Sie einen Befehl RUN aus, der den Tabellennamen ACTLOG als Wert für die Substitutionsvariable \$1 angibt. Verwenden Sie die Ausgabe, um die Befehle voranzuzeigen, die von dem Script generiert werden, bevor die Befehle ausgeführt werden.

```
001 /* SQL-Beispielabfrage im breiten Format*/
005 SET SQLDISPLAYMODE WIDE
010 SELECT colname FROM -
015 COLUMNS WHERE TABNAME='$1'

run qsample actlog preview=yes

ANR1461I RUN: Befehlsprozedur QSAMPLE wird ausgeführt.
ANR1466I RUN: Befehlsprozedur QSAMPLE, Zeile 5 :
           set sqldisplaymode wide.
ANR1466I RUN: Befehlsprozedur QSAMPLE, Zeile 15 :
           select colname from columns where tabname='ACTLOG'.
ANR1470I RUN: Befehlsprozedur QSAMPLE erfolgreich ausgeführt
           (Modus PREVIEW)
```

## Beispiel: Ein Script ausführen, um die Befehle anzuzeigen und auszuführen, die von dem Script generiert werden

---

Führen Sie dasselbe Script wie im vorherigen Beispiel aus, um sowohl die generierten Befehle als auch die Ergebnisse der Befehle anzuzeigen.

```
run qsample actlog verbose=yes

ANR1461I RUN: Befehlsprozedur QSAMPLE wird ausgeführt.
ANR1466I RUN: Befehlsprozedur QSAMPLE, Zeile 5 :
           set sqldisplaymode wide.
ANR1466I RUN: Befehlsprozedur QSAMPLE, Zeile 5 : RC=RC_OK
ANR1466I RUN: Befehlsprozedur QSAMPLE, Zeile 15 :
           select colname from columns where tabname='ACTLOG'.

COLNAME
-----
DATE_TIME
MSGNO
SEVERITYMESSAGE
ORIGINATOR
NODENAME
OWNERNAME
SCHEDNAME
DOMAINNAME
SESSID
```

ANR1466I RUN: Befehlsprozedur QSAMPLE, Zeile 15 : RC=RC\_OK  
ANR1462I RUN: Befehlsprozedur QSAMPLE erfolgreich ausgeführt.

## Beispiel: Ein Script ausführen, um nur die Ergebnisse der Befehle in dem Script anzuzeigen

Führen Sie das vorherige Beispielscript aus, um nur die Ergebnisse der generierten Befehle in dem Script anzuzeigen.

```
run qsample actlog verbose=no
```

```
COLNAME  
-----  
DATE_TIME  
MSGNO  
SEVERITYMESSAGE  
ORIGINATOR  
NODENAME  
OWNERNAME  
SCHEDNAME  
DOMAINNAME  
SESSID
```

ANR1462I RUN: Befehlsprozedur QSAMPLE erfolgreich ausgeführt.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RUN

| Befehl        | Beschreibung  |
|---------------|---|
| COPY SCRIPT   | Erstellt eine Kopie einer Prozedur.                           |
| DEFINE SCRIPT | Definiert eine Prozedur für den IBM Spectrum Protect-Server.  |
| DELETE SCRIPT | Löscht eine Prozedur oder einzelne Zeilen aus einer Prozedur. |
| QUERY SCRIPT  | Zeigt Informationen über Prozeduren an.                       |
| RENAME SCRIPT | Vergibt einen neuen Namen für eine Prozedur.                  |
| UPDATE SCRIPT | Ändert Zeilen oder fügt Zeilen in einer Prozedur hinzu.       |

### Zugehörige Tasks:

Server-Script ausführen

## SELECT (SQL-Abfrage für die IBM Spectrum Protect-Datenbank ausführen)

Verwenden Sie den Befehl SELECT, um eine angepasste Abfrage der IBM Spectrum Protect-Datenbank zu erstellen und zu formatieren.

IBM Spectrum Protect stellt eine SQL-Schnittstelle zu einem DB2-Programm zur Verfügung. Einschränkungen und Richtlinien für die Handhabung von SQL-Abfragen werden direkt von DB2 gesteuert.

Als Hilfestellung für das Auffinden der verfügbaren Informationen stellt IBM Spectrum Protect drei Systemkatalogtabellen zur Verfügung:

SYSCAT.TABLES

Enthält Informationen zu allen Tabellen, die mit dem Befehl SELECT abgefragt werden können.

SYSCAT.COLUMNNS

Beschreibt die Spalten in jeder Tabelle.

Diese Tabellen können mit dem Befehl SELECT abgefragt werden, um die Position von gewünschten Informationen zu ermitteln.

## Hinweise

Der Befehl SELECT kann nicht von einer Serverkonsole ausgegeben werden.

Da der Befehl SELECT keine Sätze sperrt und entsperrt, kann ein Konflikt bei einem Satz dazu führen, dass der Server fälschlicherweise die Nachricht ANR2034E ausgibt: *SELECT: Keine Übereinstimmung mit diesen Kriterien gefunden.* Überprüfen Sie Ihre Auswahlkriterien und wiederholen Sie den Befehl, wenn sie korrekt sind.

Um die Verarbeitung eines Befehls SELECT nach dem Start zu stoppen, brechen Sie die Verwaltungssitzung ab, in der der Befehl ausgegeben wurde. Die Sitzung entweder von der Server-Konsole oder einer anderen Verwaltungssitzung abbrechen.

Temporäre Tabellenbereiche werden verwendet, um SQL-Abfragen innerhalb von DB2 zu verarbeiten. Unzureichender temporärer Speicherbereich kann zur Folge haben, dass SQL-Abfragen fehlschlagen.

Um die Ausgabe in eine durch Kommas getrennte Datei für den Import in ein Spreadsheet zu exportieren, verwenden Sie die Befehlszeilenoptionen -comma und > im Befehl dsmdmcc.

## Berechtigungsklasse

---

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

---

Informationen zur Syntax und zu Richtlinien für die Anweisung SELECT finden Sie in der Produktinformation zu DB2.

Wichtig: Die gültige Syntax für die mit Zeitmarke versehene Anweisung SELECT lautet:

```
SELECT * FROM SUMMARY WHERE ACTIVITY='EXPIRATION' AND START_TIME >'2009-05-10 00:00:00' AND START_TIME <'2009-05-11 23:23:23'
```

## Liste der Beispiele

---

Mit dem Befehl SELECT kann eine Vielzahl von Abfragen angepasst werden. Die nachfolgend gezeigten Beispiele lassen die Vielseitigkeit dieses Befehls ahnen. Er bietet jedoch noch wesentlich mehr Möglichkeiten. Lediglich für die komplexeren Befehle werden die Ausgabedaten aus der Abfrage gezeigt, um das Ausgabeformat zu illustrieren.

In der folgenden Liste sind die SELECT-Beispielbefehle zusammengefasst:

- Kennwörter für Administrator-IDs auflisten, die mit einem externen LDAP-Verzeichnisserver authentifiziert werden
- Verfügbare Tabellen auflisten
- Clientknoten und Verwaltungsclients auflisten, die gegenwärtig für den Serverzugriff gesperrt sind
- Clientknoten und Verwaltungsclients auflisten, die in jüngster Zeit nicht das korrekte Kennwort angegeben haben
- Knoten in der Maßnahmendomäne STANDARD auflisten, die nicht dem täglichen Sicherungszeitplan DAILYBACKUP zugeordnet sind
- Die Administratoren auflisten, die über Maßnahmenberechtigung verfügen
- Nachrichten des Typs E (FEHLER) oder W (WARNUNG) auflisten, die in dem Zeitraum ausgegeben wurden, für den Aktivitätenprotokollsätze aufbewahrt wurden
- Die Verwaltungszeitpläne auflisten, die vom Administrator JAKE definiert oder geändert wurden
- Die relativen Prioritäten der Verwaltungszeitpläne auflisten
- Die Verwaltungsklassen auflisten, die eine Archivierungskopiengruppe mit einem Aufbewahrungszeitraum von mehr als 365 Tagen haben
- Die Clientknoten auflisten, die sich in jeder Maßnahmendomäne befinden
- Die Anzahl der Dateien bestimmen, die von jedem Knoten archiviert wurden
- Die Clients auflisten, die die Speicherverwaltung verwenden
- Bestimmen, wie viele Datenträger wiederhergestellt würden, wenn der Wiederherstellungsschwellenwert für Speicherpool TAPE in 50 Prozent geändert wird
- Bestimmen, wie viele Sicherungsdateien für jeden Knoten betroffen wären, wenn die Verwaltungsklasse DAILY in der Maßnahmendomäne STANDARD geändert oder gelöscht würde
- Für alle aktiven Clientsitzungen bestimmen, wie lange sie verbunden waren und wie hoch ihr effektiver Durchsatz in Byte pro Sekunde war
- Bestimmen, wie lange die aktuellen Hintergrundprozesse ausgeführt wurden und wie hoch ihr effektiver Durchsatz in Zeit und Dateien pro Sekunde war
- Die Anzahl der Clientknoten für jeden Plattformtyp bestimmen
- Die Anzahl der Dateibereiche bestimmen, die jeder Clientknoten hat, und die Clientknoten in aufsteigender Reihenfolge auflisten
- Statistische Informationen zur Berechnung der Anzahl ausgelagerter Datenträger abrufen, deren Speicherbereich während der Wiederherstellung eines Speicherpools wiederhergestellt wird
- Detailsätze zur PVU-Schätzung abrufen
- Informationen zu den Knotenrollen abrufen
- Informationen zum Status abrufen

## Beispiel: Administrator-IDs auflisten, die sich mit dem IBM Spectrum Protect-Server authentifizieren

---

Alle Administrator-IDs auflisten, deren Kennwörter mit dem IBM Spectrum Protect-Server authentifiziert werden:

```
select admin_name from admins where authentication=local
```

## Beispiel: Verfügbare Tabellen auflisten

---

Alle Tabellen auflisten, die für das Abfragen der IBM Spectrum Protect-Datenbank verfügbar sind.

```
select * from syscat.tables

      ABSHEMA: SERVER1
      TABNAME: ACTLOG
      CREATE_TIME: 1999-05-01 07:39:06
      COLCOUNT: 10
INDEX_COLCOUNT: 1
      UNIQUE_INDEX: FALSE
      REMARKS: Server-Aktivitätenprotokoll

      TABSCHEMA: SERVER1
      TABNAME: ADMIN_SCHEDULES
      CREATE_TIME: 1995-05-01 07:39:06
      COLCOUNT: 14
INDEX_COLCOUNT: 1
      UNIQUE_INDEX: TRUE
      REMARKS: Verwaltungsbefehlzeitpläne

      TABSCHEMA: SERVER1
      TABNAME: ADMINS
      CREATE_TIME: 1995-05-01 07:39:06
      COLCOUNT: 15
INDEX_COLCOUNT: 1
      UNIQUE_INDEX: TRUE
      REMARKS: Server-Administratoren

      TABSCHEMA: SERVER1
      TABNAME: ARCHIVES
      CREATE_TIME: 1995-05-01 07:39:06
      COLCOUNT: 10
INDEX_COLCOUNT: 5
      UNIQUE_INDEX: FALSE
      REMARKS: Client-Archivierungsdateien
```

## Beispiel: Clientknoten und Verwaltungsclients auflisten, die gegenwärtig für den Serverzugriff gesperrt sind

---

```
select node_name from nodes where locked='YES'

select admin_name from admins where locked='YES'
```

## Beispiel: Clientknoten, Verwaltungsclients und Server auflisten, die die Sitzungssicherheit 'Transitional' (Vorübergehend) verwenden

---

```
select node_name from nodes where session_security='Transitional'

select admin_name from admins where session_security='Transitional'

select server_name from servers where session_security='Transitional'
```

## Beispiel: Clientknoten und Verwaltungsclients auflisten, die in jüngster Zeit nicht das korrekte Kennwort angegeben haben

---

```
select node_name from nodes where invalid_pw_count <>0

select admin_name from admins where invalid_pw_count <>0
```

## Beispiel: Knoten in der Maßnahmendomäne STANDARD auflisten, die nicht dem täglichen Sicherungszeitplan DAILYBACKUP zugeordnet sind

---

```
select node_name from nodes where domain_name='STANDARD' and
node_name not in (select node_name from associations
where domain_name='STANDARD' and
schedule_name='DAILYBACKUP')
```

## Beispiel: Die Administratoren auflisten, die über Maßnahmenberechtigung verfügen

---

```
select admin_name from admins where
upper(system_priv) <>'NO'
or upper(policy_priv) <>'NO'
```

### Beispiel: Nachrichten des Typs E (FEHLER) oder W (WARNUNG) auflisten, die in dem Zeitraum ausgegeben wurden, für den Aktivitätenprotokollsätze aufbewahrt wurden

---

```
select date_time,msgno,message from actlog
where severity='E' or severity='W'
```

### Beispiel: Die Verwaltungszeitpläne auflisten, die vom Administrator JAKE definiert oder geändert wurden

---

```
select schedule_name from admin_schedules
where chg_admin='JAKE'
```

### Beispiel: Die relativen Prioritäten der Verwaltungszeitpläne auflisten

---

```
select schedule_name,priority from admin_schedules order
by priority
```

### Beispiel: Die Verwaltungsklassen auflisten, die eine Archivierungskopiengruppe mit einem Aufbewahrungszeitraum von mehr als 365 Tagen haben

---

```
select domain_name,set_name,class_name from ar_copygroups
where retver='NOLIMIT' or cast(retver as integer) >365
```

### Beispiel: Die Verwaltungsklassen auflisten, die mehr als fünf Sicherungsversionen angeben

---

```
select domain_name,set_name,class_name from bu_copygroups
where verexists = 'NOLIMIT' or
cast(verexists as integer)>5
```

### Beispiel: Die Clientknoten auflisten, die die Clientoptionsgruppe SECURE verwenden

---

```
select node_name from nodes where option_set='SECURE'
```

### Beispiel: Die Clientknoten auflisten, die sich in jeder Maßnahmendomäne befinden

---

```
select domain_name,num_nodes from domains
```

### Beispiel: Die Anzahl der Dateien bestimmen, die von jedem Knoten archiviert wurden

---

Achtung: Die Ausführung dieses Befehls nimmt unter Umständen viel Zeit in Anspruch.

```
select node_name,count(*) from archives
group by node_name
```

### Beispiel: Die Clients auflisten, die die Speicherverwaltung verwenden

---

```
select node_name from auditocc where spacemg_mb <>0
```

### Beispiel: Bestimmen, wie viele Datenträger wiederhergestellt würden, wenn der Wiederherstellungsschwellenwert für Speicherpool TAPE in 50 Prozent geändert wird

---

```
select count(*) from volumes where stgpool_name='TAPE'
and upper(status)='FULL' and pct_utilized < 50
```

### Beispiel: Bestimmen, wie viele Sicherungsdateien für jeden Knoten betroffen wären, wenn die Verwaltungsklasse DAILY in der Maßnahmendomäne STANDARD geändert oder gelöscht würde

---

Anmerkung: Die Ausführung dieses Befehls nimmt viel Zeit und viele Ressourcen in Anspruch.

```
select node_name, count(*) as "Files" from backups
where class_name='DAILY' and node_name in
```

```
(select node_name from nodes where domain_name='STANDARD')
group by node_name
```

## Beispiel: Für alle aktiven Clientsitzungen bestimmen, wie lange sie verbunden waren und wie hoch ihr effektiver Durchsatz in Byte pro Sekunde war

---

```
select session_id as "Session",
client_name as "Client",
state as "State",
current_timestamp-start_time as "Elapsed Time",
(cast(bytes_sent as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Bytes sent/second",
(cast(bytes_received as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Bytes received/second"
from sessions
```

```
          Sitzung: 24
            Client: ALBERT
            Status: Run
        Antwortzeit: 0 01:14:05.000000
    Byte gesendet (Sek): 564321.9302768451
    Byte empfangen (Sek): 0.0026748857944

          Sitzung: 26
            Client: MILTON
            Status: Run
        Antwortzeit: 0 00:06:13.000000
    Byte gesendet (Sek): 1638.5284210992221
    Byte empfangen (Sek): 675821.6888561849
```

## Beispiel: Bestimmen, wie lange die aktuellen Hintergrundprozesse ausgeführt wurden und wie hoch ihr effektiver Durchsatz in Zeit und Dateien pro Sekunde war

---

Anmerkung: Beim Verfall wird die Anzahl der verarbeiteten Byte nicht angegeben.

```
select process_num as "Number",
process,
current_timestamp-start_time as "Elapsed Time",
(cast(files_processed as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Files/second",
(cast(bytes_processed as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Bytes/second"
from processes
```

```
          Nummer: 1
        PROCESS: Expiration
    Antwortzeit: 0 00:24:36.000000
Dateien/Sekunde: 6.3216755870092
Byte/Sekunde: 0.00000000000000
```

## Beispiel: Die Anzahl der Clientknoten für jeden Plattformtyp bestimmen

---

```
select platform_name,count(*) as "Number of Nodes"
from nodes group by platform_name
```

| PLATFORM_NAME | Anzahl Knoten |
|---------------|---------------|
| AIX           | 6             |
| SunOS         | 27            |
| Win32         | 14            |
| Linux         | 20            |

## Beispiel: Die Anzahl der Dateibereiche bestimmen, die jeder Clientknoten hat, und die Clientknoten in aufsteigender Reihenfolge auflisten

---

```
select node_name, count(*) as "number of filespaces"
from filespaces group by node_name order by 2
```

| NODE_NAME | Anzahl Dateibereiche |
|-----------|----------------------|
| ALBERT    | 2                    |
| MILTON    | 2                    |
| BARNEY    | 3                    |
| SEBASTIAN | 3                    |
| MAILHOST  | 4                    |
| FALCON    | 4                    |
| WILBER    | 4                    |
| NEWTON    | 4                    |
| JEREMY    | 4                    |
| WATSON    | 5                    |
| RUSSELL   | 5                    |

## Beispiel: Statistische Informationen zur Berechnung der Anzahl ausgelagerter Datenträger abrufen, deren Speicherbereich während der Wiederherstellung eines Speicherpools wiederhergestellt wird

---

```
select * from summary where activity='OFFSITE RECLAMATION'

START_TIME: 2004-06-16 13:47:31.000000
END_TIME: 2004-06-16 13:47:34.000000
ACTIVITY: OFFSITE RECLAMATION
NUMBER: 4
ENTITY: COPYPOOL
COMMETH:
ADDRESS:
SCHEDULE_NAME:
EXAMINED: 170
AFFECTED: 170
FAILED: 0
BYTES: 17821251
IDLE: 0
MEDIAW: 0
PROCESSES: 2
SUCCESSFUL: YES
VOLUME_NAME:
DRIVE_NAME:
LIBRARY_NAME:
LAST_USE:
COMM_WAIT:
NUM_OFFSITE_VOLS: 2
```

## Beispiel: Die Speicherpools identifizieren, die von Clients deduplizierte Daten enthalten

---

```
select stgpool_name, has_client_dedup_data from stgpools

Speicherpoolname      hat vom Client deduplizierte Daten
-----
ADPOOL                NO
ARCHIVEPOOL           NO
BACKUPPOOL            NO
COPYDEDUP             NO
COPYNODEDUP          NO
FILEPOOL              YES
FILEPOOL2             NO
LANFREEFILEPOOL       YES
SPACEMGPOOL           NO
```

## Beispiel: Informationen zur Datenbank abrufen

---

```
select * from db

DATABASE_NAME: TSMDB1
TOT_FILE_SYSTEM_MB: 2048000
USED_DB_SPACE_MB: 12576
FREE_SPACE_MB: 1576871
TOTAL_PAGES: 983044
USABLE_PAGES: 982908
USED_PAGES: 977736
FREE_PAGES: 5172
BUFF_HIT_RATIO: 96.2
```

```

TOTAL_BUFF_REQ: 53967
SORT_OVERFLOW: 0
LOCK_ESCALATION: 0
PKG_HIT_RATIO: 70.0
  LAST_REORG: 2010-07-15 17:32:55.000000
FULL_DEV_CLASS: OUTFILE
NUM_BACKUP_INCR: 0
LAST_BACKUP_DATE: 2010-01-21 10:37:59.000000
PHYSICAL_VOLUMES: 0
  PAGE_SIZE:
NUM_BACKUP_STREAMS: 4

```

## Beispiel: Detailsätze zur Prozessor-Value-Unit-Schätzung abrufen

---

Die PVU-Schätzung für den Knoten ACCTSRECSRV generieren, der von dem Produkt IBM Spectrum Protect Extended Edition verwendet wird.

```
select * from pvuestimate_details where node_name='ACCTSRECSRV'
```

```

PRODUCT: PRODEE
LICENSE_NAME: MGSYSLAN
NODE_NAME: ACCTSRECSRV
LAST_USED: 2008-01-20 16:12:24.000000
  TRYBUY: FALSE
PROC_VENDOR: IBM
PROC_BRAND: POWER5+ QCM
PROC_TYPE: 4
PROC_MODEL:
PROC_COUNT: 2
  ROLE: SERVER
ROLE_OVERRIDE: USEREPORTED
ROLE_EFFECTIVE: SERVER
VALUE_UNITS: 50
VALUE_FROM_TABLE: YES
  PVU: 100
SCAN_ERROR : NO
API_CLIENT: NO
PVU_AGNOSTIC: NO
HYPERVISOR: VMWARE
  GUID: 01.2e.1c.80.e5.04-
      .11.da.aa.ab.00.-
      15.58.0b.d9.47
VERSION: 6
RELEASE: 3
LEVEL: 1
VENDOR_D: IBM(R)
BRAND_D: POWER5(TM) QCM
TYPE_D: Quad-core Module
MODEL_D: All Existing
PRODUCT_D: IBM Spectrum Protect Extended Edition

```

## Feldbeschreibungen

---

### PRODUCT

Röllup der Lizenztypen nach Produkten auf der im Befehl QUERY PVUESTIMATE angegebenen Ebene. Gültige Werte sind PRODEE, PRODBASIC, PRODDATARET, PRODMAIL, PROddb, PRODSYSB, PRODSpace, PRODSAN, PRODERP oder leer.

### LICENSE\_NAME

Die Lizenz, die diesem Knoten zugeordnet ist.

### NODE\_NAME

Der Knotenname.

### LAST\_USED

Datum und Uhrzeit, an dem bzw. zu der der angegebene Knoten zum letzten Mal unter dieser Lizenz die Verbindung zum System hergestellt hat.

### TRYBUY

Gibt an, ob die Lizenz eine Probelizenz ist. Gültige Werte sind TRUE oder FALSE.

### PROC\_VENDOR

Der Name des vom Client zurückgemeldeten Prozessorherstellers.

### PROC\_BRAND

Der Name der vom Client zurückgemeldeten Prozessormarke.

### PROC\_TYPE

Der vom Client zurückgemeldete Prozessortyp. Dieser Wert spiegelt auch die Anzahl der Kerne wieder. Beispielwerte sind 1=SINGLE CORE, 2=DUO CORE und 4=QUAD CORE.



PROC\_MODEL  
Das vom Client zurückgemeldete Prozessormodell.

PROC\_COUNT  
Die Anzahl der Prozessoren.

ROLE  
Die Knotenrolle. Gültige Werte sind CLIENT, SERVER oder OTHER.

ROLE\_OVERRIDE  
Der im Befehl UPDATE NODE angegebene Überschreibungswert.

ROLE\_EFFECTIVE  
Tatsächliche Rolle auf der Basis der Werte in den Feldern ROLE und ROLE\_OVERRIDE.

VALUE\_UNITS  
Die zugeordnete Prozessor-Value-Unit (PVU) für den Prozessor.

PVU  
Der berechnete PVU-Wert.

$$PVU \text{ pro Knoten} = \text{Anzahl Prozessoren pro Knoten} * \text{Prozessortyp} * \text{PVU-Wert}$$

Dabei stellt der `Prozessortyp` die Anzahl der Kerne dar, und der `PVU-Wert` ist der Wert, der für den Prozessortyp in der IBM® PVU-Tabelle definiert ist.

VALUE\_FROM\_TABLE  
Markierung, die angibt, ob die Prozessor-Value-Unit auf der Basis der IBM PVU-Tabelle berechnet wurde. Gültige Werte sind YES oder NO. Bei NO wird ein Wert von 100 für jeden Knoten angewendet, der als Server definiert ist. Ist keine Rolle für einen Knoten definiert, wird die Rolle 'Server' zum Zweck der PVU-Berechnung angenommen.

SCAN\_ERROR  
Markierung, die angibt, ob Lizenzinformationen vom Client zurückgemeldet wurden. Gültige Werte sind YES oder NO.

API\_CLIENT  
Markierung, die eine API-Anwendung angibt. Gültige Werte sind YES oder NO.

PVU\_AGNOSTIC  
Markierung, die angibt, dass der Release-Level der Clientversion vor IBM Spectrum Protect Version 6.3 liegt. Liegt die Version vor Version 6.3, werden keine gültigen PVU-Messwerte erwartet. Gültige Werte sind YES oder NO.

HYPERVISOR  
Der Name der vom Client zurückgemeldeten VM-Software.

GUID  
Global eindeutige ID (GUID) des Computers, auf dem sich der Knoten befindet. Die GUID wird aus der Knotentabelle abgerufen.

VERSION  
Die Version des Clients.

RELEASE  
Das Release des Clients.

LEVEL  
Die Stufe des Clients.

VENDOR\_D  
Der Anzeigewert für den Prozessorhersteller aus der PVU-Tabelle.

BRAND\_D  
Der Anzeigewert für die Prozessormarke aus der PVU-Tabelle.

TYPE\_D  
Der Anzeigewert für den Prozessortyp aus der PVU-Tabelle.

MODEL\_D  
Der Anzeigewert für das Prozessormodell aus der PVU-Tabelle.

PRODUCT\_D  
Der Anzeigewert für das Produkt aus der PVU-Tabelle. Die folgenden Werte sind gültig:

- IBM Spectrum Protect
- IBM Spectrum Protect Extended Edition
- IBM Spectrum Protect for Data Retention
- IBM Spectrum Protect for SAN
- IBM Spectrum Protect for Space Management
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for System Backup and Recovery
- Leer

## Beispiel: Informationen zur Rolle und PVU-bezogene Informationen anfordern

Das folgende Beispiel zeigt Teilergebnisse für einen ausgewählten Knoten, einschließlich PVU-bezogene Informationen und Rolleninformationen. Gültige Rollen sind CLIENT, SERVER oder OTHER. Die Prozessor-Value-Unit wird nur für Knoten berechnet, die als

Server definiert sind.

```
select * from nodes
```

```
ROLE: CLIENT
  ROLE_O: USERREPORTED
  PVENDOR: INTEL
  PBRAND: INTEL
  PTYPE: 4
  PMODEL:
  PCOUNT: 1
HYPERVISOR:
  PAPI: NO
  SCANERROR: NO
```

## SET-Befehle

---

Mit den SET-Befehlen können Sie Werte angeben, die viele verschiedene IBM Spectrum Protect-Operationen betreffen.

- SET ACCOUNTING (Abrechnungssätze aktivieren/inaktivieren)
- SET ACTLOGRETENTION (Aufbewahrungsdauer für das Aktivitätenprotokoll definieren)
- SET ALERTACTIVEDURATION (Dauer eines aktiven Alert definieren)
- SET ALERTCLOSEDDURATION (Dauer eines geschlossenen Alert definieren)
- SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren)
- SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)
- SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)
- SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)
- SET ALERTINACTIVEDURATION (Dauer eines inaktiven Alert definieren)
- SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)
- SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren)
- SET ALERTUPDATEINTERVAL (Häufigkeit definieren, mit der der Alertmonitor Alerts aktualisiert und bereinigt)
- SET ARCHIVERETENTIONPROTECTION (Aufbewahrungsschutz für Daten aktivieren)
- SET ARREPLRULEDEFAULT (Serverreplikationsregel für Archivierungsdaten definieren)
- SET BKREPLRULEDEFAULT (Serverreplikationsregel für Sicherungsdaten definieren)
- SET CLIENTACTDURATION (Verweildauer für Clientaktion definieren)
- SET CONFIGMANAGER (Konfigurationsmanager angeben)
- SET CONFIGREFRESH (Aktualisierung der Konfiguration verwalteter Server definieren)
- SET CONTEXTMESSAGING (Anzeigen von Nachrichtenkontext aktivieren oder inaktivieren)
- SET CPUINFOREFRESH (Aktualisierungsintervall für Informationssuche auf Client-Workstation)
- SET CROSSDEFINE (Querdefinition von Servern angeben)
- SET DBRECOVERY (Einheitenklasse für automatische Sicherungen definieren)
- SET DEDUPVERIFICATIONLEVEL (Prozentsatz der zu prüfenden Bereiche definieren)
- SET DEFAULTAUTHENTICATION (Standardauthentifizierungsmethode für Befehle REGISTER NODE und REGISTER ADMIN definieren)
- SET DEPLOYPKGMR (Implementierungspaketmanager aktivieren)
- SET DEPLOYREPOSITORY (Downloadpfad für Clientimplementierungspakete definieren)
- SET DEPLOYMAXPKGS (Maximale Anzahl Clientimplementierungspakete definieren, die gespeichert werden sollen)
- SET DISSIMILARPOLICIES (Die Maßnahmen auf dem Zielreplikationsserver für die Verwaltung replizierter Daten aktivieren)
- SET DRMACTIVEDATASTGPOOL (Von DRM zu verwaltende Pools für aktive Daten angeben)
- SET DRMCHECKLABEL (Kennsatzprüfung angeben)
- SET DRMCMDFILENAME (Namen einer Datei angeben, die Befehle enthalten soll)
-    SET DRMCOPYCONTAINERSTGPOOL (Containerkopierspeicherpools angeben, die von DRM-Befehlen verarbeitet werden sollen)
- SET DRMCOPYSTGPOOL (Von DRM zu verwaltende Kopierspeicherpools angeben)
- SET DRMCOURIERNAME (Kuriernamen angeben)
- SET DRMDBBACKUPEXPIREDAYS (Verfall für DB-Sicherungsreihe angeben)
- SET DRMFILEPROCESS (Dateiverarbeitung angeben)
- SET DRMINSTRPREFIX (Präfix für Wiederherstellungsanweisungsdateinamen angeben)
- SET DRMNOTMOUNTABLENAME (Nicht mountfähigen Standort angeben)
- SET DRMPPLANPREFIX (Präfix für Wiederherstellungsplandateinamen angeben)
- SET DRMPPLANVPOSTFIX (Namen für Ersatzdatenträger angeben)
- SET DRMPRIMSTGPOOL (Von DRM zu verwaltende primäre Speicherpools angeben)
- SET DRMRPFEXPIREDAYS (Kriterien für Verfall von Wiederherstellungsplandateien definieren)
- SET DRMVAULTNAME (Aufbewahrungsort angeben)
- SET EVENTRETENTION (Aufbewahrungszeitraum für Ereignissätze definieren)
- SET FAILOVERHLADDRESS (Adresse höherer Ebene für Übernahme definieren)
- SET INVALIDPWLIMIT (Anzahl der ungültigen Anmeldeversuche definieren)

- SET LDAPPASSWORD (LDAP-Kennwort für den Server definieren)
- SET LDAPUSER (ID für einen LDAP-Verzeichnisserver angeben)
- SET LICENSEAUDITPERIOD (Dauer für Lizenzprüfung definieren)
- SET MAXCMDRETRIES (Maximale Anzahl Befehlswiederholungen definieren)
- SET MAXSCHEDESESSIONS (Maximale Anzahl geplanter Sitzungen definieren)
- SET MINPWLENGTH (Mindestlänge für Kennwort definieren)
- SET MONITORINGADMIN (Name des Überwachungsadministrators definieren)
- SET MONITOREDSEVERGROUP (Gruppe überwachter Server definieren)
- SET NODEATRISKINTERVAL (Gibt den Gefährdungsmodus für einen einzelnen Knoten an)
- SET PASSEXP (Ablaufdatum für Kennwort definieren)
- SET PRODUCTOFFERING (Produktangebot definieren, das für Ihr Unternehmen lizenziert ist)
- SET QUERYSCHEDPERIOD (Zeitraum für Abfrage von Clientknoten definieren)
- SET RANDOMIZE (Zufallsgenerierung von geplanten Startzeiten definieren)
- SET REPLRECOVERDAMAGED (Angabe, ob beschädigte Dateien von einem Replikationsserver wiederhergestellt werden)
- SET REPLRETENTION (Aufbewahrungszeitraum für Replikationsdatensätze definieren)
- SET REPLSERVER (Zielreplikationsserver definieren)
- SET RETRYPERIOD (Zeitintervall zwischen Wiederholungsversuchen definieren)
- SET SCHEDMODES (Modus für zentrale Zeitplanung auswählen)
- SET SERVERHLADDRESS (Serveradresse der höheren Ebene definieren)
- SET SERVERLLADDRESS (Serveradresse der unteren Ebene definieren)
- SET SERVERNAME (Servernamen angeben)
- SET SERVERPASSWORD (Kennwort für Server definieren)
- SET SPREPLRULEDEFAULT (Serverreplikationsregel für speicher verwaltete Daten definieren)
- SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)
- SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)
- SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)
- SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll)
- SET SUBFILE (Subdateisicherung für Clientknoten definieren)
- SET SUMMARYRETENTION (Anzahl Tage für Aufbewahren in Aktivitätsübersichtstabelle definieren)
- SET TAPEALERTMSG (Bandalerts aktivieren oder inaktivieren)
- SET TOCLOADRETENTION (Aufbewahrungszeitraum für Laden für Inhaltsverzeichnis definieren)
- SET VMATRISKINTERVAL (Gibt den Gefährdungsmodus für einen einzelnen VM-Dateibereich an)


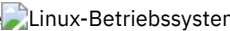
## SET ACCOUNTING (Abrechnungssätze aktivieren/inaktivieren)

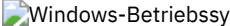
---

Mit diesem Befehl kann festgelegt werden, ob am Ende jeder Client-Knotensitzung ein Abrechnungssatz erstellt werden soll. Ein Abrechnungssatz protokolliert den von einer Client-Knotensitzung benötigten Speicherbereich.

Mit dem Befehl QUERY STATUS kann geprüft werden, ob Abrechnungssätze generiert werden. Bei der Installation wird dieser Wert auf OFF gesetzt.

Die Abrechnungssätze werden in einer Abrechnungsdatei mit dem Namen dsmacct.log gespeichert.

  Die Umgebungsvariable DSMSERV\_ACCOUNTING\_DIR gibt das Verzeichnis an, in dem sich die Abrechnungsdatei befindet.

 Ein Registryeintrag steuert die Position des Abrechnungsprotokolls.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-Set ACCounting--+-ON--+-----><
                    '-OFF-'
```

## Parameter

---

ON

Gibt an, dass der Server am Ende jeder Clientknotensitzung einen Abrechnungssatz erstellen soll.

Off

Gibt an, dass der Server keine Abrechnungssätze erstellen soll.

## Beispiel: Abrechnungssätze erstellen

Geben Sie den folgenden Befehl aus, um am Ende jeder Clientknotensitzung einen Abrechnungssatz zu erstellen:

```
set accounting on
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ACCOUNTING

| Befehl       | Beschreibung   |
|--------------|--|
| QUERY STATUS | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## SET ACTLOGRETENTION (Aufbewahrungsdauer für das Aktivitätenprotokoll definieren)

Verwenden Sie diesen Befehl, um die Sätze des Aktivitätenprotokolls nach Datum oder Größe zu verwalten. Das Aktivitätenprotokoll enthält normale Aktivitätsnachrichten, die vom Server generiert werden. Diese Nachrichten enthalten Informationen zu Server- und Clientoperationen, wie die Startzeit der Sitzungen oder E/A-Fehler von Einheiten.

Unter anderem sind folgende Nachrichten im Aktivitätenprotokoll enthalten:

- Anfang und Ende von Client-Sitzungen.
- Anfang und Ende von Umlagerungen.
- Diagnosefehlnachrichten
- Ausgabedaten geplanter Verwaltungsbefehle

Bei der Serverinstallation basiert die Verwaltung des Aktivitätenprotokolls auf dem Aufbewahrungszeitraum. Der Aufbewahrungszeitraum wird auf 30 Tage gesetzt.

Sie können den Zeitraum anpassen, für den das Aktivitätenprotokoll Nachrichten aufbewahrt, um unzureichende oder veraltete Daten zu vermeiden. Nach Ablauf des Aufbewahrungszeitraums entfernt der Server automatisch die Nachrichten aus dem Aktivitätenprotokoll.

Alternativ können Sie die Gesamtgröße des Aktivitätenprotokolls begrenzen, um den Speicherbereich zu steuern, der von dem Aktivitätenprotokoll belegt wird. Der Server entfernt regelmäßig die ältesten Sätze im Aktivitätenprotokoll, bis die Größe des Aktivitätenprotokolls nicht mehr die konfigurierte maximal zulässige Größe überschreitet.

Mit dem Befehl QUERY STATUS können Sie die aktuelle Anzahl der Sätze im Aktivitätenprotokoll und die Größe (in Megabyte) anzeigen, die das Aktivitätenprotokoll gegenwärtig belegt.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
.-Mgmtstyle---Date----.
>>-Set ACTlogretention--Anzahl-----+-----><
'-Mgmtstyle-----Date+-'
'-Size-'
```

## Parameter

Anzahl (Erforderlich)

Gibt die Anzahl der Tage an, die Nachrichten im Aktivitätenprotokoll aufbewahrt werden sollen, wenn das Protokoll nach Datum verwaltet wird, oder gibt die maximale Größe des Aktivitätenprotokolls an, wenn das Protokoll nach Größe verwaltet wird. Bei der Verwaltung auf der Basis des Aufbewahrungszeitraums gibt der Wert 1 an, dass die Sätze im Aktivitätenprotokoll nur für den aktuellen Tag aufbewahrt werden sollen. Bei der Verwaltung auf der Basis der Größe gibt der Wert 1 eine maximale Größe von 1

MB für das Aktivitätenprotokoll an. Es kann eine Zahl von 0 bis 9999 angegeben werden. Der Wert 0 inaktiviert die Aufbewahrungsdauer für das Aktivitätenprotokoll.

#### Mgmtstyle

Gibt an, ob die Verwaltung des Aktivitätenprotokolls auf dem Aufbewahrungszeitraum oder der Größe basiert. Dieser Parameter ist wahlfrei. Der Standardwert ist DATE. Gültige Werte:

#### Date

Gibt an, dass die Verwaltung des Aktivitätenprotokolls auf dem Aufbewahrungszeitraum basiert.

#### Size

Gibt an, dass die Verwaltung des Aktivitätenprotokolls auf der Größe basiert.

## Beispiel: Aufbewahrungsdauer für das Aktivitätenprotokoll definieren

Der Server soll die Sätze im Aktivitätenprotokoll 60 Tage lang aufbewahren. Den folgenden Befehl ausgeben:

```
set actlogretention 60
```

## Beispiel: Die Größe des Aktivitätenprotokolls definieren

Den Server so definieren, dass die Größe des Aktivitätenprotokolls auf 300 MB begrenzt wird. Den folgenden Befehl ausgeben:

```
set actlogretention 300 mgmtstyle=size
```

## Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET ACTLOGRETENTION

| Befehl       | Beschreibung   |
|--------------|--|
| QUERY ACTLOG | Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.   |
| QUERY STATUS | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## SET ALERTACTIVEDURATION (Dauer eines aktiven Alert definieren)

Verwenden Sie diesen Befehl, um die Dauer anzugeben, die ein Alert aktiv bleibt, bevor er inaktiv wird. Wenn ein aktiver Alert erneut ausgelöst wird, wird die Dauer erneut gestartet.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set ALERTACTiveduration -Anzahl Minuten-----<<
```

## Parameter

Anzahl Minuten (Erforderlich)

Gibt die Anzahl Minuten an, die ein Alert aktiv bleibt, bevor er inaktiv wird. Geben Sie einen Wert von 1 bis 20160 an. Der anfängliche Serverstandardwert ist 480 Minuten.

## Die Dauer eines aktiven Alert auf einen Tag setzen

Mit dem folgenden Befehl angeben, dass Alerts 1440 Minuten aktiv bleiben, bevor sich ihr Status in 'inaktiv' ändert:

```
set alertactiveduration 1440
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTACTIVEDURATION

| Befehl | Beschreibung |
|--------|--------------|
|--------|--------------|

| Befehl   | Beschreibung   |
|--|--|
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen) | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an. |
| SET ALERTINACTIVEDURATION (Dauer eines inaktiven Alert definieren)   | Gibt an, wie lange ein Alert inaktiv bleibt, bevor er geschlossen wird.                          |
| SET ALERTCLOSEDDURATION (Dauer eines geschlossenen Alert definieren)   | Gibt an, wie lange ein Alert geschlossen bleibt, bevor er gelöscht wird.                         |
| SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)   | Gibt an, ob die Alertüberwachung aktiviert oder inaktiviert ist.                                 |
| SET ALERTUPDATEINTERVAL (Häufigkeit definieren, mit der der Alertmonitor Alerts aktualisiert und bereinigt)      | Gibt an, wie oft der Alertmonitor Alerts in der Datenbank aktualisiert und bereinigt.            |

## SET ALERTCLOSEDDURATION (Dauer eines geschlossenen Alert definieren)

Verwenden Sie diesen Befehl, um die Dauer anzugeben, die ein Alert geschlossen bleibt, bevor er gelöscht wird.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-Set ALERTClosedduration -Anzahl Minuten-----<<
```

### Parameter

Anzahl Minuten (Erforderlich)

Gibt die Anzahl Minuten an, die ein Alert geschlossen bleibt, bevor er gelöscht wird. Wird der Wert 0 angegeben, werden Alerts unverzüglich gelöscht, nachdem sie geschlossen wurden. Geben Sie einen Wert von 0 bis 99999 an. Der Standardwert wird auf 60 Minuten gesetzt, wenn die IBM Spectrum Protect-Serverdatenbank anfänglich formatiert wird.

### Alerts zwei Stunden nach dem Schließen löschen

Angeben, dass Alerts 120 Minuten geschlossen bleiben, bevor sie gelöscht werden:

```
set alertclosedduration 120
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTCLOSEDDURATION

| Befehl   | Beschreibung   |
|--|--|
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen) | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an. |
| SET ALERTACTIVEDURATION (Dauer eines aktiven Alert definieren)   | Gibt an, wie lange ein Alert aktiv bleibt, bevor er in den Status 'inaktiv' versetzt wird.       |
| SET ALERTINACTIVEDURATION (Dauer eines inaktiven Alert definieren)   | Gibt an, wie lange ein Alert inaktiv bleibt, bevor er geschlossen wird.                          |
| SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)   | Gibt an, ob die Alertüberwachung aktiviert oder inaktiviert ist.                                 |
| SET ALERTUPDATEINTERVAL (Häufigkeit definieren, mit der der Alertmonitor Alerts aktualisiert und bereinigt)      | Gibt an, wie oft der Alertmonitor Alerts in der Datenbank aktualisiert und bereinigt.            |

## SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren)

Verwenden Sie diesen Befehl, um das Senden von Alerts als E-Mail an angegebene Administratoren zu ermöglichen.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set ALERTEMail---ON---+-----<<  
      '-OFF-'
```

## Parameter

ON

Gibt an, dass Alerts als E-Mail an angegebene Administratoren gesendet werden können.

OFF

Gibt an, dass Alerts nicht als E-Mail an angegebene Administratoren gesendet werden können. Wenn die Serverdatenbank anfänglich formatiert wird, wird die Einstellung für ALERTEMAIL auf OFF gesetzt.

## Das Senden von Alerts bei ihrem Auftreten an den Administrator ermöglichen

Den folgenden Befehl ausgeben, um das Senden von Alerts als E-Mail zu ermöglichen:

```
SET ALERTEMAIL ON
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTEMAIL

| Befehl  | Beschreibung   |
|---|--|
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)      | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.       |
| SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)  | Gibt die E-Mail-Adresse des Absenders des Alerts an.   |
| SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)  | Gibt den Hostnamen des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird. |
| SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)   | Gibt den Anschluss des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird. |
| SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren) | Gibt die Administratoren an, die Alertzusammenfassungen als E-Mail empfangen möchten.                  |

## SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)

Verwenden Sie diesen Befehl, um die E-Mail-Adresse des Absenders des Alert anzugeben.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set ALERTEMAILFromaddr -E-Mail-Adresse-----<<
```

## Parameter

E-Mail-Adresse (Erforderlich)

Gibt die E-Mail-Adresse des Absenders an. E-Mail-Adressen haben das Format *Name@Domäne*. E-Mail-Namen, einschließlich der Adresse, dürfen 64 Zeichen nicht überschreiten, und der Domänenname darf 255 Zeichen nicht überschreiten.

## Die E-Mail-Adresse des Absenders des Alert angeben

Den folgenden Befehl ausgeben, um die E-Mail-Adresse des Absenders anzugeben:

```
set alertemailfromaddr djadmin@mydomain.com
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTEMAILFROMADDR

| Befehl  | Beschreibung   |
|---|--|
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)      | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.       |
| SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren)                      | Ermöglicht das Senden von Alerts als E-Mail an angegebene Administratoren.                             |
| SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)  | Gibt den Hostnamen des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird. |
| SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)   | Gibt den Anschluss des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird. |
| SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren) | Gibt die Administratoren an, die Alertzusammenfassungen als E-Mail empfangen möchten.                  |

## SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)

Verwenden Sie diesen Befehl, um den Hostnamen des SMTP-Mail-Servers (SMTP = Simple Mail Transfer Protocol) anzugeben, der zum Senden der Alert-E-Mail verwendet wird.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-Set ALERTEMAILSMTPHost--Hostname-----<<
```

### Parameter

Hostname (Erforderlich)  
Gibt den Hostnamen des SMTP-Mail-Servers an.

## Den Hostnamen des SMTP-Mail-Servers als mail.domain.com angeben

Den folgenden Befehl ausgeben, um `mail.domain.com` als SMTP-Mail-Server anzugeben:

```
set alertemailsmtphost mail.domain.com
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTEMAILSMTPHOST

| Befehl  | Beschreibung   |
|---|--|
| SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren)                      | Ermöglicht das Senden von Alerts als E-Mail an angegebene Administratoren.                             |
| SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)  | Gibt die E-Mail-Adresse des Absenders des Alerts an.   |
| SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)   | Gibt den Anschluss des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird. |
| SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren) | Gibt die Administratoren an, die Alertzusammenfassungen als E-Mail empfangen möchten.                  |



## SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)

Verwenden Sie diesen Befehl, um die Anschlussnummer des SMTP-Mail-Servers anzugeben. Dieser E-Mail-Server wird zum Senden der Alerts als E-Mail verwendet.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-Set ALERTEMAILSMTPPort--TCP-Anschluss-----<<
```

### Parameter

TCP-Anschluss (Erforderlich)

Gibt die Anschlussnummer des SMTP-Mail-Servers an. Geben Sie einen Wert von 1 bis 32767 an. Die Standardanschlussnummer ist 25.

### Die Anschlussnummer des SMTP-Mail-Servers angeben

Den folgenden Befehl ausgeben, um die Anschlussnummer 450 für den SMTP-Mail-Server anzugeben:

```
set alertemailsmtpport 450
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTEMAILSMTPPORT

| Befehl  | Beschreibung   |
|---|--|
| SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren)                      | Ermöglicht das Senden von Alerts als E-Mail an angegebene Administratoren.                             |
| SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)  | Gibt die E-Mail-Adresse des Absenders des Alerts an.   |
| SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)  | Gibt den Hostnamen des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird. |
| SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren) | Gibt die Administratoren an, die Alertzusammenfassungen als E-Mail empfangen möchten.                  |

## SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren)

Verwenden Sie diesen Befehl, um die Administratoren anzugeben, die jede Stunde Alertzusammenfassungen als E-Mail empfangen möchten.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-Set ALERTSUMMARYToadmins---Administratorname-----<<  
'-',-----'
```

### Parameter

Administratorname (Erforderlich)

Gibt den Namen des Administrators an, der Alertzusammenfassungen als E-Mail empfangen möchte. Es können maximal drei Administratornamen angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden.

## Zwei Administratoren für den Empfang von Alertzusammenfassungen angeben

Mit dem folgenden Befehl angeben, dass die Administratoren HARRY und COLIN Alertzusammenfassungen empfangen möchten:

```
set alertsummarytoadmins HARRY,COLIN
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTSUMMARYTOADMINS

| Befehl   | Beschreibung   |
|--|--|
| SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren) | Ermöglicht das Senden von Alerts als E-Mail an angegebene Administratoren.                             |
| SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)                                 | Gibt die E-Mail-Adresse des Absenders des Alerts an.   |
| SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)                               | Gibt den Hostnamen des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird. |
| SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)                          | Gibt den Anschluss des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird. |

## SET ALERTINACTIVEDURATION (Dauer eines inaktiven Alert definieren)

Verwenden Sie diesen Befehl, um die Dauer anzugeben, die ein Alert inaktiv bleibt. Nach Ablauf dieses Zeitraums wird der Alert geschlossen.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set ALERTINactiveduration -Anzahl Minuten-----><
```

## Parameter

Anzahl Minuten (Erforderlich)

Gibt die Anzahl Minuten an, die ein Alert inaktiv bleibt, bevor er geschlossen wird. Sie können einen Wert im Bereich von 1 bis 20160 angeben. Der anfängliche Serverstandardwert ist 480 Minuten.

## Den Alertstatus nach 60 Minuten von 'inaktiv' in 'geschlossen' ändern

Mit dem folgenden Befehl angeben, dass ein Alert 60 Minuten im Status 'inaktiv' verbleibt, bevor sein Status in 'geschlossen' geändert wird:

```
set alertinactiveduration 60
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTINACTIVEDURATION

| Befehl   | Beschreibung   |
|--|--|
| SET ALERTACTIVEDURATION (Dauer eines aktiven Alert definieren)       | Gibt an, wie lange ein Alert aktiv bleibt, bevor er in den Status 'inaktiv' versetzt wird. |
| SET ALERTCLOSEDDURATION (Dauer eines geschlossenen Alert definieren) | Gibt an, wie lange ein Alert geschlossen bleibt, bevor er gelöscht wird.                   |
| SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)         | Gibt an, ob die Alertüberwachung aktiviert oder inaktiviert ist.                           |

| Befehl  | Beschreibung  |
|---|---|
| SET ALERTUPDATEINTERVAL (Häufigkeit definieren, mit der der Alertmonitor Alerts aktualisiert und bereinigt) | Gibt an, wie oft der Alertmonitor Alerts in der Datenbank aktualisiert und bereinigt. |

## SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)

Verwenden Sie diesen Befehl, um den Alertmonitor zu aktivieren oder zu inaktivieren.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```

>>-Set ALERTMONITOR .-Off-.
>>-Set ALERTMONITOR -+ON-+-----<<

```

### Parameter

ON

Gibt an, dass der IBM Spectrum Protect-Server Alerts überwacht.

OFF

Gibt an, dass der IBM Spectrum Protect-Server Alerts nicht überwacht. Wenn die IBM Spectrum Protect-Serverdatenbank anfänglich formatiert wird, wird die Einstellung für die Alertüberwachung auf OFF gesetzt.

### Alertüberwachung aktivieren

Den folgenden Befehl ausgeben, um die Alertüberwachung zu aktivieren:

```
set alertmonitor on
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTMONITOR

| Befehl  | Beschreibung  |
|---|---|
| SET ALERTACTIVEDURATION (Dauer eines aktiven Alert definieren)  | Gibt an, wie lange ein Alert inaktiv bleibt, bevor er geschlossen wird.               |
| SET ALERTINACTIVEDURATION (Dauer eines inaktiven Alert definieren)  | Gibt an, wie lange ein Alert inaktiv bleibt, bevor er geschlossen wird.               |
| SET ALERTCLOSEDDURATION (Dauer eines geschlossenen Alert definieren)  | Gibt an, wie lange ein Alert geschlossen bleibt, bevor er gelöscht wird.              |
| SET ALERTUPDATEINTERVAL (Häufigkeit definieren, mit der der Alertmonitor Alerts aktualisiert und bereinigt) | Gibt an, wie oft der Alertmonitor Alerts in der Datenbank aktualisiert und bereinigt. |

## SET ALERTUPDATEINTERVAL (Häufigkeit definieren, mit der der Alertmonitor Alerts aktualisiert und bereinigt)

Mit diesem Befehl können Sie angeben, wie oft der Alertmonitor Alerts aktualisiert und bereinigt, die in der IBM Spectrum Protect-Serverdatenbank gespeichert sind.

Während dieses Prüfintervalls werden vom Alertmonitor alle Alerts auf dem Server untersucht und die folgenden Aktionen ausgeführt:

- Der Alertmonitor bestimmt, ob der Zeitraum für den aktiven oder inaktiven Status abgelaufen ist. Läuft der angegebene Zeitraum ab, wird der Alertstatus in den nächsten Status aktualisiert. Beispiel:
  - 'Aktiv' in 'inaktiv'
  - 'Inaktiv' in 'geschlossen'
- Ist ein Alert für die mit dem Befehl SET ALERTCLOSEDDURATION angegebene Dauer geschlossen, wird der Alert gelöscht.

Sie können mit dem Befehl QUERY MONITORSETTINGS bestimmen, ob die Alertüberwachung aktiviert ist. Verwenden Sie den Befehl SET ALERTMONITOR, um die Alertüberwachung zu aktivieren.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set ALERTUPDateinterval -Anzahl Minuten-----><
```

## Parameter

Anzahl Minuten (Erforderlich)

Gibt die Zeit in Minuten an, die der Monitor wartet, bevor Alerts auf dem Server aktualisiert und bereinigt werden. Geben Sie einen Wert von 1 bis 9999 an. Der Server hat einen ursprünglichen Standardwert von 10 Minuten.

## Das Alertaktualisierungsintervall auf 60 Minuten setzen

Mit dem folgenden Befehl angeben, dass Alerts jede Stunde aktualisiert werden:

```
set alertupdateinterval 60
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTUPDATEINTERVAL

| Befehl   | Beschreibung   |
|--|--|
| SET ALERTACTIVEDURATION (Dauer eines aktiven Alert definieren)       | Gibt an, wie lange ein Alert aktiv bleibt, bevor er in den Status 'inaktiv' versetzt wird. |
| SET ALERTINACTIVEDURATION (Dauer eines inaktiven Alert definieren)   | Gibt an, wie lange ein Alert inaktiv bleibt, bevor er geschlossen wird.                    |
| SET ALERTCLOSEDDURATION (Dauer eines geschlossenen Alert definieren) | Gibt an, wie lange ein Alert geschlossen bleibt, bevor er gelöscht wird.                   |
| SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)         | Gibt an, ob die Alertüberwachung aktiviert oder inaktiviert ist.                           |

## SET ARCHIVERETENTIONPROTECTION (Aufbewahrungsschutz für Daten aktivieren)

Mit diesem Befehl können Sie den Aufbewahrungsschutz für Archivierungsdaten aktivieren und inaktivieren. Der Server darf keine Daten enthalten, damit dieser Befehl arbeitet. Bei der Installation wird dieser Wert auf OFF gesetzt.

Ist der Aufbewahrungsschutz für Archivierungsdaten aktiv, gilt Folgendes:

- Es können nur Archivierungskopien auf dem Server gespeichert werden.
- Eine Archivierungskopie kann erst gelöscht werden, wenn der Parameter RETVER im Befehl DEFINE COPYGROUP (Archivierung) erfüllt wurde.

Das Definieren von Speicherpools mit dem Typ RECLAMATIONTYPE=SNAPLOCK wird nur auf Servern mit aktiviertem Aufbewahrungsschutz für Daten unterstützt.

Verwenden Sie den Befehl QUERY STATUS, um den Status des Aufbewahrungsschutzes für Archivierungsdaten anzuzeigen.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-Set ARCHIVERETENTIONPROTECTIon -+-Off-+-----><
```

## Parameter

- OFF  
Gibt an, dass der Aufbewahrungsschutz für Archivierungsdaten nicht aktiv ist.
- ON  
Gibt an, dass der Aufbewahrungsschutz für Archivierungsdaten aktiv ist.

## Beispiel: Aufbewahrungsschutz für Daten aktivieren

Den Aufbewahrungsschutz für Archivierungsdaten durch Ausgabe des folgenden Befehls aktivieren:

```
set archiveretentionprotection on
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ARCHIVERETENTIONPROTECTION

| Befehl             | Beschreibung   |
|--------------------|--|
| ACTIVATE POLICYSET | Wertet eine Maßnahmengruppe aus und aktiviert sie.   |
| AUDIT VOLUME       | Vergleicht Datenbank- und Speicherpooldaten und (wahlfrei) beseitigt Inkonsistenzen.   |
| DEFINE COPYGROUP   | Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse.  |
| DEFINE VOLUME      | Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.   |
| DELETE FILESPACE   | Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt. |
| QUERY COPYGROUP    | Zeigt die Attribute einer Kopiengruppe an.   |
| QUERY STATUS       | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.   |
| UPDATE COPYGROUP   | Ändert ein oder mehrere Attribute einer Kopiengruppe.  |

## SET ARREPLRULEDEFAULT (Serverreplikationsregel für Archivierungsdaten definieren)

Mit diesem Befehl können Sie die Serverreplikationsregel für Archivierungsdaten definieren.

Einschränkung: Die Replikationsregel, die Sie mit diesem Befehl definieren, wird nur angewendet, wenn Dateibereichsregeln und Clientknotenregeln für Archivierungsdaten auf DEFAULT gesetzt sind.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Sie können eine Replikationsregel für normale Priorität oder eine Replikationsregel für hohe Priorität angeben. In einem Replikationsprozess, der sowohl Daten mit normaler Priorität als auch Daten mit hoher Priorität einschließt, werden Daten mit hoher Priorität zuerst repliziert. Bevor Sie eine Regel angeben, beachten Sie die Reihenfolge, in der die Daten repliziert werden sollen.

Beispiel: Angenommen, Ihre Clientknoten enthalten Archivierungsdaten und Sicherungsdaten. Die Replikation der Archivierungsdaten hat eine höhere Priorität als die der Sicherungsdaten. Um die Archivierungsdaten zu priorisieren, geben Sie den Befehl SET ARREPLRULEDEFAULT aus und geben Sie die Replikationsregel ALL\_DATA\_HIGH\_PRIORITY an. Um die Sicherungsdaten zu priorisieren, geben Sie den Befehl SET BKREPLRULEDEFAULT aus und geben Sie die Replikationsregel ALL\_DATA für Sicherungsdaten an. Die Regel ALL\_DATA für Sicherungsdaten repliziert Sicherungsdaten mit einer normalen Priorität.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set ARREPLRuledefault--+-ALL_DATA-----+-----><
      +-ALL_DATA_HIGH_PRIORITY-+
      '-NONE-----'
```

## Parameter

ALL\_DATA  
Repliziert Archivierungsdaten mit einer normalen Priorität.

ALL\_DATA\_HIGH\_PRIORITY  
Repliziert Archivierungsdaten mit einer hohen Priorität.

NONE  
Die Archivierungsdaten werden nicht repliziert.

## Beispiel: Die Serverreplikationsregel für Archivierungsdaten definieren

Die Standardregel für Archivierungsdaten so definieren, dass die Replikation mit einer hohen Priorität erfolgt.

```
set arreplruledefault all_data_high_priority
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ARREPLRULEDEFAULT

| Befehl                | Beschreibung   |
|-----------------------|--|
| QUERY FILESPACE       | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.                                      |
| QUERY NODE            | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.                                    |
| QUERY REPLICATION     | Zeigt Informationen zu Knotenreplikationsprozessen an.   |
| QUERY REPLRULE        | Zeigt Informationen zu Knotenreplikationsregeln an.  |
| QUERY STATUS          | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| REPLICATE NODE        | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |
| SET BKREPLRULEDEFAULT | Gibt die Serverknotenreplikationsregel für Sicherungsdaten an.   |
| SET SPREPLRULEDEFAULT | Gibt die Serverknotenreplikationsregel für speicherwaltete Daten an.   |
| UPDATE FILESPACE      | Ändert Knotenreplikationsregeln für Dateibereiche.   |
| UPDATE REPLRULE       | Aktiviert oder inaktiviert Replikationsregeln.   |
| VALIDATE REPLICATION  | Überprüft die Replikation für Dateibereiche und Datentypen.  |

## SET BKREPLRULEDEFAULT (Serverreplikationsregel für Sicherungsdaten definieren)

Mit diesem Befehl können Sie die Serverreplikationsregel für Sicherungsdaten definieren.

Einschränkung: Die Replikationsregel, die Sie mit diesem Befehl definieren, wird nur angewendet, wenn Dateibereichsregeln und Clientknotenregeln für Sicherungsdaten auf DEFAULT gesetzt sind.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Sie können Replikationsregeln für normale Priorität oder Replikationsregeln für hohe Priorität angeben. In einem Replikationsprozess, der sowohl Daten mit normaler Priorität als auch Daten mit hoher Priorität einschließt, werden Daten mit hoher Priorität zuerst repliziert. Bevor Sie eine Regel angeben, beachten Sie die Reihenfolge, in der die Daten repliziert werden sollen.

Beispiel: Angenommen, Ihre Clientknoten enthalten Archivierungsdaten und aktive Sicherungsdaten. Die Replikation der aktiven Sicherungsdaten hat eine höhere Priorität als die der Archivierungsdaten. Um die Sicherungsdaten zu priorisieren, geben Sie den Befehl SET BKREPLRULEDEFAULT aus und geben Sie die Replikationsregel ACTIVE\_DATA\_HIGH\_PRIORITY an. Um die Archivierungsdaten zu priorisieren, geben Sie den Befehl SET ARREPLRULEDEFAULT aus und geben Sie die Replikationsregel ALL\_DATA für Archivierungsdaten an. Die Regel ALL\_DATA für Archivierungsdaten repliziert Archivierungsdaten mit einer normalen Priorität.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set BKREPLRuledefault--+--ALL_DATA-----+-----><
      +-ACTIVE_DATA-----+
      +-ALL_DATA_HIGH_PRIORITY-----+
      +-ACTIVE_DATA_HIGH_PRIORITY--+
      '-NONE-----'
```

## Parameter

### ALL\_DATA

Repliziert aktive und inaktive Sicherungsdaten. Die Daten werden mit normaler Priorität repliziert.

### ACTIVE\_DATA

Repliziert aktive Sicherungsdaten. Die Daten werden mit normaler Priorität repliziert.

Achtung: Wenn Sie ACTIVE\_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

- Wenn eine frühere Serverversion als Version 7.1.1 auf dem Quellen- oder Zielreplikationsserver installiert ist.
- Wenn Sie den Befehl REPLICATE NODE mit dem Parameter FORCERECONCILE=YES verwenden.
- Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Serverversion vor Version 7.1.1 ausführen.

Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

### ALL\_DATA\_HIGH\_PRIORITY

Repliziert aktive und inaktive Sicherungsdaten. Daten werden mit einer hohen Priorität repliziert.

### ACTIVE\_DATA\_HIGH\_PRIORITY

Diese Regel entspricht der Replikationsregel ACTIVE\_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden.

### NONE

Die Sicherungsdaten werden nicht repliziert.

## Beispiel: Die Serverreplikationsregel für Sicherungsdaten definieren

Die Standardregel für Sicherungsdaten so definieren, dass nur aktive Daten und die Daten mit einer hohen Priorität repliziert werden.

```
set bkreplruledefault active_data_high_priority
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET BKREPLRULEDEFAULT

| Befehl            | Beschreibung  |
|-------------------|---|
| QUERY FILESPACE   | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.   |
| QUERY NODE        | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an. |
| QUERY REPLICATION | Zeigt Informationen zu Knotenreplikationsprozessen an.                            |
| QUERY REPLRULE    | Zeigt Informationen zu Knotenreplikationsregeln an.                               |

| Befehl                | Beschreibung   |
|-----------------------|--|
| QUERY STATUS          | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| REPLICATE NODE        | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |
| SET ARREPLRULEDEFAULT | Gibt die Serverknotenreplikationsregel für Archivierungsdaten an.  |
| SET REPLRETENTION     | Gibt den Aufbewahrungszeitraum für Replikationsprotokollsätze an.  |
| SET SPREPLRULEDEFAULT | Gibt die Serverknotenreplikationsregel für speicherverwaltete Daten an.  |
| UPDATE FILESPACE      | Ändert Knotenreplikationsregeln für Dateibereiche.   |
| UPDATE REPLRULE       | Aktiviert oder inaktiviert Replikationsregeln.   |
| VALIDATE REPLICATION  | Überprüft die Replikation für Dateibereiche und Datentypen.  |

## SET CLIENTACTDURATION (Verweildauer für Clientaktion definieren)

Mit diesem Befehl kann die Dauer des Zeitplans angegeben werden, der mit dem Befehl DEFINE CLIENTACTION definiert wurde. Eine Clientaktion definiert einen Zeitplan, der einmal auf einem Client ausgeführt wird.

Das Programm löscht diese Ereignissätze, unabhängig davon, ob der Client den Zeitplan verarbeitet hat oder nicht. Die Zeitpläne werden jedoch erst gelöscht, nachdem die ersten Ereignissätze gelöscht wurden. Der Aufbewahrungszeitraum für Ereignisse wird bei der Installation standardmäßig auf 10 Tage gesetzt.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-SET CLIENTACTDuration--Tage-----<<
```

### Parameter

Tage (Erforderlich)

Gibt die Anzahl der Tage an, die der Zeitplan für die Client-Aktion aktiv ist. Zulässige Werte sind ganze Zahlen von 0 bis 999. Der Standardwert lautet 5 Tage.

Die angegebene Anzahl der Tage bestimmt, wie lange der Zeitplan in der Datenbank aufbewahrt wird, bevor er gelöscht wird. Der Wert 0 gibt an, dass die Dauer des Zeitplans unbegrenzt ist, und der Zeitplan und die Zuordnungen werden nicht aus der Datenbank gelöscht.

### Beispiel: Eine Verweildauer von 15 Tagen für die Clientaktion definieren

Um anzugeben, dass der Zeitplan für die Clientaktion 15 Tage aktiv sein soll, den folgenden Befehl ausgeben:

```
set clientactduration 15
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET CLIENTACTDURATION

| Befehl              | Beschreibung   |
|---------------------|--|
| DEFINE CLIENTACTION | Definiert einen Befehl, der bei einem Clientknoten ausgeführt werden soll.   |
| QUERY STATUS        | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |



## SET CONFIGMANAGER (Konfigurationsmanager angeben)

---

Mit diesem Befehl kann angegeben werden, ob es sich bei einem Server um einen Konfigurationsmanager handelt. Auf einem Konfigurationsmanager können Konfigurationsprofile definiert werden, für die andere Server subscribieren können.

Ein Server kann nicht als Konfigurationsmanager bestimmt werden, wenn der Server für ein oder mehrere Profile auf einem anderen Konfigurationsmanager subscribiert.

Ist ein Server ein Konfigurationsmanager, kann diese Definition erst geändert werden, wenn alle Profile einschließlich des Standardprofils gelöscht werden.

Mit dem Befehl QUERY STATUS kann bestimmt werden, ob ein Server ein Konfigurationsmanager ist. Wenn ein Server installiert wird, wird er nicht als Konfigurationsmanager bestimmt.

### Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

---

```
>>-Set CONFIGManager--+-OF- .
                        +-----+-----><
                        '-ON--'
```

### Parameter

---

ON

Gibt an, dass der Server ein Konfigurationsmanager ist.

Wenn ein Server als Konfigurationsmanager bestimmt wird, erstellt IBM Spectrum Protect ein Standardprofil mit dem Namen DEFAULT\_PROFILE und ordnet dem Profil alle auf dem Konfigurationsmanager definierten Server und Servergruppen zu. Das Standardprofil kann geändert oder gelöscht werden.

Off

Gibt an, dass der Server kein Konfigurationsmanager ist.

### Beispiel: Einen Konfigurationsmanager angeben

---

Einen Server als Konfigurationsmanager bestimmen.

```
set configmanager on
```

### Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für SET CONFIGMANAGER

| Befehl            | Beschreibung   |
|-------------------|--|
| DEFINE PROFILE    | Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.                                      |
| QUERY STATUS      | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| SET CONFIGREFRESH | Gibt das Zeitintervall an, in dem verwaltete Server die Konfigurationsmanager ansprechen sollen.                     |

## SET CONFIGREFRESH (Aktualisierung der Konfiguration verwalteter Server definieren)

---

Mit diesem Befehl kann auf einem verwalteten Server angegeben werden, wie oft dieser Server bei seinem Konfigurationsmanager nach aktualisierten Konfigurationsdaten nachfragen soll.

Soll die aktuelle Einstellung angezeigt werden, den Befehl QUERY STATUS ausgeben. Bei der Installation wird das Intervall auf 60 Minuten gesetzt.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-Set CONFIGRefresh--Minuten-----<<
```

## Parameter

---

Minuten (Erforderlich)

Gibt das Intervall in Minuten an, in dem ein verwalteter Server aktualisierte Konfigurationsdaten von seinem Konfigurationsmanager anfordern soll. Eine ganze Zahl von 0 bis 10000 angeben.

- Ist der Wert größer als 0, nimmt der verwaltete Server sofort Verbindung mit dem Konfigurationsmanager auf. Die nächste Verbindung wird hergestellt, wenn das angegebene Intervall erreicht ist.
- Ist der Wert 0, nimmt der verwaltete Server keine Verbindung mit dem Konfigurationsmanager auf.

Dieser Wert wird ignoriert, wenn der Server nicht für mindestens ein Profil auf einem Konfigurationsmanager subskribiert.

## Beispiel: Ein Aktualisierungsintervall von 45 Minuten definieren

---

Angeben, dass ein verwalteter Server alle 45 Minuten Verbindung mit seinem Konfigurationsmanager aufnehmen soll.

```
set configrefresh 45
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für SET CONFIGREFRESH

| Befehl                 | Beschreibung   |
|------------------------|--|
| DEFINE PROFASSOCIATION | Ordnet Objekte einem Profil zu.  |
| DEFINE PROFILE         | Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.  |
| DELETE PROFASSOCIATION | Löscht die Zuordnung zwischen einem Objekt und einem Profil.                     |
| NOTIFY SUBSCRIBERS     | Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin. |
| SET CONFIGMANAGER      | Gibt an, ob ein Server ein Konfigurationsmanager ist.                            |
| UPDATE PROFILE         | Ändert die Beschreibung eines Profils.   |

## SET CONTEXTMESSAGING (Anzeigen von Nachrichtenkontext aktivieren oder inaktivieren)

---

Verwenden Sie diesen Befehl, um zusätzliche Informationen abzurufen, wenn Nachrichten ANR9999D auftreten. IBM Spectrum Protect fragt die Serverkomponenten nach Informationen ab, die den Prozessnamen, den Threadnamen, die Sitzungs-ID, die Transaktionsdaten, die aktivierten Sperrungen und die verwendeten Datenbanktabellen umfassen.

Anmerkung: Werden nachfolgende Nachrichten aus demselben Codebereich von demselben Thread ausgegeben, enthält nur die erste dieser Nachrichten die Kontextinformationen.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-Set CONTEXTmessaging--+-ON--+-----><
      '-Off-'
```

## Parameter

- ON  
Gibt an, dass das Anzeigen von Nachrichtenkontext aktiviert werden soll.
- OFF  
Gibt an, dass das Anzeigen von Nachrichtenkontext inaktiviert werden soll.

## Beispiel: Anzeigen von Nachrichtenkontext aktivieren oder inaktivieren

Das Anzeigen von Nachrichtenkontext aktivieren, um zusätzliche Informationen zu empfangen, die bei der Bestimmung der Ursache der Nachrichten ANR9999D helfen können.

```
set contextmessaging on
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET CONTEXTMESSAGING

| Befehl       | Beschreibung   |
|--------------|--|
| QUERY STATUS | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## SET CPUINFOREFRESH (Aktualisierungsintervall für Informationssuche auf Client-Workstation)

Mit diesem Befehl können Sie die Anzahl der Tage zwischen Suchläufen nach Client-Workstation-Informationen angeben, die verwendet werden, um die Prozessor-Value-Unit (PVU) zu schätzen.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set CPUINFOREFRESH--Tage-----><
```

## Parameter

- Tage (Erforderlich)  
Gibt die Anzahl der Tage zwischen Suchläufen nach Clienteinheiten an. Soll die aktuelle Einstellung abgerufen werden, geben Sie den Befehl QUERY STATUS aus. Die gültigen Werte sind 1 - 9999. Der Standardwert ist 180.

## Beispiel: Die Zeit vor der nächsten Aktualisierung auf 90 Tage setzen

```
SET CPUINFOREFRESH 90
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET CPUINFOREFRESH

| Befehl            | Beschreibung   |
|-------------------|--|
| QUERY PVUESTIMATE | Zeigt eine Schätzung der Clienteinheiten und Servereinheiten an, die verwaltet werden. |

## SET CROSSDEFINE (Querdefinition von Servern angeben)

Mit diesem Befehl kann angegeben werden, ob ein Server automatisch für einen anderen Server definiert wird.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-Set CROSSDefine--+ON--+-----<<
                          '-Off-'
```

## Parameter

---

ON

Gibt an, daß ein Server für einen anderen Server definiert werden kann. Soll ein Server automatisch für einen anderen Server definiert werden, muß diese Querdefinition auch in der Server-Definition zugelassen werden.

OFF

Gibt an, daß ein Server nicht für einen anderen Server definiert werden kann.

## Beispiel: Querdefinition von Servern angeben

---

Angeben, dass ein Server für einen anderen Server definiert werden kann.

```
set crossdefine on
```

## Zugehörige Befehle

---

Tabelle 1. Zugehöriger Befehl für SET CROSSDEFINE

| Befehl              | Beschreibung   |
|---------------------|--|
| DEFINE SERVER       | Definiert einen Server für die Übertragung zwischen Servern. |
| SET SERVERHLADDRESS | Gibt die Adresse der höheren Ebene eines Servers an.         |
| SET SERVERLLADDRESS | Gibt die Adresse der unteren Ebene eines Servers an.         |
| SET SERVERPASSWORD  | Gibt das Serverkennwort an.                                  |

## SET DBRECOVERY (Einheitenklasse für automatische Sicherungen definieren)

---

Verwenden Sie diesen Befehl, um die Einheitenklasse und die Anzahl der Datenströme anzugeben, die für automatische Datenbanksicherungen verwendet werden sollen. Mit diesem Befehl können Sie auch den Befehl BACKUP DB zum automatischen Sichern des Masterverschlüsselungsschlüssels für den Server konfigurieren.

Der Masterverschlüsselungsschlüssel wird verwendet, um Daten in Verzeichniscontainer- und Cloud-Containerspeicherpools sowie sensible Informationen in der Serverdatenbank zu verschlüsseln. Wird der Masterverschlüsselungsschlüssel nicht gesichert, können Sie möglicherweise nicht auf diese verschlüsselten Elemente zugreifen, wenn ein Katastrophenfall eintritt.

Wenn Sie den Befehl BACKUP DB ausführen und die Einheitenklasse nicht die im Befehl SET DBRECOVERY angegebene Einheitenklasse ist, wird eine Warnung zurückgegeben. Die Sicherungsoperation wird jedoch fortgesetzt und ist nicht betroffen.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
>>-SET DBRECOVery--Einheitenklassenname----->
      .-NUMStreams---1----- . -COMPRESS---No-----
>--+-----+----->
      '-NUMStreams---Anzahl-' '-COMPRESS---+No--+-'
                                   '-Yes-'
```


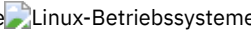
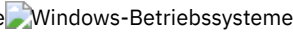


```
set dbrecovery dbback
```

## Beispiel: Eine Einheitenklasse und die Anzahl von Datenströmen für Datenbanksicherungen angeben

Die Einheitenklasse DBBACK für Datenbanksicherungen angeben und angeben, dass die Sicherung zwei Datenversetzungsdatenströme verwenden soll. Den folgenden Befehl ausgeben:

```
set dbrecovery dbback numstreams=2
```

## Beispiel: Verschlüsselungsschlüssel des Speicherpools in Datenbanksicherungen schützen

Speicherpooldaten verschlüsseln, indem angegeben wird, dass Datenbanksicherungen eine Kopie des Masterverschlüsselungsschlüssels für den Server enthalten. Den folgenden Befehl ausgeben:

```
set dbrecovery dbback protectkeys=yes password=Kennwortname
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DBRECOVERY

| Befehl        | Beschreibung   |
|---------------|--|
| BACKUP DB     | Sichert die IBM Spectrum Protect-Datenbank auf Datenträgern mit sequenziellem Zugriff. |
| QUERY DB      | Zeigt Zuordnungsinformationen zu der Datenbank an.                                     |
| QUERY DBSPACE | Zeigt Informationen zum Speicherplatz an, der für die Datenbank definiert ist.         |

## SET DEDUPVERIFICATIONLEVEL (Prozentsatz der zu prüfenden Bereiche definieren)

Verwenden Sie diesen Befehl, um die Bereiche zu überprüfen, die während der clientseitigen Deduplizierung von Daten an den Server gesendet wurden.

Eine außer Kontrolle geratene Anwendung, die sich auf einem Clientsystem befindet und die Client-, API- oder GUI-Anwendung imitiert, kann eine Attacke auf den Server auslösen. Um die Anfälligkeit des Servers für diese Attacken zu verringern, können Sie einen Prozentsatz der Clientbereiche angeben, die vom Server geprüft werden sollen.

Wenn der Server erkennt, dass gerade eine Sicherheitsattacke ausgeführt wird, wird die aktuelle Sitzung abgebrochen. Außerdem wird die Einstellung des Parameters DEDUPLICATION im Befehl REGISTER NODE geändert. Die Einstellung wird von CLIENTORSERVER in SERVERONLY geändert. Mit der Einstellung SERVERONLY wird die clientseitige Deduplizierung von Daten für diesen Knoten inaktiviert.

Der Server gibt auch in einer Nachricht an, dass eine mögliche Sicherheitsattacke festgestellt und die clientseitige Deduplizierung von Daten für den Knoten inaktiviert wurde. Wird die clientseitige Deduplizierung von Daten inaktiviert, werden alle anderen Clientoperationen (z. B. Sicherungsoperationen) fortgesetzt. Es wird nur die clientseitige Deduplizierung von Daten inaktiviert. Wird die clientseitige Deduplizierung von Daten für einen Knoten inaktiviert, da eine mögliche Attacke festgestellt wurde, dedupliziert der Server die Daten, die für die clientseitige Dateneduplizierung ausgewählt werden können.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set DEDUPVERificationlevel--+-0-----+-----><
                               '-Prozentwert-'
```

## Parameter

Prozentwert (Erforderlich)

Geben Sie einen ganzzahligen Wert zwischen 0 - 100 an, um den Prozentsatz der zu prüfenden Clientbereiche anzugeben. Der Wert 0 gibt an, dass keine Clientbereiche geprüft werden. Der Standardwert für diesen Befehl ist 0.

Tipps:

- Die Prüfung der Bereiche beansprucht Verarbeitungskapazität und hat negative Auswirkungen auf die Serverleistung. Geben Sie für eine optimale Leistung keine Werte größer als 10 für diesen Befehl an.
- Um den aktuellen Wert für SET DEDUPVERIFICATIONLEVEL anzuzeigen, geben Sie den Befehl QUERY STATUS aus.

## Beispiel: Eine Mindeststufe für die Dateneduplizierungsprüfung angeben

Um anzugeben, dass 1 % der während der clientseitigen Dateneduplizierung erstellten Bereiche geprüft werden soll, geben Sie den folgenden Befehl aus:

```
set dedupverificationlevel 1
```

## Beispiel: Die Dateneduplizierungsprüfung inaktivieren

Um anzugeben, dass keine der während der clientseitigen Dateneduplizierung erstellten Bereiche geprüft werden sollen, geben Sie den folgenden Befehl aus:

```
set dedupverificationlevel 0
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DEDUPVERIFICATIONLEVEL

| Befehl         | Beschreibung   |
|----------------|--|
| DEFINE STGPOOL | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.                                   |
| QUERY CONTENT  | Zeigt Informationen über Dateien in einem Speicherpoolatenträger an.   |
| QUERY STATUS   | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| REGISTER NODE  | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.                              |
| UPDATE NODE    | Ändert die Attribute, die einem Clientknoten zugeordnet sind.  |
| UPDATE STGPOOL | Ändert die Attribute eines Speicherpools.  |

## SET DEFAULTAUTHENTICATION (Standardauthentifizierungsmethode für Befehle REGISTER NODE und REGISTER ADMIN definieren)

Verwenden Sie diesen Befehl, um die Standardkennwortauthentifizierungsmethode für Knoten und Administratoren zu definieren, die das Ergebnis der Befehle REGISTER NODE und REGISTER ADMIN sind.

Wenn Sie LDAP angeben, definieren Sie den Standardwert für die Authentifizierung mit einem externen Verzeichnis für alle neuen Befehle REGISTER NODE oder REGISTER ADMIN. Dieser Befehl erleichtert die Registrierung von Knoten oder Administratoren, wenn Sie einen LDAP-Verzeichnisserver verwenden.

Tipp: Die Standardauthentifizierungseinstellung kann überschrieben werden, wenn die Authentifizierungsmethode in einem Befehl REGISTER NODE oder REGISTER ADMIN angegeben wird.

## Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie über die Systemberechtigung verfügen.

## Syntax

```
>>-SET DEFAULTAUTHentication---+Local+-----><
                                     '-Ldap--'
```

## Parameter

### Local

Gibt an, dass alle zukünftigen Befehle REGISTER NODE und REGISTER ADMIN, die Sie ausgeben, LOCAL als Parameterwert für die Standardauthentifizierung verwenden. Lokal authentifizierte Kennwörter sind die Kennwörter, die auf dem IBM Spectrum Protect-Server gespeichert werden. Bei den lokal authentifizierte Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden.

### LDap

Gibt an, dass alle zukünftigen Befehle REGISTER NODE und REGISTER ADMIN, die Sie ausgeben, LDAP als Parameterwert für die Standardauthentifizierung verwenden. LDAP-authentifizierte Kennwörter sind die Kennwörter, die auf einem LDAP-Verzeichnisserver gespeichert werden. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung beachtet werden.

## Beispiel: Den Wert für die Standardkennwortauthentifizierung auf LDAP setzen

Angaben, dass alle ausgegebenen Befehle REGISTER NODE oder REGISTER ADMIN Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren sollen.

```
set defaultauthentication ldap
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DEFAULTAUTHENTICATION

| Befehl           | Beschreibung   |
|------------------|--|
| SET LDAPPASSWORD | Legt das Kennwort für den LDAPUSER fest.   |
| SET LDAPUSER     | Definiert den Benutzer, der die Kennwörter und Administratoren auf dem LDAP-Verzeichnisserver überwacht. |
| SET LDAPUSER     | Definiert den Benutzer, der die Kennwörter und Administratoren auf dem LDAP-Verzeichnisserver überwacht. |
| REGISTER ADMIN   | Definiert einen neuen Administrator, ohne Administratorberechtigung zu erteilen.                         |
| REGISTER NODE    | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.                  |

## SET DEPLOYPKGMR (Implementierungspaketmanager aktivieren)

Verwenden Sie diesen Befehl, um den Implementierungspaketmanager zu aktivieren oder zu inaktivieren. Mit dieser Komponente werden Clientimplementierungspakete von der FTP-Site für die automatische Installation mithilfe des Operations Center heruntergeladen.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
.-ON--.  
>>-SET DEPLOYPKGMgr--+-OFF-+-----<<
```

## Parameter

### ON

Gibt an, dass der Implementierungspaketmanager die FTP-Site nach neuen Implementierungspaketen abfragt und neue Pakete herunterlädt, wenn sie verfügbar werden. Dies ist der Standardwert.

### OFF

Gibt an, dass der Implementierungspaketmanager die FTP-Site nicht abfragt und neue Pakete nicht herunterlädt. Wenn Sie den Implementierungspaketmanager inaktivieren, während Pakete heruntergeladen werden, werden die aktiven Downloadprozesse fortgesetzt, bis sie beendet sind.

## Beispiel: Den Implementierungspaketmanager inaktivieren



Den folgenden Befehl ausgeben, um den Implementierungspaketmanager zu inaktivieren:

```
set deploypkgmgr off
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DEPLOYPKGMR

| Befehl                | Beschreibung   |
|-----------------------|--|
| QUERY MONITORSETTINGS | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an. |
| SET DEPLOYREPOSITORY  | Gibt die Position an, an der Clientimplementierungspakete heruntergeladen werden.                |

## SET DEPLOYREPOSITORY (Downloadpfad für Clientimplementierungspakete definieren)

Verwenden Sie diesen Befehl, um die Position anzugeben, an der der automatisierte Implementierungsprozess die neuesten Clientimplementierungspakete herunterlädt. Die Implementierungspakete werden verwendet, um Aktualisierungen auf Clientsystemen zu installieren.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-SET DEPLOYREPOSITORY--Pfadname-----<<
```

### Parameter

Pfadname (Erforderlich)

Gibt den vollständig qualifizierten Pfad an, in dem Implementierungspakete heruntergeladen werden. Dieser Pfad gibt auch die Position an, an der der Server die Dateien speichert, die die Speicherdatenträger für die Clientimplementierungseinheitenklasse darstellen. Sie können den Pfadnamen entfernen, indem Sie den Befehl ohne Angabe eines Werts oder unter Angabe eines leeren Werts (") ausgeben. Wenn Sie keinen Pfadnamen angeben, werden vom Server keine Implementierungspakete heruntergeladen.

Wenn Sie die Position ändern, an der Aktualisierungspakete gespeichert werden, werden zuvor heruntergeladene Pakete automatisch gelöscht. Serverdatenträger werden gelöscht, wenn Daten bereinigt oder als verfallen gekennzeichnet werden. Wichtig: Löschen Sie nicht manuell Dateien mit der Dateinamenerweiterung .BFS. BFS-Dateien sind Datenträger, die vom Server verwaltet werden, und sie enthalten Archivierungsdaten, die automatisch als verfallen gekennzeichnet oder bereinigt werden.

### Beispiel: Einen Pfadnamen angeben

Geben Sie `/source/packages/` als Position an, an der Implementierungspakete heruntergeladen werden. Dieselbe Position wird für die Einheitenklasse `IBM_DEPLOY_CLIENT_IMPORT` verwendet, die für die Clientimplementierung verwendet wird.

```
set deployrepository /source/packages/
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DEPLOYREPOSITORY

| Befehl                | Beschreibung   |
|-----------------------|--|
| QUERY MONITORSETTINGS | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                     |
| SET DEPLOYMAXPKGS     | Gibt die maximale Anzahl Clientimplementierungspakete an, die heruntergeladen und auf dem Server gespeichert werden. |

## SET DEPLOYMAXPKGS (Maximale Anzahl Clientimplementierungspakete definieren, die gespeichert werden sollen)

Verwenden Sie diesen Befehl, um die maximale Anzahl installierbarer Clientimplementierungspakete anzugeben, die heruntergeladen und auf dem Server gespeichert werden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-SET DEPLOYMAXPkgs--Anzahl-----<<
```

### Parameter

Anzahl

Gibt die maximale Anzahl Implementierungspakete an, die im Implementierungsrepository für jede Produktversion gespeichert werden. Die Mindestanzahl der Pakete ist 1 und die maximale Anzahl ist 4. Wenn Sie die Anzahl verringern, werden ältere Versionen der Pakete entfernt, wenn die Pakete das nächste Mal aktualisiert werden. Die Aktualisierung der Pakete kann bis zu einem Tag dauern. Die Standardanzahl ist 4.

### Beispiel: Die maximale Anzahl Implementierungspakete angeben

Für die maximale Anzahl Implementierungspakete, die heruntergeladen und gespeichert werden, den Wert 3 angeben.

```
set deploymaxpkgs 3
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DEPLOYMAXPKGS

| Befehl  | Beschreibung   |
|---|--|
| QUERY MONITORSETTINGS   | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an. |
| SET DEPLOYREPOSITORY (Downloadpfad für Clientimplementierungspakete definieren) | Gibt die Position an, an der Clientimplementierungspakete heruntergeladen werden.                |

## SET DISSIMILARPOLICIES (Die Maßnahmen auf dem Zielreplikationsserver für die Verwaltung replizierter Daten aktivieren)

Verwenden Sie den Befehl SET DISSIMILARPOLICIES, um die Maßnahmen, die auf dem Zielreplikationsserver definiert sind, für die Verwaltung von replizierten Clientknotendaten zu aktivieren. Wenn Sie die Maßnahmen auf dem Zielreplikationsserver nicht verwenden, werden replizierte Clientknotendaten von Maßnahmen auf dem Quellenreplikationsserver verwaltet.

Stellen Sie sicher, dass IBM Spectrum Protect Version 7.1.1 oder höher auf dem Quellen- und Zielreplikationsserver installiert ist, bevor Sie diesen Befehl ausgeben. Geben Sie diesen Befehl auf dem Quellenreplikationsserver aus.

Bevor Sie die Maßnahmen verwenden, die auf einem Zielreplikationsserver definiert sind, müssen Sie den Befehl VALIDATE REPLPOLICY für diesen Zielreplikationsserver ausgeben. Dieser Befehl zeigt die Unterschiede zwischen den Maßnahmen für die Clientknoten auf dem Quellenreplikationsserver und den Maßnahmen auf dem Zielreplikationsserver an. Sie können die Maßnahmen auf dem Zielreplikationsserver ändern, bevor Sie diese Maßnahmen für die Verwaltung von replizierten Clientknotendaten aktivieren.

Um den Namen des Zielreplikationsservers abzurufen, für den Daten verwaltet werden sollen, und zu überprüfen, ob die Maßnahmen auf dem Zielreplikationsserver auf ON gesetzt sind, verwenden Sie den Befehl QUERY REPLSERVER. Bei der Installation wird dieser Wert auf OFF gesetzt.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set DISSIMILARPolicies--Zielservername--+-Off-+-----><
                                     .-Off-.
                                     +-Off-+
                                     '-ON--'
```

## Parameter

Zielservername (Erforderlich)

Gibt den Namen des Zielreplikationsservers an, für den die Maßnahmen aktiviert werden sollen.

ON

Gibt an, dass die replizierten Clientknotendaten von den Maßnahmen verwaltet werden, die auf dem Zielreplikationsserver definiert sind.

Off

Gibt an, dass die replizierten Clientknotendaten von den Maßnahmen verwaltet werden, die auf dem Quellenreplikationsserver definiert sind. Off ist der Standardwert.

## Beispiel: Die Maßnahmen auf einem Zielreplikationsserver verwenden

Um replizierte Clientknotendaten auf dem Zielreplikationsserver CVTCVS\_LXS\_SRV2 zu verwalten, geben Sie den folgenden Befehl auf dem Quellenreplikationsserver aus:

```
set dissimilarpolicies CVTCVS_LXS_SRV2 on
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DISSIMILARPOLICIES

| Befehl              | Beschreibung  |
|---------------------|---|
| QUERY REPLSERVER    | Zeigt Informationen zu Replikationsservern an.      |
| VALIDATE REPLPOLICY | Prüft die Maßnahmen auf dem Zielreplikationsserver. |

## SET DRMACTIVEDATASTGPOOL (Von DRM zu verwaltende Pools für aktive Daten angeben)

Mit diesem Befehl können Namen von Pools für aktive Daten angegeben werden, die nach einem Katastrophenfall wiederhergestellt werden sollen. IBM Spectrum Protect verwendet diese Namen, wenn der Befehl PREPARE, MOVE DRMEDIA oder QUERY DRMEDIA nicht den Parameter ACTIVEDATASTGPOOL enthält.

Standardmäßig sind Datenträger in Pools für aktive Daten nicht für die Verarbeitung durch Disaster Recovery Manager auswählbar. Um Datenträger im Pool für aktive Daten zu verarbeiten, müssen Sie den Befehl SET DRMACTIVEDATASTGPOOL ausgeben oder Sie müssen den Befehlszeilenparameter ACTIVEDATASTGPOOL im Befehl MOVE DRMEDIA, QUERY DRMEDIA oder PREPARE verwenden.

Mit dem Befehl QUERY DRMSTATUS können die aktuellen Einstellungen angezeigt werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set DRMACTIVEDatastgpool----->
      .,-----
      v |
>----Name_des_Pools_für_aktive_Daten+-----><
```

## Parameter

Name\_des\_Pools\_für\_aktive\_Daten (Erforderlich)

Gibt die Namen der Pools für aktive Daten an. Mehrere Namen sind ohne Leerzeichen durch Kommas voneinander zu trennen. Es können Platzhalterzeichen verwendet werden. Die angegebenen Namen überschreiben die vorherigen Einstellungen. Wird eine Nullzeichenfolge ("" ) eingegeben, werden alle aktuellen Namen entfernt, und es werden keine Datenträger im Pool für aktive Daten im Status MOUNTABLE verarbeitet, wenn sie nicht explizit als MOVE DRMEDIA-, QUERY DRMEDIA- oder PREPARE-Befehlsparameter eingegeben wurden.

## Beispiel: Einen auswählbaren Pool für aktive Daten definieren

ACTIVEDATAPOOL1 als auswählbaren Pool für aktive Daten definieren.

```
set drmactivedatapool activedatastgpool1
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMACTIVEDATASTGPOOL

| Befehl             | Beschreibung  |
|--------------------|---|
| MOVE DRMEDIA       | Versetzt DRM-Datenträger vor Ort und lagert sie aus.  |
| PREPARE            | Erstellt eine Wiederherstellungsplandatei.  |
| QUERY DRMEDIA      | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an. |
| QUERY DRMSTATUS    | Zeigt DRM-Systemparameter an.   |
| SET DRMCOPYSTGPOOL | Gibt an, dass Kopierspeicherpools von DRM verwaltet werden.                                   |
| SET DRMPRIMSTGPOOL | Gibt an, dass primäre Speicherpools von DRM verwaltet werden.                                 |

## SET DRMCHECKLABEL (Kennsatzprüfung angeben)

Mit diesem Befehl kann angegeben werden, ob IBM Spectrum Protect die Kennsätze von sequenziellen Datenträgern liest, die mit dem Befehl MOVE DRMEDIA entnommen wurden. Bei der Installation wird der Wert für DRMCHECKLABEL auf YES gesetzt.

Mit dem Befehl QUERY DRMSTATUS kann die aktuelle Einstellung überprüft werden.

  Dieser Befehl gilt nicht für Einheitentypen 349X.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
          .-Yes-.
>>-Set  DRMCHECKLabel-----><
          +-Yes-+
          '-No--'
```

## Parameter

Yes

Gibt an, dass IBM Spectrum Protect die Kennsätze sequenzieller Datenträgern liest, die mit dem Befehl MOVE DRMEDIA entnommen wurden.

No

Gibt an, dass IBM Spectrum Protect die Kennsätze sequenzieller Datenträger, die mit dem Befehl MOVE DRMEDIA entnommen wurden, nicht liest.

## Beispiel: Angeben, dass keine Kennsatzprüfung durchgeführt werden soll

Geben Sie an, dass keine Kennsatzprüfung ausgeführt wird.

```
set drmchecklabel no
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMCHECKLABEL

| Befehl          | Beschreibung   |
|-----------------|--|
| MOVE DRMEDIA    | Versetzt DRM-Datenträger vor Ort und lagert sie aus. |
| QUERY DRMSTATUS | Zeigt DRM-Systemparameter an.                        |

## SET DRMCMDFILENAME (Namen einer Datei angeben, die Befehle enthalten soll)

Mit diesem Befehl kann eine Datei angegeben werden, die die Befehle enthalten kann, die bei der Ausgabe der Befehle MOVE DRMEDIA und QUERY DRMEDIA erstellt werden. Wird der Befehl SET DRMCMDFILENAME nicht ausgegeben, generiert der Befehl MOVE DRMEDIA oder QUERY DRMEDIA einen Dateinamen.

Mit dem Befehl QUERY DRMSTATUS kann der aktuelle Name der Befehlsdatei angezeigt werden.

## Berechtigungsklasse


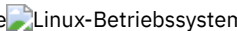
Für diesen Befehl ist die Systemberechtigung erforderlich.


## Syntax

```
>>-Set DRMCMDfilename--Dateiname-----<<
```

## Parameter

Dateiname (Erforderlich)

  Gibt einen vollständigen Pfadnamen für eine Datei an, die die von dem Befehl MOVE DRMEDIA oder QUERY DRMEDIA erstellten Befehle enthalten soll.

 Gibt einen vollständigen Pfadnamen für eine Datei an, die die von dem Befehl MOVE DRMEDIA oder QUERY DRMEDIA erstellten Befehle enthalten soll. Der Dateiname kann bis zu 259 Zeichen umfassen.

Achtung: Ist eine Datei mit demselben Namen bereits vorhanden, versucht der Befehl MOVE DRMEDIA oder QUERY DRMEDIA, die Datei zu verwenden. Die vorhandenen Daten werden dann überschrieben.

## Beispiel: Den Namen einer Datei angeben, die DRMEDIA-Befehle enthalten soll

  Den Dateinamen /adsm/drm/orm/exec.cmds angeben.

```
set drmcmdfilename /adsm/drm/orm/exec.cmds
```

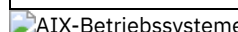
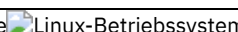
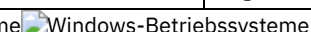
 Den Dateinamen c:\drm\orm\exec.cmd angeben.

```
set drmcmdfilename c:\drm\orm\exec.cmd
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMCMDFILENAME

| Befehl          | Beschreibung  |
|-----------------|---|
| MOVE DRMEDIA    | Versetzt DRM-Datenträger vor Ort und lagert sie aus.  |
| QUERY DRMEDIA   | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an. |
| QUERY DRMSTATUS | Zeigt DRM-Systemparameter an.   |

## SET DRMCOPYCONTAINERSTGPOOL (Containerkopierspeicherpools angeben, die von DRM-Befehlen verarbeitet werden sollen)

Verwenden Sie diesen Befehl, um die Containerkopierspeicherpools anzugeben, die vom Befehl MOVE DRMEDIA oder QUERY DRMEDIA verarbeitet werden sollen, wenn dieser Befehl nicht den Parameter COPYCONTAINERSTGPOOL enthält.

Standardmäßig werden Datenträger in Containerkopierspeicherpools von den Befehlen MOVE DRMEDIA und QUERY DRMEDIA nicht verarbeitet. Um die Datenträger zu verarbeiten, müssen Sie den Befehl SET DRMCOPYCONTAINERSTGPOOL ausgeben oder den Parameter COPYCONTAINERSTGPOOL im Befehl MOVE DRMEDIA oder QUERY DRMEDIA verwenden.

Tipp: Um die aktuellen Einstellungen anzuzeigen, verwenden Sie den Befehl QUERY DRMSTATUS.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
      .,-----.  
      v         |  
>>-Set DRMCOPYCONTAINERSTGPOOL---Poolname+-----><
```

### Parameter

Poolname (Erforderlich)

Gibt die Namen der Containerkopierspeicherpools an. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden. Die angegebenen Namen ersetzen die vorherigen Einstellungen. Wird eine Nullzeichenfolge ("" ) eingegeben, werden alle aktuellen Namen entfernt.

### Beispiel: Speicherpools angeben, die von den Befehlen MOVE DRMEDIA und QUERY DRMEDIA verarbeitet werden sollen

CONTCOPY1 und CONTCOPY2 als Containerkopierspeicherpools definieren, die verarbeitet werden sollen.

```
set drmcopycontainerstgpool contcopy1,contcopy2
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMCOPYCONTAINERSTGPOOL

| Befehl          | Beschreibung  |
|-----------------|---|
| MOVE DRMEDIA    | Versetzt DRM-Datenträger vor Ort und lagert sie aus.  |
| QUERY DRMEDIA   | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an. |
| QUERY DRMSTATUS | Zeigt DRM-Systemparameter an.   |

## SET DRMCOPYSTGPOOL (Von DRM zu verwaltende Kopierspeicherpools angeben)

Mit diesem Befehl können Namen von Kopierspeicherpools angegeben werden, die nach einem Unglück wiederhergestellt werden sollen. IBM Spectrum Protect verwendet diese Namen, wenn der Befehl PREPARE nicht den Parameter COPYSTGPOOL enthält.

Wenn der Befehl MOVE DRMEDIA oder QUERY DRMEDIA nicht den Parameter COPYSTGPOOL enthält, werden mit dem Befehl die Datenträger im Status MOUNTABLE verarbeitet, die sich in dem im Befehl SET DRMCOPYSTGPOOL angegebenen Kopierspeicherpool befinden. Bei der Installation sind alle Kopierspeicherpools für die DRM-Verarbeitung auswählbar.

Mit dem Befehl QUERY DRMSTATUS können die aktuellen Einstellungen angezeigt werden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
          .-----  
          v                                     |  
>>-Set DRMCOPYstgpool---Name_des_Kopienpools+-----<<
```

## Parameter

Name\_des\_Kopienpools (Erforderlich)

Gibt die Namen der Kopienspeicherpools an. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden. Die angegebenen Namen ersetzen die vorherigen Einstellungen. Wird eine Nullzeichenfolge ("" ) eingegeben, werden alle aktuellen Namen entfernt, und alle Kopienspeicherpools sind für die Verarbeitung auswählbar.

## Beispiel: Einen auswählbaren Kopienspeicherpool definieren

COPYSTGPOOL1 als auswählbaren Kopienspeicherpool definieren.

```
set drmcopystgpool copystgpool1
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMCOPYSTGPOOL

| Befehl             | Beschreibung  |
|--------------------|---|
| MOVE DRMEDIA       | Versetzt DRM-Datenträger vor Ort und lagert sie aus.  |
| PREPARE            | Erstellt eine Wiederherstellungsplandatei.  |
| QUERY DRMEDIA      | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an. |
| QUERY DRMSTATUS    | Zeigt DRM-Systemparameter an.   |
| SET DRMPRIMSTGPOOL | Gibt an, dass primäre Speicherpools von DRM verwaltet werden.                                 |

## SET DRMCOURIERNAME (Kuriernamen angeben)

Mit diesem Befehl kann der Name des Kuriers angegeben werden. Bei der Installation wird dieser Name auf COURIER gesetzt. Der Befehl MOVE DRMEDIA verwendet den Kuriernamen, um den Standort von Datenträgern anzugeben, die in den Status COURIER übergehen.

Mit dem Befehl QUERY DRMSTATUS kann der Kuriernamen abgefragt werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set DRMCOURiername--Kuriername-----<<
```

## Parameter

Kuriernamen (Erforderlich)

Gibt den Namen des Kuriers an. Der Name kann bis zu 255 Zeichen umfassen. Den Namen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

## Beispiel: Den Kuriernamen definieren

Den Namen des Kuriers als Joe's Courier Service definieren.

```
set drmcouriername "Joe's Courier Service"
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMCOURIERNAME

| Befehl          | Beschreibung  |
|-----------------|---|
| MOVE DRMEDIA    | Versetzt DRM-Datenträger vor Ort und lagert sie aus.  |
| QUERY DRMEDIA   | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an. |
| QUERY DRMSTATUS | Zeigt DRM-Systemparameter an.   |

## SET DRMDBBACKUPEXPIREDDAYS (Verfall für DB-Sicherungsserie angeben)

Mit diesem Befehl kann angegeben werden, wann eine Datenbanksicherungsserie für die Verfallsverarbeitung ausgewählt werden kann.

Der mit diesem Befehl definierte Wert gilt sowohl für eine Sicherungsserie mit Datenbankmomentaufnahmen als auch für eine Gesamt- und Teilsicherungsserie der Datenbank. Jede Art von Datenbanksicherungsserie kann für die Verfallsverarbeitung ausgewählt werden, wenn alle folgenden Bedingungen zutreffen:

- Das Alter des letzten Datenträgers der Serie überschreitet den mit dem Befehl SET DRMDBBACKUPEXPIREDDAYS definierten Verfallswert und den für den Parameter DELgraceperiod im Befehl DEFINE SERVER angegebenen Wert. Der Parameter DELgraceperiod gilt nur für ferne Datenbanksicherungen. Der Standardwert für den Parameter DELgraceperiod sind 5 Tage. Wenn Sie beispielsweise den Wert für den Befehl SET DRMDBBACKUPEXPIREDDAYS auf 7 Tage und den Wert für den Parameter DELgraceperiod auf 6 Tage setzen, verfällt die Serie ferner Datenbanksicherungen erst nach 13 Tagen.
- Bei Datenträgern, die keine virtuellen Datenträger sind, befinden sich alle Datenträger in der Serie im Status VAULT.
- Der Datenträger ist nicht Teil der letzten Datenbanksicherungsserie.

Hinweis: Die letzte Sicherungsserie jeder Art wird nicht gelöscht.

Weitere Informationen zum Verfall von Datenbanksicherungsdatenträgern, die keine virtuellen Datenträger sind, befinden sich in der Beschreibung des Befehls MOVE DRMEDIA. Weitere Informationen zum Verfall von Datenbanksicherungsdatenträgern, die virtuelle Datenträger sind, befinden sich in der Beschreibung des Befehls EXPIRE INVENTORY.

Mit dem Befehl QUERY DRMSTATUS kann die angegebene Anzahl der Tage angezeigt werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set DRMDBBackupexpiredays--Tage-----<<
```

## Parameter

Tage (Erforderlich)

Gibt die Anzahl Tage an, die seit der Erstellung einer Datenbanksicherungsserie vergangen sein müssen, bevor sie für die Verfallsverarbeitung ausgewählt werden kann. Die Anzahl der Tage muss mit dem Verzögerungszeitraum für die Wiederverwendung von Datenträgern für Kopierspeicherpools übereinstimmen, die von Disaster Recovery Manager verwaltet werden. Geben Sie einen ganzzahligen Wert zwischen 0 und 9999 an.

## Beispiel: Den Verfall der Datenbanksicherungsserie definieren

Der Verfallswert für die Datenbanksicherungsserie soll auf 60 gesetzt werden.

```
set drmdbbackupexpiredays 60
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMDBBACKUPEXPIREDDAYS

| Befehl | Beschreibung |
|--------|--------------|
|--------|--------------|



| Befehl             | Beschreibung  |
|--------------------|---|
| DSMSERV RESTORE DB | Schreibt eine IBM Spectrum Protect-Datenbank zurück.  |
| MOVE DRMEDIA       | Versetzt DRM-Datenträger vor Ort und lagert sie aus.  |
| QUERY DRMEDIA      | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an. |
| QUERY DRMSTATUS    | Zeigt DRM-Systemparameter an.   |
| QUERY VOLHISTORY   | Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.            |
| DEFINE SERVER      | Definiert einen Server für die Übertragung zwischen Servern.                                  |

## SET DRMFILEPROCESS (Dateiverarbeitung angeben)

Mit diesem Befehl kann angegeben werden, ob der Befehl MOVE DRMEDIA oder QUERY DRMEDIA Datenbanksicherungsdatenträger und Kopierspeicherpooldatenträger verarbeiten soll, die der Einheitenklasse FILE zugeordnet sind. Bei der Installation wird der Wert auf NO gesetzt. Mit dem Befehl QUERY DRMSTATUS kann die aktuelle Einstellung angezeigt werden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```

>>-Set DRMFILEProcess--+-No--
                        +-No--+
                        '-Yes-'

```

### Parameter

No

Gibt an, dass die Befehle MOVE DRMEDIA und QUERY DRMEDIA keine Datenbanksicherungs- und Kopierspeicherpooldatenträger verarbeiten, die der Einheitenklasse FILE zugeordnet sind. Dies ist der Standardwert.

Yes

Gibt an, dass die Befehle MOVE DRMEDIA und QUERY DRMEDIA Datenbanksicherungs- und Kopierspeicherpooldatenträger verarbeiten, die der Einheitenklasse FILE zugeordnet sind.

### Beispiel: Angeben, dass die DRMEDIA-Befehle keine Einheitenklassen des Typs FILE einschließen

Der Dateiverarbeitungswert soll auf 'No' gesetzt werden.

```
set drmfileprocess no
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMFILEPROCESS


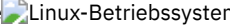
| Befehl          | Beschreibung  |
|-----------------|---|
| MOVE DRMEDIA    | Versetzt DRM-Datenträger vor Ort und lagert sie aus.  |
| QUERY DRMEDIA   | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an. |
| QUERY DRMSTATUS | Zeigt DRM-Systemparameter an.   |

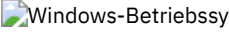
## SET DRMINSTRPREFIX (Präfix für Wiederherstellungsanweisungsdateinamen angeben)

Mit diesem Befehl kann ein Präfix für den Namen der Wiederherstellungsanweisungsdatei angegeben werden. Wenn dieser Befehl ausgegeben wird, verwendet IBM Spectrum Protect das angegebene Präfix, wenn der Befehl PREPARE ohne den Parameter

INSTRPREFIX ausgegeben wird.

Mit dem Befehl QUERY DRMSTATUS kann der aktuelle Wert für das Präfix angezeigt werden.

  Das Präfix ist das aktuelle Arbeitsverzeichnis des IBM Spectrum Protect-Servers.

 Wird kein Präfix definiert, wird das Präfix auf das Verzeichnis gesetzt, das dieses Exemplar des Servers darstellt (normalerweise das Verzeichnis, aus dem der Server ursprünglich installiert wurde).

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.





## Syntax

---

```
>>-Set DRMINSTRPrefix--Präfix-----<<
```

## Parameter

---

  Präfix (Erforderlich)  
 

Gibt ein Pfadnamenpräfix für die Dateien an, die die Wiederherstellungsanweisungen enthalten. Bei der Verarbeitung des Befehls PREPARE hängt IBM Spectrum Protect den Namen der entsprechenden Zeilengruppe für die Wiederherstellungsplandatei an, um die Datei zu lokalisieren. Die maximale Länge beträgt 250 Zeichen.

Das Präfix kann Folgendes sein:

- **Verzeichnispfad:** Das Präfix mit einem Schrägstrich (/) beenden. Beispiel:

```
/admsrv/recinstr/
```

Für die Datei RECOVERY.INSTRUCTIONS.GENERAL würde der daraus resultierende Dateiname wie folgt lauten:

```
/admsrv/recinstr/RECOVERY.INSTRUCTIONS.GENERAL
```

- **Verzeichnispfad gefolgt von einer Zeichenfolge:** IBM Spectrum Protect behandelt die Zeichenfolge als Teil des Dateinamens. Beispiel:

```
/admsrv/recinstr/accounts
```

Für die Datei RECOVERY.INSTRUCTIONS.GENERAL würde der daraus resultierende Dateiname wie folgt lauten:

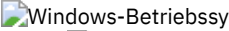
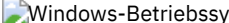
```
/admsrv/recinstr/accounts.RECOVERY.INSTRUCTIONS.GENERAL
```

- **Nur Zeichenfolge:** IBM Spectrum Protect gibt den Verzeichnispfad an und hängt den entsprechenden Namen der Zeilengruppe für die Wiederherstellungsplandatei an.
  - IBM Spectrum Protect verwendet den Namen des aktuellen Arbeitsverzeichnisses. Das aktuelle Arbeitsverzeichnis lautet beispielsweise /opt/tivoli/tsm/server/bin. Sie geben Folgendes an:

```
shipping
```

Für die Datei RECOVERY.INSTRUCTIONS.GENERAL würde der daraus resultierende Dateiname wie folgt aussehen:

```
/opt/tivoli/tsm/server/bin/shipping.RECOVERY.INSTRUCTIONS.GENERAL
```

 Präfix (Erforderlich)  


Gibt ein Pfadnamenpräfix für die Dateien an, die die Wiederherstellungsanweisungen enthalten. Bei der Verarbeitung des Befehls PREPARE hängt IBM Spectrum Protect den Namen der entsprechenden Zeilengruppe für die Wiederherstellungsplandatei an, um die Datei zu lokalisieren. Die maximale Länge beträgt 200 Zeichen.

Das Präfix kann Folgendes sein:

- **Verzeichnispfad:** Das Präfix mit einem umgekehrten Schrägstrich (\) beenden. Beispiel:

```
c:\admsrv\recinstr\
```

Für die Datei RECOVERY.INSTRUCTIONS.GENERAL würde der daraus resultierende Dateiname wie folgt lauten:

```
c:\admsrv\recinstr\RECOVERY.INSTRUCTIONS.GENERAL
```

- **Verzeichnispfad gefolgt von einer Zeichenfolge:** IBM Spectrum Protect behandelt die Zeichenfolge als Teil des Dateinamens. Beispiel:

```
c:\admsrv\recinstr\accounts
```

Für die Datei RECOVERY.INSTRUCTIONS.GENERAL würde der daraus resultierende Dateiname wie folgt lauten:

```
c:\admsrv\recinstr\accounts.RECOVERY.INSTRUCTIONS.GENERAL
```


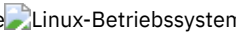
- **Nur Zeichenfolge:** IBM Spectrum Protect gibt den Verzeichnispfad an und hängt den entsprechenden Namen der Zeilengruppe für die Wiederherstellungsplandatei an. Der Verzeichnispfad ist das Verzeichnis, das dieses Exemplar des IBM Spectrum Protect-Servers darstellt (normalerweise das ursprüngliche Installationsverzeichnis des IBM Spectrum Protect-Servers). Beispielsweise lautet das Verzeichnis, das dieses Exemplar des Servers darstellt, c:\Programme\Tivoli\TSM;\server2, und das folgende Präfix wird angegeben:

```
shipping
```


Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

```
c:\Programme\Tivoli\TSM;\server2\shipping.19971115.051421
```

## Beispiel: Das Präfix für den Wiederherstellungsplan angeben

  Angeben, dass die Wiederherstellungsplananweisungen aus dem Verzeichnis /drmpln/primesrv gelesen werden sollen.

```
set drminstrprefix /drmpln/primesrv/
```

 Angeben, dass die Wiederherstellungsplananweisungen aus dem Verzeichnis c:\win32app\ibm\adsm\server2\ gelesen werden sollen.

```
set drminstrprefix c:\win32app\ibm\adsm\server2\
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMINSTRPREFIX

| Befehl          | Beschreibung                               |
|-----------------|--|
| PREPARE         | Erstellt eine Wiederherstellungsplandatei. |
| QUERY DRMSTATUS | Zeigt DRM-Systemparameter an.              |

## SET DRMNOTMOUNTABLENAME (Nicht mountfähigen Standort angeben)

Mit diesem Befehl kann der Name des Standorts vor Ort zum Speichern der Datenträger angegeben werden. Bei der Installation wird der Name auf NOTMOUNTABLE gesetzt. Mit dem Befehl QUERY DRMSTATUS kann der Standortname angezeigt werden.

Der Standortname wird vom Befehl MOVE DRMEDIA verwendet, um den Standort von Datenträgern anzugeben, die in den Status NOTMOUNTABLE übergehen.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set DRMNOTMOUNTABLENAME--Standort-----<<
```

## Parameter

Standort (Erforderlich)

Gibt den Namen des Standorts vor Ort zum Speichern der Datenträger an. Der Name kann bis zu 255 Zeichen umfassen. Den Namen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

## Beispiel: Den Namen des Standorts vor Ort angeben

Den Namen des Standorts auf room 123/31 setzen.

```
set drmnotmountablename "room 123/31"
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMNOTMOUNTABLERNAME

| Befehl          | Beschreibung  |
|-----------------|---|
| MOVE DRMEDIA    | Versetzt DRM-Datenträger vor Ort und lagert sie aus.  |
| QUERY DRMEDIA   | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an. |
| QUERY DRMSTATUS | Zeigt DRM-Systemparameter an.   |

## SET DRMPLANPREFIX (Präfix für Wiederherstellungsplandateinamen angeben)

Mit diesem Befehl kann ein Präfix für einen Wiederherstellungsplandateinamen angegeben werden.

Wenn dieser Befehl ausgegeben wird, verwendet IBM Spectrum Protect das angegebene Präfix, wenn der Befehl PREPARE nicht den Parameter PLANPREFIX enthält.

Mit dem Befehl QUERY DRMSTATUS kann der aktuelle Wert für das Wiederherstellungsplanpräfix angezeigt werden.

## Berechtigungsklasse


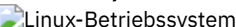
Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set DRMPLANPrefix--Präfix-----<<
```

## Parameter

  Präfix (Erforderlich)

  Gibt das Präfix für den Namen einer Wiederherstellungsplandatei an. Die maximale Länge des Präfix beträgt 250 Zeichen. Wird eine Nullzeichenfolge ("" ) eingegeben, wird das aktuelle Präfix entfernt, und der Server verwendet den Algorithmus, der im Parameter PLANPREFIX im Befehl PREPARE beschrieben ist.

Für das Präfix kann folgendes angegeben werden:

- **Ein Verzeichnispfad gefolgt von einem Schrägstrich (/):** IBM Spectrum Protect hängt an das Präfix das Datum und die Uhrzeit im Format `jjjjmmtt.hhmmss` an. Beispielsweise wird SET DRMPLANPREFIX auf folgenden Wert gesetzt:

```
/admsrv/recplans/
```

Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

```
/admsrv/recplans/19971115.051421
```

- **Ein Verzeichnispfad gefolgt von einer Zeichenfolge:** IBM Spectrum Protect verwendet die Zeichenfolge als Teil des Dateinamens. IBM Spectrum Protect hängt an das Präfix das Datum und die Uhrzeit im Format `.jjjjmmtt.hhmmss` an (den Punkt am Anfang beachten). Beispielsweise wird SET DRMPLANPREFIX auf folgenden Wert gesetzt:

```
/admsrv/recplans/accounting
```

Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

```
/admsrv/recplans/accounting.19971115.051421
```

- **Eine Zeichenfolge, der kein Verzeichnispfad vorausgeht:** IBM Spectrum Protect hängt an das Präfix das Datum und die Uhrzeit im Format `.jjjjmmtt.hhmmss` an (den Punkt am Anfang beachten). IBM Spectrum Protect bestimmt den Verzeichnispfad wie folgt:


- IBM Spectrum Protect verwendet den Verzeichnispfadnamen des aktuellen Arbeitsverzeichnisses des IBM Spectrum Protect-Servers. Beispielsweise lautet das aktuelle IBM Spectrum Protect-Arbeitsverzeichnis `/opt/tivoli/tsm/server/bin`. Der Befehl `SET DRMPLANPREFIX` ist auf folgenden Wert gesetzt:

```
shipping
```

Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

```
/opt/tivoli/tsm/server/bin/shipping.19971115.051421
```

#### Windows-BetriebssystemePräfix (Erforderlich)

 Windows-BetriebssystemeGibt ein Präfix für den Pfadnamen an, das zum Generieren des Wiederherstellungsplandateinamens verwendet wird. Das Präfix kann bis zu 200 Zeichen umfassen. IBM Spectrum Protect verwendet das Präfix, wenn der Befehl `PREPARE` ohne den Parameter `PLANPREFIX` ausgegeben wird. IBM Spectrum Protect erstellt einen eindeutigen Wiederherstellungsplandateinamen, indem an das Präfix das Datum und die Uhrzeit im Format `jjjjmmtt.hhmmss` angehängt wird (zum Beispiel `19951115.051421`). Wenn Sie eine Nullzeichenfolge ("" ) eingeben, wird das aktuelle Präfix entfernt und der Server verwendet den Algorithmus, der im Parameter `PLANPREFIX` im Befehl `PREPARE` beschrieben ist. Für das Präfix kann folgendes angegeben werden:

1. Ein Verzeichnispfad
2. Ein Verzeichnispfad, gefolgt von einer Zeichenfolge
3. Eine Zeichenfolge

Nachfolgend sind die Regeln für die Angabe von möglichen Präfixen beschrieben:

1. Soll ein Verzeichnispfad für das Präfix angegeben werden, muss das Präfix mit einem umgekehrten Schrägstrich (`\`) beendet werden. IBM Spectrum Protect hängt an das Präfix das Datum und die Uhrzeit im Format `jjjjmmtt.hhmmss` an. Beispielsweise ist `SET DRMPLANPREFIX` auf den folgenden Wert gesetzt:

```
c:\admsrv\recplans\
```

Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

```
c:\admsrv\recplans\19951115.051421
```

Wichtig: Wird der Befehl `SET DRMPLANPREFIX` von einem Befehlszeilenclient ausgegeben und ist das letzte Zeichen in der Befehlszeile ein umgekehrter Schrägstrich, interpretiert IBM Spectrum Protect das Zeichen als Fortsetzungszeichen. Um dies zu vermeiden, das Präfix in Anführungszeichen einschließen. Beispiel: `"c:\admsrv\recplans\"`

2. Ist das Präfix ein Verzeichnispfad gefolgt von einer Zeichenfolge, verwendet IBM Spectrum Protect die Zeichenfolge als Teil des Dateinamens. IBM Spectrum Protect hängt an das Präfix das Datum und die Uhrzeit im Format `.jjjjmmtt.hhmmss` an (den Punkt am Anfang beachten). Beispielsweise ist `SET DRMPLANPREFIX` auf den folgenden Wert gesetzt:

```
c:\admsrv\recplans\accounting
```

Der hierdurch erstellte Name der Wiederherstellungsplandatei würde wie folgt lauten:

```
c:\admsrv\recplans\accounting.19951115.051421
```

3. Ist das Präfix eine Zeichenfolge, der kein Verzeichnispfad vorausgeht, hängt IBM Spectrum Protect an das Präfix das Datum und die Uhrzeit im Format `.jjjjmmtt.hhmmss` an (den Punkt am Anfang beachten). Der Verzeichnispfad, der von IBM Spectrum Protect verwendet wird, ist der Verzeichnispfad, der dieses Exemplar des IBM Spectrum Protect-Servers darstellt (normalerweise das Verzeichnis, aus dem der IBM Spectrum Protect-Server ursprünglich installiert wurde). Beispielsweise lautet das Verzeichnis, das dieses Exemplar des Servers darstellt, `c:\Programme\Tivoli\TSM;\server2`, und das Präfix wird auf folgenden Wert gesetzt:




```
shipping
```



Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

```
c:\Programme\Tivoli\TSM;\server2\shipping.19951115.051421
```

## Beispiel: Ein Präfix für Wiederherstellungsplandateinamen angeben

Ein Präfix angeben, so dass die generierten Wiederherstellungsplandateien in dem folgenden Verzeichnis gespeichert werden:

-  AIX-Betriebssysteme  Linux-Betriebssysteme/drmlan/primsrv
-  Windows-Betriebssystemec:\drmtest\prepare\

Den folgenden Befehl ausgeben:  AIX-Betriebssysteme  Linux-Betriebssysteme

```
set drmlanprefix /drmlan/primsrv/
```

```
set drmplanprefix c:\drmtest\prepare\
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für SET DRMPLANPREFIX

| Befehl          | Beschreibung                               |
|-----------------|--|
| PREPARE         | Erstellt eine Wiederherstellungsplandatei. |
| QUERY DRMSTATUS | Zeigt DRM-Systemparameter an.              |

## SET DRMPLANVPOSTFIX (Namen für Ersatzdatenträger angeben)

---

Mit diesem Befehl kann das Zeichen angegeben werden, das an Ersatzdatenträgernamen in der Wiederherstellungsplandatei angehängt werden soll. Das Zeichen kann Ihnen beim Suchen oder Generieren von Ersatzdatenträgernamen helfen, wenn Sie die Wiederherstellungsplandatei verwenden.

Bei der Installation wird das Zeichen auf @ gesetzt. IBM Spectrum Protect generiert Ersatznamen für Datenträger im primären Speicherpool, die mit dem Befehl DEFINE VOLUME hinzugefügt wurden. Das angehängte Zeichen verwenden, um

- Ersatzdatenträgernamen in den Zeilengruppen des Wiederherstellungsplans zu suchen, so daß die Namen zum Zeitpunkt der Wiederherstellung geändert werden können. Beispielsweise sind unter Umständen die Namen der verfügbaren Banddatenträger am Wiederherstellungsort nicht bekannt.
- Ersatzdatenträgernamen zu generieren. Es wird eine Namenskonvention benötigt, die sich auf alle Einheitentypen in den primären Speicherpools anwenden läßt. Folgendes beachten:
  - Die generierte Länge des Ersatzdatenträgernamens
  - Welche Zeichen dürfen für den Namen von Ersatzdatenträgern verwendet werden?
  - Wie ist bei Konflikten mit bestehenden Datenträgernamen vorzugehen?
  - Ein Ersatzdatenträgername darf nicht mit dem Namen eines zerstörten, vorhandenen oder neuen Datenträgers übereinstimmen.

Mit dem Befehl QUERY DRMSTATUS kann das Zeichen angezeigt werden, das an das Ende der Ersatzdatenträgernamen hinzugefügt wurde.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---


```
>>-Set DRMPLANVpostfix--Zeichen-----<<
```


## Parameter

---

Zeichen (Erforderlich)

Gibt das Zeichen an, das an die Ersatzdatenträgernamen in der Wiederherstellungsplandatei angehängt werden soll. Ein alphanumerisches Zeichen oder Sonderzeichen angeben.

 **Achtung:** Ein Sonderzeichen kann zu unvorhersehbaren Ergebnissen in der AIX-Shell oder Befehlszeilenumgebung führen.

 **Achtung:** Ein Sonderzeichen kann zu unvorhersehbaren Ergebnissen in der Windows-Stapel-/Befehlszeilenumgebung führen.

## Beispiel: Das angehängte Zeichen für Ersatzdatenträgernamen angeben

---

Für das Zeichen, das an die Ersatzdatenträgernamen angehängt wird, soll R definiert werden.

```
set drmplanvpostfix R
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für SET DRMPLANVPOSTFIX

| Befehl          | Beschreibung                               |
|-----------------|--|
| PREPARE         | Erstellt eine Wiederherstellungsplandatei. |
| QUERY DRMSTATUS | Zeigt DRM-Systemparameter an.              |

## SET DRMPRIMSTGPOOL (Von DRM zu verwaltende primäre Speicherpools angeben)

Mit diesem Befehl können die Namen von primären Speicherpools angegeben werden, die wiederhergestellt werden sollen. Enthält der Befehl PREPARE nicht den Parameter PRIMSTGPOOL, verarbeitet DRM die in diesem Befehl angegebenen Namen.

Mit dem Befehl QUERY DRMSTATUS können die aktuellen Einstellungen angezeigt werden. Bei der Installation sind alle für den Server definierten primären Speicherpools für die DRM-Verarbeitung auswählbar.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```

      .-----
      v                                     |
>>-Set DRMPRIMstgpool----Name_des_primären_Pools-+-----<<

```

### Parameter

Name\_des\_primären\_Pools (Erforderlich)

Gibt die Namen der primären Speicherpools an, die wiederhergestellt werden sollen. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Die angegebenen Namen ersetzen die vorherigen Einstellungen. Wird eine Nullzeichenfolge ("" ) eingegeben, werden alle aktuellen Namen entfernt, und alle primären Speicherpools sind für die DRM-Verarbeitung auswählbar.

### Beispiel: Einen primären Speicherpool definieren, der von DRM verwaltet werden soll

Den primären Speicherpool, der von DRM verwaltet werden soll, auf PRIMSTGPOOL1 setzen.

```
set drmprimstgpool primstgpool1
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMPRIMSTGPOOL

| Befehl             | Beschreibung  |
|--------------------|---|
| PREPARE            | Erstellt eine Wiederherstellungsplandatei.                  |
| QUERY DRMSTATUS    | Zeigt DRM-Systemparameter an.                               |
| SET DRMCOPYSTGPOOL | Gibt an, dass Kopierspeicherpools von DRM verwaltet werden. |

## SET DRMRPFEXPIREDAYS (Kriterien für Verfall von Wiederherstellungsplandateien definieren)

Mit diesem Befehl kann angegeben werden, wann Wiederherstellungsplandateien für die Verfallsverarbeitung ausgewählt werden können. Dieser Befehl und die Verfallsverarbeitung gelten nur für Wiederherstellungsplandateien, die mit dem Parameter DEVCLASS erstellt wurden, der im Befehl PREPARE angegeben wurde (d. h. virtuelle Datenträger des Typs RPFIL und RPSNAPSHOT). Mit der Verfallsverarbeitung auf dem Quellenserver werden Plandateien, die auf dem Zielservers gespeichert sind, als verfallen gekennzeichnet. Lokal erstellte Wiederherstellungsplandateien verfallen nicht.

Eine RPFIL-Datei ist einer Gesamt- und Teilsicherungsserie der Datenbank zugeordnet. Eine RPSNAPSHOT-Datei ist einer Sicherungsserie mit Datenbankmomentaufnahmen zugeordnet.

Achtung: Die neuesten RPFIL- und RPFSSNAPSHOT-Dateien werden nie gelöscht.  
Eine Wiederherstellungsplandatei kann für die Verfallsverarbeitung ausgewählt werden, wenn die beiden folgenden Bedingungen zutreffen:

- Die letzte Wiederherstellungsplandatei der Serie überschreitet den im Befehl SET DRMRPFEXPIREDDAYS angegebenen Verfallswert und den für den Parameter DELgraceperiod im Befehl DEFINE SERVER angegebenen Wert. Der Standardwert für den Parameter DELgraceperiod sind 5 Tage. Wenn Sie beispielsweise den Wert für den Befehl SET DRMRPFEXPIREDDAYS auf 80 Tage und den Wert für den Parameter DELgraceperiod auf 6 Tage setzen, verfällt die Wiederherstellungsplandatei erst nach 86 Tagen.
- Die letzte Wiederherstellungsplandatei ist nicht der neuesten Datenbanksicherungsserie zugeordnet.

Weitere Informationen zur Verfallsverarbeitung befinden sich in der Beschreibung des Befehls EXPIRE INVENTORY.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set DRMRPFEXpiredays--Tage-----<<
```

## Parameter

Tage (Erforderlich)

Gibt die Anzahl Tage an, die verstreichen müssen, bevor eine Wiederherstellungsplandatei verfällt. Sie können eine Zahl von 0 bis 9999 angeben. Bei der Installation wird dieser Wert auf 60 gesetzt.

## Beispiel: Den Verfall des Wiederherstellungsplans definieren

Der Verfallswert für die Wiederherstellungsplandatei soll auf 30 gesetzt werden.

```
set drmrpfexpiredays 30
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMRPFEXPIREDDAYS

| Befehl                     | Beschreibung   |
|----------------------------|--|
| PREPARE                    | Erstellt eine Wiederherstellungsplandatei.   |
| QUERY DRMSTATUS            | Zeigt DRM-Systemparameter an.  |
| QUERY RPFCONTENT           | Zeigt den Inhalt einer Wiederherstellungsplandatei an.                             |
| QUERY RPFIL                | Zeigt Informationen über Wiederherstellungsplandateien an.                         |
| QUERY VOLHISTORY           | Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden. |
| SET DRMDBBACKUPEXPIREDDAYS | Gibt die Kriterien für den Verfall von Datenbanksicherungsserien an.               |
| DEFINE SERVER              | Definiert einen Server für die Übertragung zwischen Servern.                       |

## SET DRMVaultNAME (Aufbewahrungsort angeben)

Mit diesem Befehl kann der Name des Aufbewahrungsorts angegeben werden. Bei der Installation wird der Name auf VAULT gesetzt. Mit dem Befehl QUERY DRMSTATUS kann der Name des Aufbewahrungsorts angezeigt werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-SET DRMVaultname--Name_des_Aufbewahrungsorts-----<<
```



## Parameter

---

Name\_des\_Aufbewahrungsorts (Erforderlich)

Gibt den Namen des Aufbewahrungsorts an. Der Name kann bis zu 255 Zeichen umfassen. Den Namen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

## Beispiel: Den Namen eines Aufbewahrungsorts angeben

---

ironmountain als Namen des Aufbewahrungsorts angeben.

```
set drmvaultname ironmountain
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für SET DRMVAULTNAME

| Befehl          | Beschreibung  |
|-----------------|---|
| MOVE DRMEDIA    | Versetzt DRM-Datenträger vor Ort und lagert sie aus.  |
| QUERY DRMEDIA   | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an. |
| QUERY DRMSTATUS | Zeigt DRM-Systemparameter an.   |

## SET EVENTRETENTION (Aufbewahrungszeitraum für Ereignissätze definieren)

---

Mit diesem Befehl kann der Aufbewahrungszeitraum für Ereignissätze in der Server-Datenbank definiert werden, mit dem abgeschlossene Zeitpläne überwacht werden können. Ein Ereignissatz wird erstellt, wenn die Verarbeitung eines geplanten Befehls gestartet wird oder fehlschlägt.

Der Aufbewahrungszeitraum für Ereignisdaten kann so angepaßt werden, dass unzureichende oder veraltete Daten vermieden werden. Der Server entfernt die Ereignissätze automatisch aus der Datenbank, wenn das Ende des Aufbewahrungszeitraums erreicht und das Startfenster für das Ereignis abgelaufen ist.

Mit dem Befehl QUERY EVENT können Informationen zu geplanten und abgeschlossenen Ereignissen angezeigt werden.

Mit dem Befehl DELETE EVENT können Ereignissätze gelöscht werden, und zwar unabhängig davon, ob der Aufbewahrungszeitraum abgelaufen ist.

Der Befehl QUERY STATUS kann ausgegeben werden, um den Wert für den Aufbewahrungszeitraum anzuzeigen. Bei der Installation wird dieser Wert auf 10 Tage gesetzt.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-Set EVentretention--Tage-----<<
```

## Parameter

---

Tage (Erforderlich)

Die Anzahl der Tage, die Ereignissätze in der Datenbank aufbewahrt werden. Zulässige Werte sind ganze Zahlen von 0 bis 9999.

Der Wert 0 gibt an, dass nur Ereignissätze für den aktuellen Tag aufbewahrt werden.

## Beispiel: Den Aufbewahrungszeitraum für Ereignissätze definieren

---

Den Aufbewahrungszeitraum auf 15 Tage setzen.

```
set eventretention 15
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET EVENTRETENTION

| Befehl       | Beschreibung   |
|--------------|--|
| DELETE EVENT | Löscht Ereignissätze, die vor einem bestimmten Zeitpunkt erstellt wurden.  |
| QUERY EVENT  | Zeigt Informationen über geplante und abgeschlossene Ereignisse für ausgewählte Clients an.                          |
| QUERY STATUS | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## SET FAILOVERHLADDRESS (Adresse höherer Ebene für Übernahme definieren)

Verwenden Sie diesen Befehl, um die IP-Adresse anzugeben, die ein Client während der Übernahme (Failover) für die Herstellung der Verbindung zu diesem Server als sekundärer Replikationsserver verwendet, wenn die Adresse von der IP-Adresse abweicht, die für den Replikationsprozess angegeben ist.

Sie müssen die Adresse des Servers angeben, die verwendet wird, wenn die Adresse der höheren Ebene abweicht. Dieser Befehl ist nur erforderlich, wenn Sie separate dedizierte Netze für die Übertragung zwischen Servern und den Clientzugriff verwenden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-SET FAILOVERHladdress--Adresse der höheren Ebene-----<<
```

### Parameter

Adresse der höheren Ebene (Erforderlich)

Gibt die Adresse der höheren Ebene eines Servers als numerischen Namen in Schreibweise mit Trennzeichen oder als Hostnamen für die Verwendung während der Übernahme an. Wenn Sie einen Hostnamen angeben, muss ein Server verfügbar sein, der den Namen in das Format in Schreibweise mit Trennzeichen auflösen kann.

Um die IP-Übernahmeadresse zu entfernen, geben Sie den Befehl ohne Angabe eines Werts aus.

### Beispiel: Adresse der höheren Ebene für die Übernahme definieren

Der Name der Adresse der höheren Ebene, der für Übernahmeoperationen auf diesem Server definiert werden soll.

```
set failoverhladdress server1
```

### Beispiel: Adresse der höheren Ebene entfernen

Um eine Adresse der höheren Ebene für einen Übernahmeserver zu entfernen, geben Sie den folgenden Befehl aus:

```
set failoverhladdress
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY REPLSERVER

| Befehl   | Beschreibung                                   |
|--|--|
| QUERY REPLSERVER (Replikationsserver abfragen)   | Zeigt Informationen zu Replikationsservern an. |
| REMOVE REPLSERVER (Replikationsserver entfernen) | Entfernt einen Server aus der Replikation.     |

## SET INVALIDPWLIMIT (Anzahl der ungültigen Anmeldeversuche definieren)

Mit diesem Befehl kann die Anzahl der zulässigen ungültigen Anmeldeversuche angegeben werden, bevor ein Knoten gesperrt wird.

Der Befehl SET INVALIDPWLIMIT gilt auch für LDAP-Verzeichnisse, die komplexe Knotenkennwörter speichern. LDAP-Verzeichnisse können die Anzahl der Anmeldeversuche mit ungültigen Kennwörtern unabhängig vom IBM Spectrum Protect-Server begrenzen. Möglicherweise soll der LDAP-Verzeichnisse nicht für ungültige Anmeldeversuche für den IBM Spectrum Protect-Namensbereich konfiguriert werden, wenn Sie den Befehl SET INVALIDPWLIMIT verwenden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-Set--INVALIDPwlimit--Anzahl-----<<
```

### Parameter

Anzahl (Erforderlich)

Gibt an, wie viele ungültige Anmeldeversuche zulässig sind, bevor ein Knoten gesperrt wird.

Zulässige Werte sind ganze Zahlen von 0 bis 9999. Der Wert 0 bedeutet, dass nicht geprüft wird, ob ungültige Anmeldeversuche vorliegen. Der Wert 1 bedeutet, dass der Knoten vom Server gesperrt wird, wenn ein Benutzer einmal ein ungültiges Kennwort eingibt. Der Standardwert ist 0.

Wichtig: Wenn Ihr Kennwort mit einem LDAP-Verzeichnisse authentifiziert wird, kann es vom LDAP-Server und vom IBM Spectrum Protect-Server verwaltet werden. Nicht alle IBM Spectrum Protect-Serverbefehle betreffen Kennwörter, die mit einem LDAP-Server authentifiziert werden. Beispielsweise haben die Befehle SET PASSEXP und RESET PASSEXP keine Auswirkungen auf Kennwörter, die mit einem LDAP-Verzeichnisse authentifiziert werden. Sie können Ihre Kennwortfunktionen über den IBM Spectrum Protect-Server verwalten. Wenn Sie den Befehl SET INVALIDPWLIMIT ausgegeben haben, werden alle IBM Spectrum Protect-Kennwörter durch den Grenzwert gesteuert, den Sie definiert haben. Wird der LDAP-Verzeichnisse zur Begrenzung der Anzahl der Anmeldeversuche mit ungültigen Kennwörtern konfiguriert, kann ein Konflikt auftreten.

### Beispiel: Die Anzahl zulässiger ungültiger Anmeldeversuche definieren

Für die zulässige Anzahl ungültiger Anmeldeversuche soll der Wert 6 definiert werden.

```
set invalidpwlmit 6
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET INVALIDPWLIMIT

| Befehl          | Beschreibung   |
|-----------------|--|
| QUERY ADMIN     | Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.                               |
| QUERY NODE      | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.                                    |
| QUERY STATUS    | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| SET MINPWLENGTH | Legt die Mindestlänge für Clientkennwörter fest.   |

## SET LDAPPASSWORD (LDAP-Kennwort für den Server definieren)

Verwenden Sie diesen Befehl, um ein Kennwort für die Benutzer-ID oder Konto-ID zu definieren, die mithilfe des Befehls SET LDAPUSER angegeben wurde.

Voraussetzung: Sie müssen die Option LDAPURL definieren und den Befehl SET LDAPUSER ausgeben, bevor Sie den Befehl SET LDAPPASSWORD ausgeben. Wenn die Option LDAPURL nicht definiert ist, wenn Sie das Benutzerkennwort für den Lightweight Directory

Access Protocol-Server (LDAP-Server) festlegen, müssen Sie den IBM Spectrum Protect-Server nach dem Definieren der Option LDAPURL erneut starten.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set LDAPPassword--LDAP-Benutzerkennwort-----<<
```

## Parameter

### LDAP-Benutzerkennwort

Gibt das Kennwort an, das der IBM Spectrum Protect-Server verwendet, wenn er sich mit dem LDAP-Server authentifiziert. Das Kennwort darf maximal 64 Zeichen lang sein. Wenn Ihr Kennwort Gleichheitszeichen enthält, muss das vollständige Kennwort in Anführungszeichen eingeschlossen werden. Sie können die folgenden Zeichen verwenden:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )  
| { } [ ] : ; < > , ? / ~
```

## Beispiel: LDAP-Kennwort festlegen

```
set ldappassword LdAp20&12PaSsWoRd
```

## Beispiel: Ein LDAP-Kennwort definieren, das Gleichheitszeichen enthält

```
set ldappassword "LdAp=LastWoRd"
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET LDAPPASSWORD

| Befehl                    | Beschreibung  |
|---------------------------|---|
| AUDIT LDAPDIRECTORY       | Prüft einen von IBM Spectrum Protect gesteuerten Namensbereich auf einem LDAP-Verzeichnisserver.          |
| SET DEFAULTAUTHENTICATION | Gibt die Standardkennwortauthentifizierungsmethode für alle Befehle REGISTER NODE oder REGISTER ADMIN an. |
| SET LDAPUSER              | Definiert den Benutzer, der die Kennwörter und Administratoren auf dem LDAP-Verzeichnisserver überwacht.  |

## SET LDAPUSER (ID für einen LDAP-Verzeichnisserver angeben)

Verwenden Sie diesen Befehl, um die ID eines Benutzers oder Kontos anzugeben, mit der auf einen LDAP-Server (LDAP = Lightweight Directory Access Protocol) zugegriffen werden kann.

Die angegebene ID muss über Lesezugriff auf die Konten auf dem LDAP-Server verfügen, die für die Authentifizierung verwendet werden. Um LDAP-IDs zu ändern oder Kennwörter für LDAP-IDs zurückzusetzen, muss die angegebene ID über Schreibberechtigung für die Konten auf dem LDAP-Server verfügen.

Tipp: Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set LDAPUser--LDAP-Benutzer-DN-----<<
```

## Parameter

LDAP-Benutzer-DN

Gibt die ID eines Benutzers oder Kontos an, mit der auf einen LDAP-Server zugegriffen werden kann.

## Beispiel: Benutzer-ID mit Administratorberechtigung für die Durchführung von Operationen auf einem LDAP-Server angeben

Um einen Administrator mit der Benutzer-ID JACKSPRATT für ein US-Unternehmen mit dem Namen EXAMPLE anzugeben, geben Sie den folgenden Befehl aus:

```
set ldapuser JackSpratt@us.example.com
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET LDAPUSER

| Befehl                    | Beschreibung  |
|---------------------------|---|
| AUDIT LDAPDIRECTORY       | Prüft einen von IBM Spectrum Protect gesteuerten Namensbereich auf einem LDAP-Verzeichnisserver.          |
| SET DEFAULTAUTHENTICATION | Gibt die Standardkennwortauthentifizierungsmethode für alle Befehle REGISTER NODE oder REGISTER ADMIN an. |
| SET LDAPPASSWORD          | Legt das Kennwort für den LDAPUSER fest.  |

## SET LICENSEAUDITPERIOD (Dauer für Lizenzprüfung definieren)

Mit diesem Befehl kann das Zeitintervall in Tagen angegeben werden, in dem automatisch Lizenzprüfungen von IBM Spectrum Protect durchgeführt werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set--LICenseauditperiod--+-30---+-----<<
                             '-Tage-'
```

## Parameter

Tage

Gibt die Anzahl Tage zwischen den automatischen Server-Lizenzprüfungen an. Dieser Parameter ist wahlfrei. Der Standardwert ist 30. Es kann eine ganze Zahl von 1 bis einschließlich 30 angegeben werden.

## Beispiel: Eine 14-tägige Serverlizenzprüfung angeben

Angaben, dass der Server alle 14 Tage Lizenzen prüft.

```
set licenseauditperiod 14
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET LICENSEAUDITPERIOD

| Befehl         | Beschreibung                                   |
|----------------|--|
| AUDIT LICENSES | Prüft die Einhaltung der definierten Lizenzen. |

| Befehl              | Beschreibung   |
|---------------------|--|
| QUERY AUDITOCUPANCY | Zeigt die Serverspeicherauslastung für einen Clientknoten an.  |
| QUERY LICENSE       | Zeigt Informationen über Lizenzen und Prüfvorgänge an.   |
| QUERY STATUS        | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| REGISTER LICENSE    | Registriert eine Lizenz für den IBM Spectrum Protect-Server.   |

## SET MAXCMDRETRIES (Maximale Anzahl Befehlswiederholungen definieren)

Mit diesem Befehl kann angegeben werden, wie oft ein Scheduler auf einem Client-Knoten maximal versuchen darf, einen geplanten Befehl, der fehlgeschlagen ist, zu wiederholen.

Der Befehl kann verwendet werden, um die maximale Anzahl Wiederholungen zu überschreiben, die von dem Client-Knoten angegeben wird. Der Wert eines Clients wird nur dann überschrieben, wenn der Client den Server ansprechen kann.

Dieser Befehl wird zusammen mit dem Befehl SET RETRYPERIOD verwendet, um die Zeit und die Anzahl Wiederholungen für die erneute Ausführung eines fehlgeschlagenen Befehls zu steuern.

Der Befehl QUERY STATUS kann ausgegeben werden, um die aktuelle Anzahl Wiederholungen anzuzeigen. Bei der Installation wird IBM Spectrum Protect so konfiguriert, daß jeder Client seine eigene Anzahl Wiederholungen festlegt.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-Set MAXCMDRetries-----<<
      '-Anzahl-'
```

### Parameter

Zahl

Gibt an, wie oft der Scheduler auf einem Client-Knoten maximal versuchen darf, einen geplanten Befehl, der fehlgeschlagen ist, zu wiederholen. Dieser Parameter ist wahlfrei.

Standardmäßig bestimmt jeder Client seinen eigenen Wert für diesen Parameter. Zulässige Werte sind ganze Zahlen von 0 bis 9999. Näheres zum Definieren der maximalen Anzahl Befehlswiederholungen auf dem Client steht in der entsprechenden Client-Dokumentation.

### Beispiel: Die maximale Anzahl der Befehlswiederholungen auf 2 setzen

Den fehlgeschlagenen Versuch, einen geplanten Befehl zu verarbeiten, nur zweimal wiederholen.

```
set maxcmdretries 2
```

### Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET MAXCMDRETRIES

| Befehl          | Beschreibung   |
|-----------------|--|
| QUERY STATUS    | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| SET RETRYPERIOD | Gibt die Zeitspanne zwischen Wiederholungsversuchen des Client-Schedulers an.  |

## SET MAXSCHEDESESSIONS (Maximale Anzahl geplanter Sitzungen definieren)

---

Mit diesem Befehl kann die Anzahl der Sitzungen definiert werden, die der Server für die Verarbeitung geplanter Operationen verwenden kann. Dieser Befehl gibt die maximal zulässige Anzahl geplanter Sitzungen als Prozentsatz aller verfügbaren Serversitzungen an.

Mit der Begrenzung der Anzahl der Sitzungen wird sichergestellt, dass einige Sitzungen für nicht geplante Operationen, wie Sichern oder Archivieren, verfügbar sind. Es kann entweder die Gesamtzahl der Sitzungen (mit dem Parameter MAXSESSIONS) oder der maximale Prozentsatz geplanter Sitzungen erhöht werden. Wird die Gesamtzahl der verfügbaren Sitzungen erhöht, kann dies jedoch negative Auswirkungen auf die Serverleistung haben. Wird der maximale Prozentsatz geplanter Sitzungen erhöht, kann dies die verfügbaren Sitzungen für nicht geplante Operationen verringern.

### Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

---

```
>>-Set MAXSCHEDESESSIONS--Prozent-----<<
```

### Parameter

---

Prozent (Erforderlich)

Gibt den Prozentsatz der gesamten Server-Sitzungen an, die für geplante Operationen verwendet werden können. Zulässige Werte sind ganze Zahlen von 0 bis 100. Der Parameter MAXSESSIONS in der Serveroptionsdatei bestimmt die maximale Anzahl der insgesamt zur Verfügung stehenden Serversitzungen.

Wird der maximale Prozentsatz geplanter Sitzungen auf 0 gesetzt, können keine geplanten Ereignisse beginnen. Wird der maximale Prozentsatz geplanter Sitzungen auf 100 gesetzt, entspricht die maximale Anzahl geplanter Sitzungen dem Wert der Option MAXSESSIONS.

Tipp: Wenn die maximale Anzahl geplanter Sitzungen nicht mit dem Prozentsatz übereinstimmt, der im Befehl SET MAXSCHEDESESSIONS definiert wurde, führen Sie den Befehl SET MAXSCHEDESESSIONS erneut aus. Bestimmen Sie die Anzahl, die in der Option MAXSESSIONS angegeben ist. Wenn die Anzahl in der Option MAXSESSIONS geändert und der Befehl SET MAXSCHEDESESSIONS seit der Änderung nicht ausgegeben wurde, kann sich die maximale Anzahl geplanter Sitzungen ändern.

### Maximal 20 Sitzungen für geplante Aktivitäten definieren

---

Die Option MAXSESSIONS hat den Wert 80. Sollen nicht mehr als 20 Sitzungen für geplante Aktivitäten verfügbar sein, setzen Sie den Prozentsatz auf 25.

```
set maxschedsessions 25
```

### Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für SET MAXSCHEDESESSIONS

| Befehl       | Beschreibung   |
|--------------|--|
| QUERY OPTION | Zeigt Informationen über Serveroptionen an.  |
| QUERY STATUS | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## SET MINPWLENGTH (Mindestlänge für Kennwort definieren)

---

Mit diesem Befehl kann die Mindestlänge eines Kennworts definiert werden.

### Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-Set--MINPwlength--Länge-----><
```

## Parameter

Länge (Erforderlich)

Gibt die Mindestlänge eines Kennworts an. Zulässige Werte sind ganze Zahlen von 0 bis 64. Der Wert 0 bedeutet, daß die Kennwortlänge nicht geprüft wird. Der Standardwert für die Mindestlänge des Kennworts wird auf 0 gesetzt.

## Beispiel: Die Mindestkennwortlänge definieren

Die Mindestlänge für Kennwörter auf 5 Zeichen setzen.

```
set minpwlenth 5
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET MINPWLENGTH

| Befehl             | Beschreibung   |
|--------------------|--|
| QUERY STATUS       | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| SET INVALIDPWLIMIT | Definiert die Anzahl ungültiger Anmeldeversuche, die zulässig sind, bevor ein Knoten gesperrt wird.                  |

## SET MONITOREDSEVERGROUP (Gruppe überwachter Server definieren)

Verwenden Sie diesen Befehl, um die Gruppe der Server zu definieren, die hinsichtlich Alerts und Status überwacht werden. Sie können diesen Befehl auch verwenden, um die Gruppe der überwachten Server zu ändern oder zu entfernen.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set MONITOREDSEVERGroup--+-----+-----><  
      '-Gruppenname-'
```

## Parameter

Gruppenname

Gibt den Namen der IBM Spectrum Protect-Servergruppe an, die alle überwachten Server enthält. Sie können den Namen einer überwachten Servergruppe entfernen, indem Sie den Befehl ohne Angabe eines Werts oder unter Angabe eines leeren Werts ("" ) ausgeben. Jede Überwachung hinsichtlich Alerts und Status von fernen Servern wird beendet.

## Den Namen einer überwachten Servergruppe definieren

Den folgenden Befehl ausgeben, um den Namen SUBS einer überwachten Servergruppe zu definieren:

```
set monitoredservergroup subs
```

## Den Namen einer überwachten Servergruppe entfernen

Den folgenden Befehl ausgeben, um die überwachte Servergruppe zu entfernen:

```
set monitoredservergroup
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET MONITOREDSEVERGROUP



| Befehl   | Beschreibung   |
|--|--|
| DEFINE SERVERGROUP (Server-Gruppe definieren)  | Definiert eine neue Servergruppe.  |
| DEFINE GRPMEMBER (Server zu einer Servergruppe hinzufügen)   | Definiert einen Server als Teil einer Servergruppe.  |
| DELETE GRPMEMBER (Server aus einer Servergruppe löschen)   | Löscht einen Server aus einer Servergruppe.  |
| QUERY SERVERGROUP (Servergruppe abfragen)  | Zeigt Informationen über Servergruppen an.   |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen) | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an. |
| SET MONITORINGADMIN (Name des Überwachungsadministrators definieren)   | Definiert den Namen des Überwachungsadministrators.  |

## SET MONITORINGADMIN (Name des Überwachungsadministrators definieren)

Verwenden Sie diesen Befehl, um den Namen des Überwachungsadministrators zu definieren, der verwendet wird, um die Verbindung zu den Servern in der überwachten Servergruppe herzustellen.

Um den Namen der überwachten Servergruppe anzuzeigen, geben Sie den Befehl QUERY MONITORSETTINGS aus.

Der angegebene Administratorname muss mit dem Namen eines vorhandenen Administrators übereinstimmen, andernfalls schlägt der Befehl fehl.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-Set MONITORINGADMIN--+-+-----+----->>
                        '-Administratorname-'
```

### Parameter

Administratorname

Gibt Administratornamen an. Sie können Namen entfernen, indem Sie den Befehl ohne Angabe eines Werts oder unter Angabe eines leeren Werts ("" ) ausgeben.

### Den Namen des Überwachungsadministrators definieren

Den folgenden Befehl ausgeben, um den Namen MONADMIN für den Überwachungsadministrator zu definieren:

```
set monitoringadmin monadmin
```

### Den Namen des Überwachungsadministrators entfernen

Den folgenden Befehl ausgeben, um den Überwachungsadministrator zu entfernen:

```
set monitoringadmin ""
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET MONITORINGADMIN

| Befehl   | Beschreibung   |
|--|--|
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen) | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an. |
| SET MONITOREDSEVERGROUP (Gruppe überwachter Server definieren)   | Definiert die Gruppe der überwachten Server.   |

# SET NODEATRISKINTERVAL (Gibt den Gefährdungsmodus für einen einzelnen Knoten an)

Verwenden Sie diesen Befehl, um den Auswertungsmodus für Gefährdung für einen einzelnen Knoten anzupassen.

## Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie die Systemberechtigung, die Maßnahmenberechtigung für die Domäne, der der Knoten zugeordnet ist, oder die Clienteignerberechtigung für den Knoten haben.

## Syntax

```
>>---Set NODEATRISKINTERVAL--Knotenname----->
>--TYPE-----+DEFAULT-----+-----><
      +-BYPASSED-----+
      '-CUSTOM--Interval---Wert-'
```

## Parameter

Knotenname (Erforderlich)

Gibt den Namen des Clientknotens an, der aktualisiert werden soll.

TYPE (Erforderlich)

Gibt den Auswertungstyp für Gefährdung an. Geben Sie einen der folgenden Werte an:

DEFAULT

Gibt an, dass der Knoten mit demselben Intervall ausgewertet wird, das für die Knotenklassifizierung mit dem Befehl SET STATUSATRISKINTERVAL angegeben wurde. Der Wert lautet entweder 'System' oder 'Anwendungen' oder 'VM' und wird vom Statusmonitor bestimmt.

Sie können beispielsweise `TYPE = DEFAULT` angeben, womit es dem Statusmonitor ermöglicht wird, fortzufahren und den Knoten automatisch zu klassifizieren. Das Intervall, das dann verwendet wird, ist das Intervall, das für diese Klassifizierung mit dem Befehl SET STATUSATRISKINTERVAL definiert wurde.

BYPASSED

Gibt an, dass der Gefährdungsstatus für den Knoten nicht vom Statusmonitor ausgewertet wird. Der Gefährdungsstatus wird auch an das Operations Center als 'Bypassed' (Übergangen) zurückgemeldet.

CUSTOM

Gibt an, dass der Knoten mit dem angegebenen Intervall und nicht mit dem Intervall ausgewertet wird, das mit dem Befehl SET STATUSATRISKINTERVAL angegeben wurde.

Interval

Gibt die Zeit in Stunden zwischen Clientsicherungsaktivitäten an, bevor der Statusmonitor den Client als gefährdet ansieht. Sie können eine ganze Zahl im Bereich von 6 bis 8808 angeben. Bei `TYPE = CUSTOM` müssen Sie diesen Parameter angeben. Bei `TYPE = BYPASSED` oder `TYPE = DEFAULT` wird dieser Parameter nicht angegeben. Der Intervallwert für alle Clienttypen wird bei der Serverinstallation auf 24 gesetzt.

## Für einen Knotennamen ein angepasstes Gefährdungsintervall von 90 Tagen definieren

Das Gefährdungsintervall für einen Knoten mit dem Namen *fred* auf 90 Tage setzen.

```
set nodeatriskinterval fred type=custom interval=2160
```

## Die Auswertung für das Gefährdungsintervall übergehen

Die Überprüfung des Gefährdungsintervalls für einen Knoten mit dem Namen *bob* übergehen.

```
set nodeatriskinterval bob type=bypassed
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für set nodeatriskinterval

| Befehl | Beschreibung |
|--------|--------------|
|--------|--------------|

| Befehl  | Beschreibung   |
|---|--|
| SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)        | Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.         |
| SET VMATRISKINTERVAL (Gibt den Gefährdungsmodus für einen einzelnen VM-Dateibereich an)   | Definiert den Gefährdungsmodus für einen VM-Dateibereich.  |
| QUERY MONITORSTATUS (Überwachungsstatus abfragen)   | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                             |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)                                      | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                             |
| SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)   | Gibt an, ob die Statusüberwachung aktiviert werden soll.   |
| SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)   | Gibt das Aktualisierungsintervall für die Statusüberwachung an.  |
| SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll) | Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll. |
| QUERY NODE (Knoten abfragen)  | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.  |
| QUERY FILESPACE (Dateibereiche abfragen)  | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.  |

## SET PASSEXP (Ablaufdatum für Kennwort definieren)

Mit diesem Befehl kann die Kennwortablaufdauer für Kennwörter von Administratoren und Clientknoten angegeben werden. Sie können entweder eine allgemeine Kennwortablaufdauer für die Kennwörter aller Administratoren und Clientknoten definieren oder die Kennwortablaufdauer jeweils selektiv festlegen.

Einschränkung: Der Befehl SET PASSEXP gilt nicht für Kennwörter, die sich mit einem LDAP-Verzeichnisserver authentifizieren.

Sie können die Einstellung für SET PASSEXP für einen oder mehrere Knoten überschreiben, indem Sie den Befehl REGISTER NODE oder UPDATE NODE mit dem Parameter PASSEXP verwenden.

Der Parameter NODE oder ADMIN muss angegeben werden, um die Kennwortablaufdauer für Clientknoten oder Administratoren zu ändern, für die Kennwortablaufdauer jeweils selektiv festgelegt wurde. Wird der Parameter NODE oder ADMIN nicht angegeben, verwenden *alle* Clientknoten- und Administratorkennwörter die neue Kennwortablaufdauer. Wenn Sie eine Kennwortablaufdauer für einen Clientknoten oder einen Administrator individuell definieren, der noch nicht über eine definierte Kennwortablaufdauer verfügt, wird sie nicht geändert, wenn Sie später eine Kennwortablaufdauer für alle Benutzer festlegen.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set PASSExp--Tage--+-+-----+-----+----->
|           .-,----- . |
|           v             | |
|'-Node-----Knotenname-+-'|
>+-----+-----+-----+-----><
|           .-,----- . |
|           v             | |
|'-Admin-----Administratorname-+-'|
```

## Parameter

Tage (Erforderlich)

Gibt die Anzahl der Tage an, die ein Kennwort gültig ist.

Sie können einen Wert von 1 bis 9999 angeben, wenn Sie den Parameter NODE oder ADMIN nicht angeben. Wird der Parameter NODE oder ADMIN angegeben, kann ein Wert von 0 bis 9999 angegeben werden. Der Wert 0 bedeutet, dass das Kennwort niemals abläuft. Läuft ein Kennwort ab, fordert der Server zur Eingabe eines neuen Kennworts auf, wenn der Administrator oder der Clientknoten eine Verbindung zum Server herstellt.

#### Node

Gibt den Namen des Knotens an, für den die Kennwortablaufdauer definiert wird. Soll eine Liste mit Knoten angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Dieser Parameter ist wahlfrei.

#### Admin

Gibt den Namen des Administrators an, dessen Kennwortablaufdauer definiert werden soll. Soll eine Liste mit Administratoren angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Dieser Parameter ist wahlfrei.

## Beispiel: Die Kennwortablaufdauer für das Administrator- und Clientknoten Kennwort definieren

Die Kennwortablaufdauer für das Administrator- und Clientknoten Kennwort soll auf 45 Tage gesetzt werden.

```
set passexp 45
```

## Beispiel: Die Kennwortablaufdauer für einen Administrator definieren

Die Kennwortablaufdauer für den Administrator LARRY auf 120 Tage setzen.

```
set passexp 120 admin=larry
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET PASSEXP

| Befehl        | Beschreibung   |
|---------------|--|
| QUERY STATUS  | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| REGISTER NODE | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.                              |
| RESET PASSEXP | Setzt die Kennwortablaufdauer für Knoten oder Administratoren zurück.  |
| UPDATE ADMIN  | Ändert das Kennwort eines Administrators bzw. die zu einem Administrator gehörigen Kontaktinformationen.             |
| UPDATE NODE   | Ändert die Attribute, die einem Clientknoten zugeordnet sind.  |

## SET PRODUCTOFFERING (Produktangebot definieren, das für Ihr Unternehmen lizenziert ist)

Verwenden Sie den Befehl SET PRODUCTOFFERING, um das IBM Spectrum Protect-Produktangebot zu definieren, das für Ihr Unternehmen lizenziert ist.

Die Definition wird verwendet, um zu bestimmen, ob automatische Berechnungen der Speicherkapazitätsmesswerte erforderlich sind und für die Verwendung durch das IBM® License Metric Tool (ILMT) verfügbar gemacht werden. Führen Sie diesen Befehl nur aus, wenn Sie ILMT verwenden, um die Lizenznutzung zu bestimmen.

Für Produktangebote, bei denen automatische Berechnungen der Speicherkapazitätsmesswerte für die Verwendung durch ILMT verfügbar gemacht werden, definiert der Parameter auch die Methode der Kapazitätsmessung, die für diese Berechnungen verwendet wird.

Die Methode der Kapazitätsmessung wird durch die Lizenzbedingungen Ihres speziellen Produktangebots definiert. Um die derzeit berechnete Speicherkapazität für Ihr Produktangebot zu bestimmen, lesen Sie die Informationen in Lizenzinhaltung prüfen.

Dieselben Speicherkapazitätsinformationen werden ILMT in einem wöchentlichen Intervall zur Verfügung gestellt. Nachdem ein gültiges Produktangebot mithilfe dieses Befehls definiert wurde, stellt IBM Spectrum Protect die aktuelle Kapazitätsberechnung für dieses Angebot ILMT zur Verfügung. Nachdem die anfängliche Kapazitätsberechnung ILMT zur Verfügung gestellt wurde, wird der Wert wöchentlich von IBM Spectrum Protect aktualisiert.

## Berechtigungsklasse

Um diesen Befehl auszuführen, müssen Sie über die Systemberechtigung verfügen.

## Syntax

---

```
>>-SET PRODUCTOFFERING--Produktangebot-----<<
```

## Parameter

---

### Produktangebot (Erforderlich)

Gibt ein Produktangebot an. Die maximale Länge der Zeichenfolge beträgt 255 Zeichen. Folgende Optionen sind verfügbar:

#### ENTry

Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Entry ist. Dieses Produktangebot verwendet eine Lizenzmetrik pro verwaltetem Server. Kapazitätsmesswerte für dieses Produktangebot sind nicht zutreffend.

#### DATARet

Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect for Data Retention ist. Kapazitätsmesswerte für dieses Produktangebot werden nicht automatisch berechnet oder für die Verwendung durch ILMT verfügbar gemacht.

#### BASIC

Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect ist. Dieses Produktangebot verwendet eine PVU-Lizenzmetrik (PVU = Prozessor-Value-Unit). Kapazitätsmesswerte für dieses Produktangebot sind nicht zutreffend.

#### EE

Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Extended Edition ist. Dieses Produktangebot verwendet eine PVU-Lizenzmetrik. Kapazitätsmesswerte für dieses Produktangebot sind nicht zutreffend.

#### SUIte

Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Suite ist. Kapazitätsmesswerte für dieses Produktangebot werden automatisch berechnet und für die Verwendung durch ILMT verfügbar gemacht.

#### SUITEEntry

Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Suite Entry ist. Kapazitätsmesswerte für dieses Produktangebot werden automatisch berechnet und für die Verwendung durch ILMT verfügbar gemacht.

#### SUITEArchive

Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Suite - Archive ist. Kapazitätsmesswerte für dieses Produktangebot werden automatisch berechnet und für die Verwendung durch ILMT verfügbar gemacht.

#### SUITEProtectier

Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Suite - ProtectTier ist. Kapazitätsmesswerte für dieses Produktangebot werden automatisch berechnet und für die Verwendung durch ILMT verfügbar gemacht.

#### SUITEFrontend

Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Suite - FrontEnd ist. Kapazitätsmesswerte für dieses Produktangebot werden automatisch berechnet und für die Verwendung durch ILMT verfügbar gemacht.

#### SUITEENTRYFrontend

Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Suite Entry - FrontEnd ist. Kapazitätsmesswerte für dieses Produktangebot werden automatisch berechnet und für die Verwendung durch ILMT verfügbar gemacht.

#### CLEAR

Es ist kein Produktangebot angegeben.

## Beispiel: Für das Produktangebot IBM Spectrum Protect (BASIC) definieren

---

```
set productoffering BASIC
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET PRODUCTOFFERING

| Befehl       | Beschreibung   |
|--------------|--|
| QUERY STATUS | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## SET QUERYSCHEDPERIOD (Zeitraum für Abfrage von Clientknoten definieren)

Mit diesem Befehl kann gesteuert werden, wie oft Client-Knoten den Server ansprechen, um geplante Arbeit abzurufen, wenn der Planungsmodus Client-Sendeaufruf lautet.

Jeder Client kann beim Starten seines Schedulers seinen eigenen Wiederholungszeitraum definieren. Mit diesem Befehl kann der Wert überschrieben werden, der von allen Clients angegeben wird, die eine Verbindung zum Server herstellen können.

Wenn Client-Knoten Zeitpläne häufiger abfragen, werden Änderungen an den Zeitplänen von den Knoten schneller empfangen. Häufigere Sendeaufrufe durch die Client-Knoten führen jedoch auch zu vermehrtem Datenaustausch auf dem Netz.

Der Befehl QUERY STATUS kann ausgegeben werden, um den Wert für die Periode zwischen Zeitplanabfragen anzuzeigen. Bei der Installation wird IBM Spectrum Protect so konfiguriert, daß jeder Client-Knoten seinen eigenen Wert für diese Einstellung festlegt.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-Set QUERYSChedperiod--+-+-----+-----><  
                    '-Stunden-'
```

### Parameter

Stunden

Gibt die maximale Anzahl Stunden an, die der Scheduler auf einem Client-Knoten zwischen Versuchen wartet, den Server anzusprechen, um einen Zeitplan abzurufen. Dieser Parameter ist wahlfrei. Zulässige Werte sind ganze Zahlen von 1 bis 9999. Wird kein Wert für diesen Parameter angegeben, legt jeder Client seinen eigenen Wert für diesen Parameter fest.

### Beispiel: Das Überwachungsintervall für alle Clientknoten definieren

Alle Clients, die den Planungsmodus Sendeaufruf verwenden, sollen den Server alle 24 Stunden ansprechen.

```
set querieschedperiod 24
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET QUERYSCHEDPERIOD

| Befehl         | Beschreibung   |
|----------------|--|
| QUERY STATUS   | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| SET SCHEDMODES | Gibt den zentralen Planungsmodus für den Server an.  |

## SET RANDOMIZE (Zufallsgenerierung von geplanten Startzeiten definieren)

Mit diesem Befehl können wahlfreie Startzeiten innerhalb des Startfensters jedes Zeitplans für Clients definiert werden, indem der Planungsmodus Client-Sendeaufruf verwendet wird. Ein Startfenster ist die Startzeit und die Dauer, während der ein Zeitplan eingeleitet werden muß. Der Planungsmodus Client-Sendeaufruf ist eine Client/Server-Übertragungstechnik, bei der der Client den Server nach Arbeit abfragt.

Jeder Zeitplan verfügt über ein Fenster, innerhalb dessen er ausgeführt werden kann. Um einen Ausgleich hinsichtlich der Belastung für Netz und Server zu schaffen, können die Startzeiten für Clients über dieses Fenster gestreut werden. Mit Hilfe dieses Befehls kann der Bruchteil des Fensters angegeben werden, über den die Startzeiten für Clients gestreut werden.

Die Zufallsgenerierung tritt am Anfang des Fensters auf, um Zeit für Wiederholungsversuche zu lassen (falls erforderlich). Ist der Planungsmodus nicht auf 'Sendeaufruf' gesetzt, erfolgt keine Zufallsgenerierung, wenn der erste Kontakt des Clients mit dem Server nach der Startzeit für das Ereignis stattfindet.

Der Befehl QUERY STATUS kann ausgegeben werden, um den Prozentsatz für die Zufallsgenerierung anzuzeigen. Bei der Installation lautet der Wert 25 Prozent.

Der Prozentsatz für die Zufallsgenerierung sollte auf einen Wert größer als 0 gesetzt werden, um Übertragungsfehler zu vermeiden. Übertragungsfehler können auftreten, wenn eine große Gruppe von Clients gleichzeitig die Verbindung zum Server herstellen will. Kommt es zu Übertragungsfehlern, kann der Prozentsatz vergrößert werden, so dass die Kontaktaufnahme vom Client zum Server über einen längeren Zeitraum erfolgen kann. Dadurch wird die Wahrscheinlichkeit von Übertragungsüberlastung und -fehlern verringert.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-Set RANDomize--Prozent-----><
```

## Parameter

---

Prozent (Erforderlich)

Gibt den Prozentsatz des Startfensters an, über den die Startzeiten für einzelne Clients verteilt werden. Zulässige Werte sind ganze Zahlen von 0 bis 50.

Der Wert 0 gibt an, dass keine Zufallsgenerierung stattfindet und alle Clients Zeitpläne am Anfang der Startfenster ausführen.

Der Wert 50 gibt an, dass den Clients Startzeiten zugeordnet werden, die willkürlich über die erste Hälfte jedes Startfensters verteilt werden.

Bei der Installation lautet dieser Wert 25 Prozent. Der Wert gibt an, dass die ersten 25 Prozent des Fensters für die Zufallsgenerierung verwendet werden.

Wurde DURUNITS=INDEFINITE im Befehl DEFINE SCHEDULE angegeben, wird der Prozentsatz auf eine 24-Stunden-Periode angewendet. Ein Wert von 25 Prozent hätte beispielsweise ein 6-Stunden-Fenster zur Folge.

## Beispiel: Die Zufallsgenerierung von geplanten Startzeiten definieren

---

Der Wert für die Zufallsgenerierung soll auf 50 Prozent gesetzt werden.

```
set randomize 50
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für SET RANDOMIZE

| Befehl          | Beschreibung   |
|-----------------|--|
| DEFINE SCHEDULE | Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl.                                      |
| QUERY STATUS    | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| SET SCHEDMODES  | Gibt den zentralen Planungsmodus für den Server an.  |

## SET REPLRECOVERDAMAGED (Angaben, ob beschädigte Dateien von einem Replikationsserver wiederhergestellt werden)

---

Verwenden Sie diesen Befehl, um die systemweite Wiederherstellung beschädigter Dateien durch einen Zielreplikationsserver zu aktivieren. Ist diese Einstellung aktiviert, kann der Knotenreplikationsprozess so konfiguriert werden, dass beschädigte Dateien auf dem Quellenreplikationsserver erkannt und durch unbeschädigte Dateien vom Zielreplikationsserver ersetzt werden.

Der Systemparameter REPLRECOVERDAMAGED betrifft alle Dateiwiederherstellungsprozesse bei allen Replikationsprozessen für alle Knoten und Dateibereiche. Die Dateiwiederherstellung ist nur möglich, wenn die Server-Software der Version 7.1.1 oder höher auf dem Quellen- und Zielreplikationsserver installiert ist und die Knotendaten repliziert wurden, bevor die Dateibeschädigung aufgetreten ist.

Soll die aktuelle Einstellung angezeigt werden, verwenden Sie den Befehl QUERY STATUS.

Wenn Sie den Server installieren, lautet die Standardeinstellung ON.

Wenn ein Upgrade für den Server durchgeführt wird und keine beschädigten Dateien erkannt werden, lautet die Standardeinstellung ON.

Wenn ein Upgrade für den Server durchgeführt wird und beschädigte Dateien erkannt werden, wird der Parameter auf OFF gesetzt und eine Nachricht ausgegeben, die angibt, dass die Wiederherstellung beschädigter Dateien inaktiviert ist. Die Einstellung OFF verhindert, dass der Server Datenbanktabellen nach beschädigten Objekten durchsucht, die wiederhergestellt werden können. Das Verhindern der Suche ist erforderlich, wenn viele beschädigte Dateien erkannt werden. In diesem Fall kann eine Suche sehr viel Zeit in Anspruch nehmen und sollte geplant werden, wenn die Verwendung von Serverressourcen auf ein Minimum beschränkt ist. Wenn die Suche gestartet werden kann und beschädigte Dateien wiederhergestellt werden können, müssen Sie den Befehl SET REPLRECOVERDAMAGED ausgeben und die Einstellung ON angeben. Nachdem der Server die Suche erfolgreich beendet hat, wird der Systemparameter REPLRECOVERDAMAGED auf ON gesetzt.

In der folgenden Tabelle wird beschrieben, wie sich der Systemparameter REPLRECOVERDAMAGED und andere Parameter auf die Wiederherstellung beschädigter, replizierter Dateien auswirken.

Tabelle 1. Einstellungen, die sich auf die Wiederherstellung beschädigter Dateien auswirken

| Einstellung für den Systemparameter REPLRECOVERDAMAGED | Wert des Parameters RECOVERDAMAGED im Befehl REPLICATE NODE | Wert des Parameters RECOVERDAMAGED in den Befehlen REGISTER NODE und UPDATE NODE | Ergebnis  |
|--|---|--|---|
| OFF  | YES, NO oder nicht angegeben                                | YES oder NO  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.    |
| OFF  | ONLY  | YES oder NO  | Eine Fehlernachricht wird angezeigt, weil Dateien nicht wiederhergestellt werden können, wenn der Systemparameter REPLRECOVERDAMAGED auf OFF gesetzt ist. |
| ON   | YES   | YES oder NO  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.          |
| ON   | NO  | YES oder NO  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.    |
| ON   | ONLY  | YES oder NO  | Beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt, aber es findet keine Standardknotenreplikation statt.                            |
| ON   | Nicht angegeben   | YES  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.          |
| ON   | Nicht angegeben   | NO   | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.    |

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax



```

.-Set REPLRECOVERDamaged---ON----- .
>>+-----+-----><
'-Set REPLRECOVERDamaged---+OFF+-'
      '-ON--'

```

## Parameter

- ON  
Gibt an, dass die Knotenreplikation aktiviert ist, um beschädigte Dateien durch einen Zielreplikationsserver wiederherzustellen.
- OFF  
Gibt an, dass die Knotenreplikation nicht aktiviert ist, um beschädigte Dateien durch einen Zielreplikationsserver wiederherzustellen.

## Beispiel: Wiederherstellung beschädigter Dateien aktivieren

Um eine systemweite Einstellung anzugeben, die es dem Server ermöglicht, beschädigte Dateien von einem Zielreplikationsserver wiederherzustellen, geben Sie den folgenden Befehl aus:

```
set replrecoverdamaged on
```

## Zugehörige Befehle

Tabelle 2. Zugehörige Befehle für SET REPLRECOVERDAMAGED

| Befehl         | Beschreibung   |
|----------------|--|
| QUERY STATUS   | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| REGISTER NODE  | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.                              |
| REPLICATE NODE | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |
| UPDATE NODE    | Ändert die Attribute, die einem Clientknoten zugeordnet sind.  |

## SET REPLRETENTION (Aufbewahrungszeitraum für Replikationsdatensätze definieren)

Um geeignete Informationen zu Replikationsprozessen aufzubewahren, können Sie mit diesem Befehl den Zeitraum anpassen, für den der Quellenreplikationsserver Replikationsdatensätze in seiner Datenbank aufbewahren soll. Mit dem Befehl SET REPLRETENTION wird der Aufbewahrungszeitraum für Replikationsdatensätze für Clientknoten in der Datenbank des Quellenreplikationsservers angegeben. Sie können Replikationsdatensätze für Clientknoten verwenden, um aktive und abgeschlossene Prozesse zu überwachen.

Ein Replikationsdatensatz wird erstellt, wenn die Verarbeitung des Befehls REPLICATE NODE gestartet wird. Standardmäßig werden Replikationsdatensätze für Clientknoten von IBM Spectrum Protect 30 Kalendertage aufbewahrt. Ein Kalendertag besteht aus 24 Stunden, von Mitternacht bis Mitternacht. Beispiel: Angenommen, der Aufbewahrungszeitraum beträgt zwei Kalendertage. Wird ein Replikationsprozess um 23:00 Uhr am Tag *n* abgeschlossen, wird ein Datensatz dieses Prozesses für 25 Stunden bis Mitternacht am Tag *n+1* aufbewahrt. Um den Aufbewahrungszeitraum für Replikationsdatensätze anzuzeigen, geben Sie den Befehl QUERY STATUS auf dem Quellenreplikationsserver aus.

Geben Sie den Befehl SET REPLRETENTION auf dem Server aus, der als Quelle für replizierte Daten agiert.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```

.-30----- .
>>-Set REPLRETention---+-----+-----><
      '-Anzahl_Tage-'

```

## Parameter

---

Anzahl\_Tage (Erforderlich)

Die Anzahl der Tage, die der Quellenreplikationsserver Replikationsdatensätze aufbewahrt. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Standardwert ist 30.

## Beispiel: Einen Aufbewahrungszeitraum für Replikationsdatensätze für Clientknoten definieren

---

Replikationsdatensätze für Clientknoten sollen 10 Tage aufbewahrt werden.

```
set replretention 10
```

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für SET REPLRETENTION

| Befehl            | Beschreibung   |
|-------------------|--|
| QUERY REPLICATION | Zeigt Informationen zu Knotenreplikationsprozessen an.   |
| QUERY REPLNODE    | Zeigt Informationen zum Replikationsstatus eines Clientknotens an.   |
| QUERY REPLRULE    | Zeigt Informationen zu Knotenreplikationsregeln an.  |
| REPLICATE NODE    | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |
| QUERY STATUS      | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## SET REPLSERVER (Zielreplikationsserver definieren)

---

Verwenden Sie diesen Befehl, um den Namen eines Zielreplikationsservers zu definieren. Sie können diesen Befehl auch verwenden, um einen Zielreplikationsserver zu ändern oder zu entfernen.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Um den Namen eines Zielreplikationsservers anzuzeigen, geben Sie auf einem Quellenreplikationsserver den Befehl QUERY STATUS aus.

Wichtig:

- Der Servername, der mit diesem Befehl angegeben wird, muss mit dem Namen einer vorhandenen Serverdefinition übereinstimmen. Er muss auch dem Namen des Servers entsprechen, der als Zielreplikationsserver verwendet werden soll. Wenn der mit diesem Befehl angegebene Servername nicht mit dem Servernamen einer vorhandenen Serverdefinition übereinstimmt, schlägt der Befehl fehl.
- Gehen Sie mit Vorsicht vor, wenn Sie einen Zielreplikationsserver ändern oder entfernen. Wenn Sie einen Zielreplikationsserver ändern, werden replizierte Clientknotendaten an einen anderen Zielreplikationsserver gesendet. Wenn Sie einen Zielreplikationsserver entfernen, werden Clientknotendaten nicht repliziert.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-Set REPLSERVER--+-----+----->>  
                    '-Zielservername-'
```

## Parameter

---

Zielservername

Gibt den Namen des Zielreplikationsservers an. Der angegebene Name muss mit dem Namen eines vorhandenen Servers übereinstimmen. Die maximale Länge eines Namens beträgt 64 Zeichen.

Um einen Zielreplikationsserver zu entfernen, geben Sie den Befehl ohne Angabe eines Werts aus.  
Anmerkung: Soll das Replizieren von Daten nicht fortgesetzt werden, können Sie die Knotenreplikationskonfiguration entfernen, nachdem Sie den Zielreplikationsserver entfernt haben.

## Beispiel: Einen Zielreplikationsserver definieren

Der Name des Servers, der als Zielreplikationsserver definiert werden soll, lautet SERVER1.

```
set replserver server1
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET REPLSERVER

| Befehl            | Beschreibung   |
|-------------------|--|
| DEFINE SERVER     | Definiert einen Server für die Übertragung zwischen Servern.   |
| QUERY SERVER      | Zeigt Informationen über Server an.  |
| QUERY STATUS      | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| UPDATE SERVER     | Aktualisiert Informationen über einen Server.  |
| REMOVE REPLNODE   | Entfernt einen Knoten aus der Replikation.   |
| REMOVE REPLSERVER | Entfernt einen Server aus der Replikation.   |

## SET RETRYPERIOD (Zeitintervall zwischen Wiederholungsversuchen definieren)

Mit diesem Befehl kann die Anzahl Minuten angegeben werden, die der Scheduler auf einem Client-Knoten nach einem fehlgeschlagenen Versuch, den Server anzusprechen, bzw. nach Fehlschlagen eines geplanten Befehls wartet, bis er den Versuch wiederholt.

Jeder Client kann beim Starten seines Scheduler-Programms ein eigenes Wiederholungsintervall angeben. Mit diesem Befehl können die Werte überschrieben werden, die von allen Clients angegeben werden, die eine Verbindung mit dem Server herstellen können.

Dieser Befehl wird in Verbindung mit dem Befehl SET MAXCMDRETRIES verwendet, um das Wiederholungsintervall und die Anzahl Wiederholungsversuche bei einem fehlgeschlagenen Befehl zu regulieren.

Der Befehl QUERY STATUS kann ausgegeben werden, um den Wert für die Periode zwischen Wiederholungen anzuzeigen. Bei der Installation erlaubt IBM Spectrum Protect jedem Client, seinen eigenen Wiederholungszeitraum zu bestimmen.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set RETRYPeriod--+-+-----+-----><  
                    '-Minuten-'
```

## Parameter

### Minuten

Gibt die Anzahl Minuten zwischen den Wiederholungsversuchen an, die der Scheduler auf einem Client-Knoten unternimmt, wenn es ihm nicht gelingt, den Server anzusprechen bzw. einen geplanten Befehl auszuführen. Beim Definieren des Wiederholungszeitraums ist eine Zeitspanne anzugeben, die innerhalb eines typischen Startfensters mehrere Wiederholungsversuche zulässt. Zulässige Werte sind ganze Zahlen von 1 bis 9999.

## Beispiel: Einen Zeitraum von fünfzehn Minuten zwischen Wiederholungsversuchen definieren

Der Client-Scheduler soll die Ausführung alle fünfzehn Minuten wiederholen, wenn es ihm nicht gelingt, den Server anzusprechen bzw. geplante Befehle zu verarbeiten.

```
set retryperiod 15
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET RETRYPERIOD

| Befehl            | Beschreibung   |
|-------------------|--|
| QUERY STATUS      | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| SET MAXCMDRETRIES | Gibt die maximale Anzahl Wiederholungen nach der fehlgeschlagenen Ausführung eines geplanten Befehls an.             |

## SET SCHEDMODES (Modus für zentrale Zeitplanung auswählen)

Mit diesem Befehl kann bestimmt werden, wie die Clients mit dem Server kommunizieren, um geplante Arbeit zu beginnen. Sie müssen jeden Client so konfigurieren, dass er den gewünschten Planungsmodus auswählt.

Verwenden Sie diesen Befehl mit dem Befehl SET RETRYPERIOD, um die Zeit und die Anzahl Wiederholungen für die Verarbeitung eines fehlgeschlagenen Befehls zu steuern.

Der Befehl QUERY STATUS kann ausgegeben werden, um den Wert für den unterstützten Planungsmodus anzuzeigen. Bei der Installation lautet dieser Wert ANY.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set SCHEDMODES---ANY-----+-----<
      +-Polling--+
      '-Prompted-'
```

## Parameter

### ANY

Gibt an, dass Clients entweder im Planungsmodus Clientsendeaufruf (Polling) oder im Planungsmodus Serversystemanfrage (Prompted) ausgeführt werden können.

### POLLING

Gibt an, daß nur der Modus Client-Sendeaufruf (Polling) verwendet werden kann. Client-Knoten fragen den Server in festgelegten Zeitintervallen nach geplanter Arbeit ab.

### PROMPTED

Gibt an, daß nur der Modus Server-Systemanfrage (Prompted) verwendet werden kann. Dieser Modus steht nur für Clients zur Verfügung, die mit Hilfe von TCP/IP kommunizieren. Client-Knoten warten auf die Kontaktaufnahme durch den Server, wenn geplante Arbeit ausgeführt werden muß und eine Sitzung verfügbar ist.

## Beispiel: Geplante Operationen auf Clients beschränken, die den Modus Clientsendeaufruf (Polling) verwenden

Clients können sowohl unter der zentralen Zeitplanung "Serversystemanfrage" als auch "Clientsendeaufruf" ausgeführt werden. Die geplanten Operationen sollen vorübergehend auf Clients beschränkt werden, die den Modus Client-Sendeaufruf (Polling) verwenden. Wenn für den Planungsmodus POLLING festgelegt wird, unterbleibt die Aufforderung des Servers an die Clients, geplante Befehle auszuführen. Das heißt, daß alle Client-Scheduler, die den Modus Server-Systemanfrage (Prompted) verwenden, warten, bis für den Planungsmodus ANY oder PROMPTED angegeben wird.

```
set schedmodes polling
```

## Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET SCHEDMODES

| Befehl | Beschreibung |
|--------|--------------|
|--------|--------------|

| Befehl          | Beschreibung   |
|-----------------|--|
| QUERY STATUS    | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| SET RETRYPERIOD | Gibt die Zeitspanne zwischen Wiederholungsversuchen des Client-Schedulers an.  |

## SET SCRATCHPADRETENTION (Aufbewahrungszeitraum für Scratchpad definieren)

Mit diesem Befehl können Sie den Zeitraum definieren, den Scratchpadeinträge aufbewahrt werden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-SET SCRATCHPADRETENTION--Tage-----<<
```

### Parameter

Tage (Erforderlich)

Gibt die Anzahl der Tage an, die ein Scratchpadeintrag nach der letzten Aktualisierung des Scratchpadeintrags aufbewahrt wird. Sie können eine ganze Zahl im Bereich von 1 bis 9999 eingeben.

### Beispiel: Scratchpadeinträge für die Dauer von 367 Tagen nach ihrer letzten Aktualisierung aufbewahren

```
set scratchpadretention 367
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET SCRATCHPADRETENTION

| Befehl                 | Beschreibung  |
|------------------------|---|
| DEFINE SCRATCHPADENTRY | Erstellt eine Zeile mit Daten im Scratchpad.              |
| DELETE SCRATCHPADENTRY | Löscht eine Zeile mit Daten aus dem Scratchpad.           |
| QUERY SCRATCHPADENTRY  | Zeigt Informationen an, die im Scratchpad enthalten sind. |
| UPDATE SCRATCHPADENTRY | Aktualisiert Daten in einer Zeile im Scratchpad.          |

## SET SERVERHLADDRESS (Serveradresse der höheren Ebene definieren)

Mit diesem Befehl kann die Adresse der höheren Ebene (IP) eines Servers definiert werden. IBM Spectrum Protect verwendet die Adresse, wenn ein Befehl DEFINE SERVER mit CROSSDEFINE=YES ausgegeben wird. Sie müssen den Befehl SET SERVERHLADDRESS für alle automatischen Clientimplementierungen verwenden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-Set SERVERHladdress--IP-Adresse-----<<
```

### Parameter

IP-Adresse (Erforderlich)

Gibt die Adresse der höheren Ebene eines Servers als numerischen Namen in Schreibweise mit Trennzeichen oder als Host-Namen an. Wird ein Host-Name angegeben, muß ein Server verfügbar sein, der den Namen in das Format in Schreibweise mit Trennzeichen auflösen kann.

## Beispiel: Die Adresse der höheren Ebene eines Servers definieren

---

Die Adresse der höheren Ebene von HQ\_SERVER auf 9.230.99.66 setzen.

```
set serverhladdress 9.230.99.66
```

## Zugehörige Befehle

---

Tabelle 1. Zugehöriger Befehl für SET SERVERHLADDRESS

| Befehl              | Beschreibung  |
|---------------------|---|
| SET CROSSDEFINE     | Gibt an, ob Server überkreuz definiert werden sollen. |
| SET SERVERLLADDRESS | Gibt die Adresse der unteren Ebene eines Servers an.  |
| SET SERVERPASSWORD  | Gibt das Serverkennwort an.                           |

## SET SERVERLLADDRESS (Serveradresse der unteren Ebene definieren)

---

Mit diesem Befehl kann die Adresse der unteren Ebene eines Servers definiert werden. IBM Spectrum Protect verwendet die Adresse, wenn ein Befehl DEFINE SERVER mit CROSSDEFINE=YES ausgegeben wird.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-Set SERVERLladdress--TCP-Anschluss-----<<
```

## Parameter

---

TCP-Anschluss (Erforderlich)

Gibt die Adresse der unteren Ebene des Servers an. Im allgemeinen ist diese Adresse mit der Adresse in der Option TCPPOINT in der Server-Optionsdatei des Servers identisch.

## Beispiel: Die Adresse der unteren Ebene eines Servers definieren

---

Die Adresse der unteren Ebene von HQ\_SERVER auf 1500 setzen.

```
set serverlladdress 1500
```

## Zugehörige Befehle

---

Tabelle 1. Zugehöriger Befehl für SET SERVERLLADDRESS

| Befehl              | Beschreibung  |
|---------------------|---|
| SET CROSSDEFINE     | Gibt an, ob Server überkreuz definiert werden sollen. |
| SET SERVERHLADDRESS | Gibt die Adresse der höheren Ebene eines Servers an.  |
| SET SERVERPASSWORD  | Gibt das Serverkennwort an.                           |

## SET SERVERNAME (Servernamen angeben)

---

Mit diesem Befehl kann der Server-Name geändert werden. Wenn Sie den IBM Spectrum Protect-Server installieren, wird der Name bei der Installation auf SERVER1 gesetzt.

Mit dem Befehl QUERY STATUS kann der Servername angezeigt werden.

Wird von ADSM nach IBM Spectrum Protect migriert, wird der Name auf ADSM oder auf den Namen gesetzt, der zuletzt mit dem Befehl SET SERVERNAME in ADSM angegeben wurde.

Wichtig:

- Ist dies ein Quellenserver für eine Operation mit virtuellem Datenträger, kann das Ändern des Namens Auswirkungen auf die Fähigkeit des Quellenservers haben, auf die Daten zuzugreifen und die Daten zu verwalten, die er auf dem entsprechenden Zielserver gespeichert hat.
- Um Probleme bezüglich des Eigentumsrechts für Datenträger zu vermeiden, ändern Sie nicht den Namen eines Servers, wenn er ein Kassettenarchivclient ist.

Wenn Sie den Namen eines Servers ändern, beachten Sie die folgenden zusätzlichen Einschränkungen:

- Windows-Clients identifizieren anhand des Servernamens, welche Kennwörter zu welchen Servern gehören. Wird der Servername geändert, nachdem die Clients die Verbindung hergestellt haben, müssen die Clients die Kennwörter erneut eingeben.
- Sie müssen eindeutige Namen auf Servern definieren, die miteinander kommunizieren. In einem Netz, in dem Clients die Verbindung zu mehreren Servern herstellen, wird empfohlen, dass alle Server eindeutige Namen haben.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-Set SERVERname--Servername-----<<
```

## Parameter

---

Servername (Erforderlich)

Gibt den neuen Server-Namen an. Der Name muss im Servernetz für die unternehmensweite Ereignisprotokollierung, die unternehmensweite Konfiguration die Befehlsweiterleitung oder für virtuelle Datenträger eindeutig sein. Die maximale Länge des Namens beträgt 64 Zeichen.

## Beispiel: Den Server benennen

---

Für den Server soll der Name WELLS\_DESIGN\_DEPT vergeben werden.

```
set servername wells_design_dept
```

## Zugehörige Befehle

---

Tabelle 1. Zugehöriger Befehl für SET SERVERNAME

| Befehl       | Beschreibung   |
|--------------|--|
| QUERY STATUS | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## SET SERVERPASSWORD (Kennwort für Server definieren)

---

Mit diesem Befehl kann das Kennwort für die Kommunikation zwischen Servern definiert werden, um die Unternehmensverwaltung sowie die Protokollierung und Überwachung von Unternehmensereignissen zu unterstützen.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-Set SERVERPAssword--Kennwort-----<<
```

## Parameter

---

Kennwort (Erforderlich)

Gibt ein Kennwort für den Server an. Andere Server müssen dasselbe Kennwort in ihren Definitionen dieses Servers haben.

## Beispiel: Ein Serverkennwort definieren

---

Das Kennwort für HQ\_SERVER auf agave setzen.

```
set serverpassword agave
```

## Zugehörige Befehle

---

Tabelle 1. Zugehöriger Befehl für SET SERVERPASSWORD

| Befehl              | Beschreibung  |
|---------------------|---|
| SET CROSSDEFINE     | Gibt an, ob Server überkreuz definiert werden sollen. |
| SET SERVERHLADDRESS | Gibt die Adresse der höheren Ebene eines Servers an.  |
| SET SERVERLLADDRESS | Gibt die Adresse der unteren Ebene eines Servers an.  |

## SET SPREPLRULEDEFAULT (Serverreplikationsregel für speicherverwaltete Daten definieren)

---

Mit diesem Befehl können Sie die Serverreplikationsregel für speicherverwaltete Daten definieren.

Einschränkung: Die Replikationsregel, die Sie mit diesem Befehl definieren, wird nur angewendet, wenn Dateibereichsregeln und Clientknotenregeln für speicherverwaltete Daten auf DEFAULT gesetzt sind.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Sie können eine Replikationsregel für normale Priorität oder eine Replikationsregel für hohe Priorität angeben. In einem Replikationsprozess, der sowohl Daten mit normaler Priorität als auch Daten mit hoher Priorität einschließt, werden Daten mit hoher Priorität zuerst repliziert. Bevor Sie eine Regel angeben, beachten Sie die Reihenfolge, in der die Daten repliziert werden sollen.

Beispiel: Angenommen, Ihre Clientknoten enthalten speicherverwaltete Daten und Sicherungsdaten. Die Replikation der speicherverwalteten Daten hat eine höhere Priorität als die der Sicherungsdaten. Um die speicherverwalteten Daten zu priorisieren, geben Sie den Befehl SET SPREPLRULEDEFAULT aus und geben Sie die Replikationsregel ALL\_DATA\_HIGH\_PRIORITY an. Um die Sicherungsdaten zu priorisieren, geben Sie den Befehl SET BKREPLRULEDEFAULT aus und geben Sie die Replikationsregel ALL\_DATA für Sicherungsdaten an. Die Regel ALL\_DATA für Sicherungsdaten repliziert Sicherungsdaten mit einer normalen Priorität.

## Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

---

```
>>-Set SPREPLRuledefault--+-ALL_DATA-----+-----><
                        +-ALL_DATA_HIGH_PRIORITY-+
                        '-NONE-----'
```

## Parameter

---

- ALL\_DATA  
Repliziert speicherverwaltete Daten mit einer normalen Priorität.
- ALL\_DATA\_HIGH\_PRIORITY  
Repliziert speicherverwaltete Daten mit einer hohen Priorität.
- NONE  
Speicherverwaltete Daten werden nicht repliziert.

## Beispiel: Die Serverreplikationsregel für speicherverwaltete Daten definieren

---

Die Standardregel für speicherverwaltete Daten so definieren, dass die Replikation mit einer hohen Priorität erfolgt.

```
set spreplruledefault all_data_high_priority
```



## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET BKREPLRULEDEFAULT

| Befehl                | Beschreibung   |
|-----------------------|--|
| QUERY FILESPACE       | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.                                      |
| QUERY NODE            | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.                                    |
| QUERY REPLICATION     | Zeigt Informationen zu Knotenreplikationsprozessen an.   |
| QUERY REPLRULE        | Zeigt Informationen zu Knotenreplikationsregeln an.  |
| QUERY STATUS          | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| REPLICATE NODE        | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |
| SET ARREPLRULEDEFAULT | Gibt die Serverknotenreplikationsregel für Archivierungsdaten an.  |
| SET BKREPLRULEDEFAULT | Gibt die Serverknotenreplikationsregel für Sicherungsdaten an.   |
| UPDATE FILESPACE      | Ändert Knotenreplikationsregeln für Dateibereiche.   |
| UPDATE REPLRULE       | Aktiviert oder inaktiviert Replikationsregeln.   |
| VALIDATE REPLICATION  | Überprüft die Replikation für Dateibereiche und Datentypen.  |

## SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)

Verwenden Sie diesen Befehl, um das Sicherheitsaktivitätsintervall anzupassen, das verwendet wird, wenn der Statusmonitor bewertet, ob Clients gefährdet sind.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>---Set STATUSATRISKINTERVAL--TYPE-----+All-----+----->
                                     +-Applications-+
                                     +-VM-----+
                                     '-Systems-----'

>---Interval---Wert-----><
```

### Parameter

TYPE (Erforderlich)

Gibt den Typ des Clients an, der bewertet werden soll. Geben Sie einen der folgenden Werte an:

ALL

Geben Sie diese Einstellung für alle Clienttypen an.

Applications

Geben Sie diese Einstellung für Anwendungsclients an.

VM

Geben Sie diese Einstellung für VM-Clients an.

Systems

Geben Sie diese Einstellung für Systemclients an.

Interval (Erforderlich)



Speicherpools automatisch so definiert, dass eine Warnung angezeigt wird, wenn der Schwellenwert 80 % erreicht, und ein Fehler angezeigt wird, wenn der Schwellenwert eine Auslastung von 90 % erreicht.

OFF

Gibt an, dass die Statusüberwachung inaktiviert wird. Off ist der Standardwert.

## Statusüberwachung aktivieren

Die Statusüberwachung auf 'On' setzen, um die Statusüberwachung zu aktivieren.

```
set statusmonitor on
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET STATUSMONITOR

| Befehl  | Beschreibung   |
|---|--|
| DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)   | Definiert einen Schwellenwert für die Statusüberwachung.   |
| DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)  | Löscht einen Schwellenwert für die Statusüberwachung.  |
| QUERY MONITORSTATUS (Überwachungsstatus abfragen)   | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                             |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)                                      | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                             |
| QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)   | Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.   |
| SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)        | Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.         |
| SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)   | Gibt das Aktualisierungsintervall für die Statusüberwachung an.  |
| SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll) | Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll. |
| UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)  | Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.   |

## SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)

Mit diesem Befehl können Sie die Anzahl der Minuten zwischen Serverabfragen für die Statusüberwachung angeben.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-Set STATUSREFreshinterval--Minuten-----<<
```

### Parameter

Minuten (Erforderlich)

Gibt die ungefähre Anzahl der Minuten zwischen Serverabfragen für die Statusüberwachung an. Sie können eine ganze Zahl im Bereich von 1 bis 2440 angeben. Der Standardwert ist 5.  
Einschränkungen:

- Definieren Sie in einer Speicherumgebung, die vom Operations Center überwacht wird, dasselbe Aktualisierungsintervall auf dem Hub-Server und den Peripherieservern. Werden verschiedene Intervalle verwendet, kann das Operations Center ungenaue Informationen für die Peripherieserver anzeigen.
- Kurze Statusaktualisierungsintervalle verwenden mehr Speicherbereich in der Serverdatenbank und erfordern möglicherweise mehr Prozessor- und Plattenressourcen. Wird beispielsweise das Intervall um die Hälfte verringert, wird der erforderliche Speicherbereich für die Datenbank und das Archivprotokoll verdoppelt. Lange Intervalle verringern die Aktualität von Operations Center-Daten, sind aber für eine Konfiguration mit einem Netz mit langer Latenzzeit besser geeignet.
- Ein Statusaktualisierungsintervall von weniger als 5 Minuten kann die folgenden Probleme verursachen:
  - Operations Center-Daten, von denen angenommen wird, dass sie nach dem definierten Intervall aktualisiert werden, benötigen eine längere Zeit für ihre Aktualisierung.
  - Operations Center-Daten, von denen angenommen wird, dass sie nahezu unverzüglich nach dem Auftreten einer zugehörigen Änderung in der Speicherumgebung aktualisiert werden, benötigen ebenfalls eine längere Zeit für ihre Aktualisierung.

## Das Aktualisierungsintervall für die Statusüberwachung definieren

Mit dem folgenden Befehl angeben, dass der Serverstatus alle 6 Minuten abgefragt wird:

```
set statusrefreshinterval 6
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET STATUSREFRESHINTERVAL

| Befehl  | Beschreibung   |
|---|--|
| DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)   | Definiert einen Schwellenwert für die Statusüberwachung.   |
| DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)  | Löscht einen Schwellenwert für die Statusüberwachung.  |
| QUERY MONITORSTATUS (Überwachungsstatus abfragen)   | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                             |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)                                      | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                             |
| QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)   | Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.   |
| SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)        | Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.         |
| SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)   | Gibt an, ob die Statusüberwachung aktiviert werden soll.   |
| SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll) | Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll. |
| UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)  | Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.   |

## SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll)

Verwenden Sie diesen Befehl, wenn der Statusmonitor bei der Bewertung des Status für jeden Client Clients als gefährdet ansehen soll.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set STATUSSKIPASFAILURE--+-Yes+----->
                               '-No--'

>--TYPE-----+All-----><
                +-Applications+
                +-VM-----+
                '-Systems-----'
```

## Parameter

### State (Erforderlich)

Gibt an, ob die Überprüfung auf Dateien, die während der letzten Sicherung übersprungen wurden, aktiviert werden soll. Diese Überprüfung zeigt an, dass der Client gefährdet ist, wenn Dateien übersprungen wurden. Clientdaten, die übersprungen oder nicht korrekt gesichert werden, werden als gefährdet angesehen.

#### Yes

Gibt an, dass der Server bewertet, ob ein Client gefährdet ist.

#### No

Gibt an, dass der Server nicht bewertet, ob ein Client gefährdet ist.

### TYPE (Erforderlich)

Gibt den Typ des Clients an, der bewertet werden soll. Geben Sie einen der folgenden Werte an:

#### ALL

Geben Sie diese Einstellung für alle Clienttypen an.

#### Applications

Geben Sie diese Einstellung für Anwendungsclients an.

#### VM

Geben Sie diese Einstellung für VM-Clients an.

#### Systems

Geben Sie diese Einstellung für Systemclients an.

## Überprüfung auf Gefährdung für virtuelle Systeme inaktivieren

Die Überprüfung auf Gefährdung für virtuelle Systeme inaktivieren, indem der folgende Befehl ausgegeben wird:

```
set statusskipasfailure off type=vm
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET STATUSSKIPASFAILURE

| Befehl   | Beschreibung   |
|--|--|
| DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)  | Definiert einen Schwellenwert für die Statusüberwachung.   |
| DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)   | Löscht einen Schwellenwert für die Statusüberwachung.  |
| QUERY MONITORSTATUS (Überwachungsstatus abfragen)  | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                     |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)                               | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                     |
| QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)  | Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.   |
| SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll) | Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll. |
| SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)  | Gibt an, ob die Statusüberwachung aktiviert werden soll.   |
| SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)  | Gibt das Aktualisierungsintervall für die Statusüberwachung an.  |

| Befehl   | Beschreibung   |
|--|--|
| UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren) | Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung. |

## SET SUBFILE (Subdateisicherung für Clientknoten definieren)

Mit diesem Befehl kann der Server so definiert werden, dass er Clients das Sichern von Subdateien erlaubt. Auf der Workstation des Clients müssen die Optionen SUBFILECACHEPATH und SUBFILECACHESIZE in der Clientoptionsdatei (dsm.opt) angegeben werden. Wenn Sie einen Windows-Client verwenden, müssen Sie auch die Option SUBFILEBACKUP angeben.

Wurde eine Clientdatei zuvor bereits gesichert, wird mit einer Subdateisicherung normalerweise der Teil (eine Subdatei) der Clientdatei gesichert, der sich geändert hat, und nicht die gesamte Datei.

Mit dem Befehl QUERY STATUS kann bestimmt werden, ob Subdateien auf dem Server gesichert werden können, der diesen Befehl ausführt.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-Set SUBFILE--+-Client-+-----<
                '-No-----'
```

### Parameter

Client

Gibt an, dass der Client-Knoten bestimmen kann, ob eine Subdateisicherung verwendet werden soll.

No

Gibt an, dass die Subdateisicherungen nicht verwendet werden sollen. Bei der Installation wird dieser Wert auf No gesetzt.

### Beispiel: Subdateisicherung für Clientknoten definieren

Dem Client-Knoten das Sichern von Subdateien auf dem Server erlauben.

```
set subfile client
```

### Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET SUBFILE

| Befehl       | Beschreibung   |
|--------------|--|
| QUERY STATUS | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |

## SET SUMMARYRETENTION (Anzahl Tage für Aufbewahren in Aktivitätsübersichtstabelle definieren)

Mit diesem Befehl kann die Anzahl der Tage angegeben werden, die Informationen in der SQL-Aktivitätsübersichtstabelle aufbewahrt werden sollen.

Die SQL-Aktivitätsübersichtstabelle enthält Statistiken zu allen Client-Sitzungen und Server-Prozessen. Soll eine Beschreibung der Informationen in der SQL-Aktivitätsübersichtstabelle aufgerufen werden, den folgenden Befehl ausgeben:

```
select colname, remarks from columns where tabname='SUMMARY'
```

Den Befehl QUERY STATUS ausgeben, um die Anzahl der Tage anzuzeigen, die die Informationen aufbewahrt werden. Bei der Installation erlaubt IBM Spectrum Protect jedem Server, seine eigene Anzahl Tage für das Aufbewahren von Informationen in der SQL-Aktivitätsübersichtstabelle zu bestimmen.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-Set SUMmaryretention--+-----+-----<<
                          '-Tage-'
```

## Parameter

### Tage

Gibt die Anzahl der Tage an, die Informationen in der Aktivitätsübersichtstabelle aufbewahrt werden sollen. Es kann eine Zahl von 0 bis 9999 angegeben werden. Der Wert 0 gibt an, daß die Informationen in der Aktivitätsübersichtstabelle nicht aufbewahrt werden. Der Wert 1 gibt an, daß die Aktivitätsübersichtstabelle für den aktuellen Tag aufbewahrt wird.

## Beispiel: Die Anzahl der Tage angeben, die Informationen in der SQL-Aktivitätsübersichtstabelle aufbewahrt werden sollen

Angeben, daß der Server die Informationen in der Aktivitätsübersichtstabelle 15 Tage aufbewahrt.

```
set summaryretention 15
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET SUMMARYRETENTION

| Befehl              | Beschreibung   |
|---------------------|--|
| QUERY STATUS        | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| SET ACTLOGRETENTION | Gibt die Anzahl Tage an, die Protokollsätze im Aktivitätenprotokoll aufbewahrt werden sollen.                        |
| QUERY ACTLOG        | Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.   |
| SELECT              | Erlaubt angepasste Abfragen der IBM Spectrum Protect-Datenbank.  |

## SET TAPEALERTMSG (Bandalerts aktivieren oder inaktivieren)

Verwenden Sie diesen Befehl, um es dem IBM Spectrum Protect-Server zu ermöglichen, Hinweise auf Diagnoseinformationen von Kassettenarchiv- und Laufwerkeinheiten zu protokollieren. Bei der Installation wird dieser Wert auf OFF gesetzt. Bei einer Aktivierung kann der Server Diagnoseinformationen aus einer Band- oder Kassettenarchiveneinheit abrufen und mit Hilfe von ANR-Nachrichten anzeigen. Bei einer Inaktivierung fragt der Server eine Einheit nicht nach diesen Informationen ab.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-Set TAPEAlertmsg--+ON--+-----<<
                          '-OFF-'
```

## Parameter

### ON

Gibt an, dass Diagnoseinformationen an den Server gemeldet werden.

### OFF

Gibt an, dass Diagnoseinformationen nicht an den Server gemeldet werden.

## Beispiel: Das Empfangen von Bandalernachrichten aktivieren

Dem Server den Empfang von Diagnoseinformationsnachrichten gestatten.

```
set tapealertmsg on
```

## Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET TAPEALERTMSG

| Befehl             | Beschreibung   |
|--------------------|--|
| QUERY TAPEALERTMSG | Zeigt an, ob der Server Hardwarediagnoseinformationen protokolliert. |

## SET TOCLOADRETENTION (Aufbewahrungszeitraum für Laden für Inhaltsverzeichnis definieren)

Mit diesem Befehl kann die ungefähre Anzahl Minuten angegeben werden, die Inhaltsverzeichnisdaten, auf die nicht verwiesen wird, in der Serverdatenbank geladen bleiben.

Während NDMP-gesteuerter Sicherungsoperationen von NAS-Dateisystemen kann der Server wahlweise Informationen zu Dateien und Verzeichnissen im Image sammeln und diese Informationen in einem Inhaltsverzeichnis innerhalb eines Speicherpools speichern. Mithilfe des Webclients können Dateien und Verzeichnisse in mindestens einem Dateisystemimage untersucht werden. Hierbei werden Einträge aus den Inhaltsverzeichnisdaten angezeigt. Der Server lädt die erforderlichen Inhaltsverzeichnisdaten in eine temporäre Datenbanktabelle.

Nach dem Laden der Daten kann der Benutzer diese Dateien und Verzeichnisse zum Zurückschreiben auswählen. Da diese Datenbanktabelle temporär ist, bleiben die Daten nur über einen bestimmten Zeitraum geladen (gemessen ab dem letzten Verweis auf diese Daten). Bei der Installation wird ein Aufbewahrungszeitraum von 120 Minuten festgelegt. Verwenden Sie den Befehl QUERY STATUS, um den Aufbewahrungszeitraum für das Laden des Inhaltsverzeichnisses anzuzeigen.

## Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie über die Systemberechtigung verfügen.

## Syntax

```
>>-Set TOCLOADRetention--Minuten-----><
```

## Parameter

Minuten (Erforderlich)

Gibt die ungefähre Anzahl der Minuten an, die Inhaltsverzeichnisdaten, auf die nicht verwiesen wird, in der Datenbank aufbewahrt werden. Sie können eine ganze Zahl von 30 bis 1000 angeben.

## Beispiel: Den Aufbewahrungszeitraum für das Laden des Inhaltsverzeichnisses definieren

Geben Sie mit dem Befehl SET TOCLOADRETENTION an, dass Inhaltsverzeichnisdaten, auf die nicht verwiesen wird, 45 Minuten in der Datenbank aufbewahrt werden sollen.

```
set toclodretention 45
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET TOCLOADRETENTION

| Befehl       | Beschreibung   |
|--------------|--|
| QUERY STATUS | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |



# SET VMATRISKINTERVAL (Gibt den Gefährdungsmodus für einen einzelnen VM-Dateibereich an)

Verwenden Sie diesen Befehl, um den Auswertungsmodus für Gefährdung für einen einzelnen VM-Dateibereich anzupassen.

## Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie die Systemberechtigung, die Maßnahmenberechtigung für die Domäne, der der Knoten zugeordnet ist, oder die Clienteignerberechtigung für den Knoten haben.

## Syntax

```
>>---Set VMATRISKINTERVAL--Knotenname--FSID----->
>--TYPE-----+DEFAULT-----+-----><
      +-BYPASSED+  '-Interval-----Wert-'
      '-CUSTOM---'
```

## Parameter

Knotenname (Erforderlich)

Gibt den Namen des zu aktualisierenden Clientknotens an, der Eigner des VM-Dateibereichs ist.

FSID (Erforderlich)

Gibt die Dateibereichs-ID des Clientknotens an, der aktualisiert werden soll.

TYPE (Erforderlich)

Gibt an, welchen Auswertungsmodus für Gefährdung der Statusmonitor verwenden soll, wenn die Gefährdungsklassifizierung für den VM-Dateibereich des angegebenen Knotens ausgewertet wird. Geben Sie einen der folgenden Werte an:

DEFAULT

Gibt an, dass der VM-Dateibereich mit demselben Intervall ausgewertet wird, das für den Befehl SET STATUSATRISKINTERVAL angegeben wurde.

BYPASSED

Gibt an, dass der Gefährdungsstatus für den VM-Dateibereich nicht vom Statusmonitor ausgewertet wird. Der Gefährdungsstatus wird auch an das Operations Center als 'Bypassed' (Übergangen) zurückgemeldet.

CUSTOM

Gibt an, dass der VM-Dateibereich mit dem angegebenen Intervall und nicht mit dem Intervall ausgewertet wird, das für den Befehl SET STATUSATRISKINTERVAL angegeben wurde.

Interval

Gibt die Zeit in Stunden zwischen Clientsicherungsaktivitäten an, bevor der Statusmonitor den Client als gefährdet ansieht. Sie können eine ganze Zahl im Bereich von 6 bis 8808 angeben. Bei TYPE = CUSTOM müssen Sie diesen Parameter angeben. Bei TYPE = BYPASSED oder TYPE = DEFAULT wird dieser Parameter nicht angegeben. Der Intervallwert für alle Clienttypen wird bei der Serverinstallation auf 24 gesetzt.

## Für einen Knotennamen ein angepasstes Gefährdungsintervall von 90 Tagen definieren

Das Gefährdungsintervall für einen Knoten mit dem Namen *charlievm* (Dateibereichs-ID 50) auf dem Datencenterknoten *alice* auf 90 Tage setzen. Mit dem Befehl QUERY FILESPACE kann die Dateibereichs-ID für die virtuelle Maschine bestimmt werden.

```
set vmatriskinterval alice 50 type=custom interval=2160
```

## Die Auswertung für das Gefährdungsintervall übergehen

Die virtuelle Maschine *davevm* (Dateibereichs-ID 213) auf dem Datencenterknoten *erin* von der Überprüfung des Gefährdungsintervalls ausschließen. Mit dem Befehl QUERY FILESPACE kann die Dateibereichs-ID für die virtuelle Maschine *davevm* bestimmt werden. Anschließend die Überprüfung des Gefährdungsintervalls für die virtuelle Maschine auf 'Bypassed' (Übergangen) setzen.

```
set vmatriskinterval erin 213 type=bypassed
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für set vmatriskinterval

| Befehl  | Beschreibung   |
|---|--|
| SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)        | Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.         |
| SET NODEATRISKINTERVAL (Gibt den Gefährdungsmodus für einen einzelnen Knoten an)  | Definiert den Gefährdungsmodus und das Gefährdungsintervall für einen Knoten.  |
| QUERY MONITORSTATUS (Überwachungsstatus abfragen)   | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                             |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)                                      | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                             |
| SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)   | Gibt an, ob die Statusüberwachung aktiviert werden soll.   |
| SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)   | Gibt das Aktualisierungsintervall für die Statusüberwachung an.  |
| SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll) | Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll. |
| QUERY NODE (Knoten abfragen)  | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.  |
| QUERY FILESPACE (Dateibereiche abfragen)  | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.  |

## SETOPT (Serveroption für dynamisches Aktualisieren definieren)

Mit dem Befehl SETOPT können Sie die meisten Serveroptionen dynamisch aktualisieren, ohne den Server zu stoppen und erneut zu starten. Für die Option DBDIAGLOGSIZE müssen Sie den Server stoppen und erneut starten. Ein Befehl SETOPT, der in einem Makro oder in einer Prozedur enthalten ist, kann nicht rückgängig gemacht werden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.


### Syntax

```
>>-SETOPT--Optionsname--Optionswert-----<<
```

### Parameter

Optionsname (Erforderlich)

Gibt eine Zeichenfolge mit Informationen an, die die zu aktualisierende Server-Option identifizieren. Die maximale Länge der Zeichenfolge beträgt 255 Zeichen. Folgende Optionen sind verfügbar:

- ADMINCOMMTIMEOUT
- ADMINIDLETIMEOUT
- ALLOWREORGINDEX
- ALLOWREORGTABLE
- ARCHLOGCOMPRESS
- BACKUPINITIATIONROOT
- CHECKTAPEPOS
- CLIENTDEDUPTXNlimit
- CLIENTDEPLOYCATALOGURL
- CLIENTDEPLOYUSELOCALCATALOG
- COMMTIMEOUT
-  Windows-BetriebssystemeDATEFORMAT
- DBDIAGLOGSIZE
- DBDIAGPATHFSTHRESHOLD
- DEDUPTIER2FILESIZE

- DEDUPTIER3FILESIZE
- DEDUPREQUIRESBACKUP
- DNSLOOKUP
- EXPINterval
- EXPQJiet
- FSUSEDTHreshold
- IDLETimeout
- LDAPCACHEDURATION
- MAXSessions
- MOVEBatchsize
- MOVESizethresh
- NDMPPREFDATAINTERFACE
-  Windows-BetriebssystemeNUMBERFORMAT
- NUMOPENVOLSallowed
- RECLAIMDELAY
- RECLAIMPERIOD
- REORGBEGINTime
- REORGDURation
- RESOURCETimeout
- RESTOREINTERVAL
- RETENTIONEXTENSION
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-BetriebssystemeSANDISCOVERY
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-BetriebssystemeSANREFRESHTIME
- SERVERDEDUPTXNlimit
- SHREDding
-  Windows-BetriebssystemeTCPPOrt
- THROUGHPUTDatathreshold
- THROUGHPUTTimethreshold
-  Windows-BetriebssystemeTIMEFORMAT
- TXNGroupmax

Optionswert (Erforderlich)

Gibt den Wert für die Server-Option an.

## Beispiel: Die maximale Anzahl Clientsitzungen definieren

Die Serveroption für die maximale Anzahl Clientsitzungen mit dem Wert 40 aktualisieren.

```
setopt maxsessions 40
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SETOPT

| Befehl       | Beschreibung   |
|--------------|--|
| QUERY OPTION | Zeigt Informationen über Serveroptionen an.                                |
| QUERY SYSTEM | Zeigt ausführliche Informationen zum IBM Spectrum Protect-Serversystem an. |

## SHRED DATA (Daten schreddern)

Verwenden Sie diesen Befehl, um den Prozess zum Schreddern gelöschter sensibler Daten manuell zu starten. Das manuelle Schreddern ist nur möglich, wenn das automatische Schreddern inaktiviert ist.

Der automatische Schredderprozess kann mit der Serveroption SHREDDING gesteuert werden.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Werden Daten aus einem Speicherpool, der das Schreddern erzwingt, gelöscht, während ein manueller Schredderprozess ausgeführt wird, wird die Löschoption zum aktiven Prozess hinzugefügt.

## Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie über die Systemberechtigung verfügen.

## Syntax

```

                                     .-Wait---No-----
>>-SHRED DATA-----+-----+-----+-----+----->
      '-Duration---Minuten-'   '-Wait---+No---+'
                                     '-Yes-'

.-IOERROR---SHREDFailure-----
>-----+-----+-----+-----+-----<
      '-IOERROR---+SHREDFailure-+'
      '-SHREDSuccess-'
```

## Parameter

### DURATION

Gibt die maximale Anzahl Minuten an, die der Schredderprozess ausgeführt wird, bevor er automatisch abgebrochen wird. Wenn die angegebene Anzahl Minuten verstrichen ist, bricht der Server den Schredderprozess ab. Sobald der Prozess den Abbruch erkennt, wird er beendet. Daher kann der Prozess länger dauern als mit dem Wert für diesen Parameter angegeben ist. Es kann eine Zahl von 1 bis 9999 angegeben werden. Dieser Parameter ist wahlfrei. Falls nicht angegeben, stoppt der Server erst dann, nachdem alle gelöschten sensiblen Daten geschreddert wurden.

### Wait



Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

#### No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Bei dem Hintergrundprozess erstellte Nachrichten werden im Aktivitätenprotokoll und/oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden. Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird dieser Prozess abgebrochen, wurden möglicherweise einige Dateien bereits vor dem Abbruch geschreddert. Dies ist der Standardwert.

#### Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Die Operation muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dem Verwaltungsclient an, wenn die Operation beendet ist. Nachrichten werden auch im Aktivitätenprotokoll und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.

  Anmerkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

### IOERROR

Gibt an, ob beim Auftreten eines E/A-Fehlers während des Schredderns der Daten das Schreddern als erfolgreich betrachtet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist SHREDFAILURE. Gültige Werte:

#### SHREDFailure

Gibt an, dass die Daten als nicht erfolgreich geschreddert angesehen werden, wenn der Server einen E/A-Fehler während des Schredderns entdeckt, und die Datei, die die Daten enthält, wird als beschädigt markiert. Der Server versucht die Daten bei der nächsten Ausführung des Schredderprozesses erneut zu schreddern. Damit haben Sie die Möglichkeit, den Fehler zu korrigieren und sicherzustellen, dass die Daten ordnungsgemäß geschreddert werden können.

#### SHREDSuccess

Gibt an, dass die Daten als erfolgreich geschreddert angesehen werden, wenn der Server während des Schredderns einen E/A-Fehler entdeckt und die Datei, die die Daten enthält, zuvor als beschädigt markiert wurde. Sie sollten diese Option nur verwenden, wenn der Server während des Schredderns E/A-Fehler zurückgemeldet hat und Sie den Fehler nicht korrigieren können.

## Beispiel: Daten schreddern

Das Schreddern aller gelöschten sensiblen Daten manuell starten. Den Prozess bis zu sechs Stunden ausführen, bevor er automatisch abgebrochen wird.

```
shred data duration=360
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SHRED DATA

| Befehl            | Beschreibung  |
|-------------------|---|
| CANCEL PROCESS    | Bricht einen Serverhintergrundprozess ab.                       |
| QUERY PROCESS     | Zeigt Informationen über Hintergrundprozesse an.                |
| QUERY SHREDSTATUS | Zeigt Informationen zu Daten an, die auf das Schreddern warten. |

## SUSPEND EXPORT (Momentan aktive Exportoperation aussetzen)

Mit diesem Befehl können Sie eine momentan aktive Exportoperation zwischen Servern aussetzen, die einen anderen FILEDATA-Wert als NONE hat. Die Exportoperation, die ausgesetzt werden soll, muss nach der Initialisierungsphase liegen, um für die Aussetzung ausgewählt werden zu können. Der Status der Exportoperation wird gespeichert. Die Operation kann mit dem Befehl RESTART EXPORT erneut gestartet werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung erforderlich.

### Syntax

```
>>-SUSPend EXPORT .-*-----+-----><
                    +-----+-----><
                    '---Export-ID---'
```

### Parameter

#### EXPORTIDentifier

Dieser optionale Parameter gibt den Namen der Exportoperation an. Der Name kann mit dem Befehl QUERY EXPORT ermittelt werden, der alle momentan aktiven Exportoperationen zwischen Servern, die ausgesetzt werden können, auflistet. Es kann auch das Platzhalterzeichen verwendet werden, um den Namen anzugeben.

### Beispiel: Eine bestimmte Exportoperation aussetzen

Die aktive Exportoperation EXPORTALLACCTNODES aussetzen. Es wird keine Ausgabe generiert, wenn Sie den Befehl SUSPEND EXPORT ausgeben. Sie müssen den Befehl QUERY EXPORT ausgeben, um zu überprüfen, ob die Operation EXPORTALLACCTNODES ausgesetzt ist.

```
suspend export exportallacctnodes
```

### Beispiel: Alle aktiven Exportoperationen aussetzen

Alle Exportoperationen mit dem Status AKTIV aussetzen.

```
suspend export *
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SUSPEND EXPORT

| Befehl         | Beschreibung  |
|----------------|---|
| CANCEL EXPORT  | Löscht eine ausgesetzte Exportoperation.  |
| EXPORT NODE    | Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.                       |
| EXPORT SERVER  | Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server. |
| QUERY EXPORT   | Zeigt die Exportoperationen an, die gerade aktiv oder ausgesetzt sind.  |
| RESTART EXPORT | Startet eine ausgesetzte Exportoperation erneut.  |

## UNLOCK-Befehle

---

Verwenden Sie die UNLOCK-Befehle, um den Zugriff erneut einzurichten, nachdem ein Objekt gesperrt wurde.

- UNLOCK ADMIN (Sperrung für einen Administrator aufheben)
- UNLOCK NODE (Clientknoten freigeben)
- UNLOCK PROFILE (Profil freigeben)

## UNLOCK ADMIN (Sperrung für einen Administrator aufheben)

---

Verwenden Sie den Befehl UNLOCK ADMIN, um es einem gesperrten Administrator zu ermöglichen, wieder auf den Server zuzugreifen. Sie können auch mehrere Administratoren entsperren, die sich mit derselben Methode authentifizieren.

### Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

---

```
>>-UNLOCK Admin--+*-----+--+-----+<<
      '-Administratorname-' '-AUTHentication--===+Local--'
                                   '-LDap--'
```

### Parameter

---

Administratorname (Erforderlich)

Gibt den Namen des Administrators an, der entsperrt werden soll. Sie können Platzhalterzeichen verwenden, um den Administratornamen anzugeben. Sie müssen keinen Administratornamen eingeben, wenn alle Administratoren gemäß ihrer Authentifizierungsmethode entsperrt werden sollen. Verwenden Sie das Platzhalterzeichen mit einer Authentifizierungsmethode, um mehrere Administratoren zu entsperren. Der Parameter ist erforderlich (kein Standardplatzhalterzeichen).

AUTHentication

Gibt die Methode der Kennwortauthentifizierung an, die für einen Administrator zur Anmeldung erforderlich ist.

Local

Gibt an, dass Sie Administrator-IDs entsperren möchten, die Kennwörter mit dem IBM Spectrum Protect-Server authentifizieren.

LDap

Gibt an, dass Sie Administrator-IDs entsperren möchten, die Kennwörter mit einem LDAP-Verzeichnissever authentifizieren.

### Beispiel: Eine Administrator-ID entsperren

---

Der Administrator-ID JOE wird momentan der Zugriff auf IBM Spectrum Protect verweigert. JOE erlauben, auf den Server zuzugreifen. Geben Sie den folgenden Befehl aus:

```
unlock admin joe
```

### Beispiel: Alle Administrator-IDs entsperren, die Kennwörter mit einem LDAP-Verzeichnissever authentifizieren

---

Die Administrator-IDs, die Kennwörter verwenden, die mit einem LDAP-Verzeichnissever authentifiziert werden, müssen entsperrt werden, damit die IDs mit dem IBM Spectrum Protect-Server kommunizieren können.

```
unlock admin * authentication=ldap
```

### Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für UNLOCK ADMIN

| Befehl     | Beschreibung   |
|------------|--|
| LOCK ADMIN | Verweigert einem Administrator den Zugriff auf IBM Spectrum Protect. |

| Befehl      | Beschreibung   |
|-------------|--|
| QUERY ADMIN | Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an. |

## UNLOCK NODE (Clientknoten freigeben)

Mit diesem Befehl kann einem gesperrten Clientknoten wieder der Zugriff auf den Server ermöglicht werden. Sie können auch mehrere Knoten entsperren, die dieselbe Methode der Authentifizierung verwenden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, der der Clientknoten zugeordnet ist.

### Syntax

```
>>-UNLOCK Node--+-*-----+-----+-----+-----+>>
                '-Knotenname-'  '-AUTHentication-----+LOCAL+-'
                                '-LDap--'
```

### Parameter

Knotenname (Erforderlich)

Gibt den Namen des Clientknotens an, der entsperrt werden soll. Es können Platzhalterzeichen verwendet werden, um den Knotennamen anzugeben. Sie müssen keinen Knotennamen eingeben, wenn alle Knoten gemäß ihrer Authentifizierungsmethode entsperrt werden sollen. Verwenden Sie das Platzhalterzeichen mit einer Authentifizierungsmethode, um Gruppen von Knoten zu entsperren. Der Parameter ist erforderlich. Es ist kein Standardplatzhalterzeichen verfügbar.

AUTHentication

Gibt die Kennwortauthentifizierungsmethode für den Knoten an. Dieser Parameter ist wahlfrei.

Local

Gibt an, dass Sie Knoten entsperren möchten, die Kennwörter mit dem IBM Spectrum Protect-Server authentifizieren.

LDap

Gibt an, dass Sie Knoten entsperren möchten, die Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren.

### Beispiel: Einen Knoten entsperren

Dem Clientknoten SMITH wird momentan der Zugriff auf IBM Spectrum Protect verweigert. SMITH erlauben, auf den Server zuzugreifen.

```
unlock node smith
```

### Beispiel: Alle Knoten entsperren, die sich mit dem IBM Spectrum Protect-Server authentifizieren

Die Knoten, die keine Kennwörter mit LDAP-Verzeichnisservern authentifizieren, müssen entsperrt werden.

```
unlock node * authentication=local
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UNLOCK NODE

| Befehl     | Beschreibung  |
|------------|---|
| LOCK NODE  | Verhindert, dass ein Client auf den Server zugreift.                              |
| QUERY NODE | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an. |

## UNLOCK PROFILE (Profil freigeben)

Mit diesem Befehl kann auf einem Konfigurationsmanager ein Konfigurationsprofil freigegeben werden, damit es an subscribierende verwaltete Server verteilt werden kann.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-UNLOCK PROFILE--Profilname-----<<
```

## Parameter

Profilname (Erforderlich)

Gibt das Profil an, das freigegeben werden soll. Es können Platzhalterzeichen verwendet werden, um mehrere Namen anzugeben.

## Beispiel: Ein Profil entsperren

Das Profil TOM entsperren.

```
unlock profile tom
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UNLOCK PROFILE

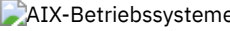
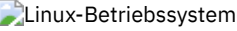
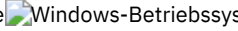
| Befehl                 | Beschreibung  |
|------------------------|---|
| COPY PROFILE           | Erstellt eine Kopie eines Profils.  |
| DEFINE PROFASSOCIATION | Ordnet Objekte einem Profil zu.   |
| DEFINE PROFILE         | Definiert ein Profil für die Verteilung von Informationen an verwaltete Server. |
| DELETE PROFASSOCIATION | Löscht die Zuordnung zwischen einem Objekt und einem Profil.                    |
| DELETE PROFILE         | Löscht ein Profil aus einem Konfigurationsmanager.                              |
| LOCK PROFILE           | Verhindert die Verteilung eines Konfigurationsprofils.                          |
| QUERY PROFILE          | Zeigt Informationen über Konfigurationsprofile an.                              |
| SET CONFIGMANAGER      | Gibt an, ob ein Server ein Konfigurationsmanager ist.                           |
| UPDATE PROFILE         | Ändert die Beschreibung eines Profils.  |

## UPDATE-Befehle

Mit den UPDATE-Befehlen können ein oder mehrere Attribute eines vorhandenen IBM Spectrum Protect-Objekts geändert werden.

- UPDATE ADMIN (Administrator aktualisieren)
- UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)
- UPDATE ALERTSTATUS (Status eines Alert aktualisieren)
- UPDATE BACKUPSET (Aufbewahrungszeitraum einer Sicherungsgruppe aktualisieren)
- UPDATE CLIENTOPT (Folgennummer einer Clientoption aktualisieren)
- UPDATE CLOPTSET (Beschreibung einer Clientoptionsgruppe aktualisieren)
- UPDATE COLLOGROUP (Kollokationsgruppe aktualisieren)
- UPDATE COPYGROUP (Kopiengruppe aktualisieren)
- UPDATE DATAMOVER (Einheit zum Versetzen von Daten aktualisieren)
- UPDATE DEVCLASS (Attribute einer Einheitenklasse aktualisieren)
- UPDATE DOMAIN (Maßnahmendomäne aktualisieren)
- UPDATE DRIVE (Laufwerk aktualisieren)
- UPDATE FILESPACE (Knotenreplikationsregeln für Dateibereich aktualisieren)
- UPDATE LIBRARY (Kassettenarchiv aktualisieren)
- UPDATE LIBVOLUME (Status eines Speicherdatenträgers ändern)
- UPDATE MACHINE (Maschineninformationen aktualisieren)
- UPDATE MGMTCLASS (Verwaltungsklasse aktualisieren)
- UPDATE NODE (Attribute eines Knotens aktualisieren)
- UPDATE NODEGROUP (Knotengruppe aktualisieren)



- UPDATE PATH (Pfad ändern)
- UPDATE POLICYSET (Beschreibung einer Maßnahmengruppe aktualisieren)
- UPDATE PROFILE (Profilbeschreibung aktualisieren)
- UPDATE RECOVERYMEDIA (Wiederherstellungsdatenträger aktualisieren)
- UPDATE REPLRULE (Replikationsregeln aktualisieren)
- UPDATE SCHEDULE (Zeitplan aktualisieren)
- UPDATE SCRIPT (IBM Spectrum Protect-Prozedur aktualisieren)
- UPDATE SERVER (Server aktualisieren, der für die Übertragung zwischen Servern definiert ist)
- UPDATE SERVERGROUP (Beschreibung einer Servergruppe aktualisieren)
- UPDATE SPACETRIGGER (Speicherbereichsauslöser aktualisieren)
- UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)
- UPDATE STGRULE (Speicherregel für einen oder mehrere Speicherpools aktualisieren)
- UPDATE STGPPOOL (Speicherpool aktualisieren)
-    UPDATE STGPOOLDIRECTORY (Speicherpoolverzeichnis aktualisieren)
- UPDATE VIRTUALSMAPPING (Zuordnung eines virtuellen Dateibereichs aktualisieren)
- UPDATE VOLHISTORY (History-Daten für sequentielle Datenträger aktualisieren)
- UPDATE VOLUME (Speicherpooldatenträger ändern)

## UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)

Verwenden Sie diesen Befehl, um die Attribute eines oder mehrerer Alertauslöser zu aktualisieren.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```

      .-,------.
      v          |
>>-UPDate ALERTTrigger---+-Nachrichtennummer-+----->

      .-CAteGory---SErver-----.
>-+-----+-----+-----+-----+----->
      '-CAteGory---+-ApPlication--'
              +-INventory---+
              +-CLient-----+
              +-DEvice-----+
              +-SErver-----+
              +-STorage-----+
              +-SYstem-----+
              '-VMcliEnt----'

>-+-----+-----+-----+-----+-----+-----+-----><
      |               .-,------. | |               .-,------. | |
      |               v          | |               v          | |
      '-ADDAdmin---Administratorname-+' '-DELAdmin---Administratorname-+'

```

### Parameter

#### Nachrichtennummer (Erforderlich)

Gibt die Nachrichtennummer an, die dem Alertauslöser zugeordnet werden soll. Geben Sie mehrere Nachrichtennummern durch Kommas getrennt und ohne Leerzeichen an. Nachrichtennummern haben eine maximale Länge von acht Zeichen.

#### CATeGory

Gibt den Kategorietyt für den Alert an, der durch die Nachrichtentypen bestimmt wird. Der Standardwert ist SERVER.

Anmerkung: Wenn Sie die Kategorie eines Alertauslösers ändern, wird die Kategorie von vorhandenen Alerts auf dem Server nicht geändert. Neue Alerts werden mit der neuen Kategorie kategorisiert.

Geben Sie einen der folgenden Werte an:

#### ApPlication

Der Alert wird als Anwendungskategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Anwendungsclients (TDP) zugeordnet sind.

#### INventory

Der Alert wird als Bestandskategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die der Datenbank, der aktiven Protokolldatei oder der Archivprotokolldatei zugeordnet sind.

#### Client

Der Alert wird als Clientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die allgemeinen Clientaktivitäten zugeordnet sind.

#### DEvice

Der Alert wird als Einheitenkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Einheitenklassen, Kassettenarchiven, Laufwerken oder Pfaden zugeordnet sind.

#### SErver

Der Alert wird als allgemeine Serverkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die allgemeinen Serveraktivitäten oder -ereignissen zugeordnet sind.

#### STorage

Der Alert wird als Speicherkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Speicherpools zugeordnet sind.

#### SYstems

Der Alert wird als Systemclientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Systemsicherungs- und -archivierungsclients oder HSM-Clients zugeordnet sind.

#### VMclient

Der Alert wird als VM-Clientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die VM-Clients zugeordnet sind.

#### ADmin

Dieser optionale Parameter gibt den Namen des Administrators an, der eine E-Mail-Benachrichtigung über diesen Alert empfängt. Der Alertauslöser wird erfolgreich definiert, auch wenn keine Administratornamen angegeben werden.

#### ADDadmin

Gibt den Namen des Administrators an, der der Liste der Administratoren hinzugefügt werden soll, die E-Mail-Alerts empfangen. Geben Sie mehrere Administratornamen durch Kommas getrennt und ohne Leerzeichen an.

#### DELadmin

Gibt den Namen des Administrators an, der aus der Liste der Administratoren gelöscht werden soll, die E-Mail-Alerts empfangen. Geben Sie mehrere Administratornamen durch Kommas getrennt und ohne Leerzeichen an.

## Alertauslöser aktualisieren

Mit dem folgenden Befehl die Namen der Administratoren hinzufügen, die beim Auftreten der Alerts ANR1073E und ANR1074E benachrichtigt werden möchten, und den Namen eines Administrators löschen, der nicht mehr benachrichtigt werden möchte:

```
update alerttrigger ANR1073E,ANR1074E ADDadmin=djee,cdawson,mhaye deladmin=harryh
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE ALERTTRIGGER

| Befehl   | Beschreibung   |
|--|--|
| DEFINE ALERTTRIGGER (Alertauslöser definieren)   | Ordnet angegebene Nachrichten einem Alertauslöser zu.  |
| DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)  | Entfernt eine Nachrichtennummer, die einen Alert auslösen kann.                                  |
| QUERY ALERTSTATUS (Status eines Alert abfragen)  | Zeigt Informationen zu Alerts an, die auf dem Server ausgegeben wurden.                          |
| QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)  | Zeigt Nachrichtennummern an, die einen Alert auslösen.   |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen) | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an. |
| UPDATE ALERTSTATUS (Status eines Alert aktualisieren)  | Aktualisiert den Status eines zurückgemeldeten Alert.  |

## UPDATE ALERTSTATUS (Status eines Alert aktualisieren)

Mit diesem Befehl kann der Status eines zurückgemeldeten Alert aktualisiert werden.

## Berechtigungsstufe

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

```
      .-|-----|
      V      |
>>-UPDate ALERTStatus-----Alert-ID----->
>--+-----+-----+-----+----->
  '-Status-----+Inactive-+-' '-ASSigned-----Text-'
      '-Closed---'
>--+-----+-----+-----+-----><
  '-RESolvedby-----Text-' '-REMark-----Text-'
```

## Parameter

### Alert-ID (Erforderlich)

Gibt den Alert an, der aktualisiert werden soll. Es können mehrere Nachrichtennummern angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden.

### Status

Gibt den Statustyp an, der aktualisiert werden soll. Alerts können von 'aktiv' in 'inaktiv' oder 'geschlossen' oder von 'inaktiv' in 'geschlossen' geändert werden. Gültige Werte:

#### Inactive

Aktive Alerts können in den Status 'inaktiv' geändert werden.

#### Closed

Aktive und inaktive Alerts können in den Status 'geschlossen' geändert werden.

### ASSigned

Gibt den Namen des Administrators an, dem der Alert zugeordnet ist, der abgefragt werden soll.

### RESolvedby

Gibt den Namen des Administrators an, der den Alert behoben hat, der abgefragt werden soll.

### REMark

Dieser Parameter gibt Begleittext an. Der Begleittext darf 255 Zeichen nicht überschreiten. Enthält die Beschreibung Leerzeichen, schließen Sie den gesamten Text in Anführungszeichen (") ein. Entfernen Sie zuvor definierten Text, indem Sie eine leere Zeichenfolge (") für diesen Wert angeben.

## Den Begleittext in einem Alert aktualisieren

Den folgenden Befehl ausgeben, um den Begleittext für die Alert-ID-Nummer 25 zu aktualisieren und anzugeben, dass *DJADMIN* den Alert bearbeitet:

```
update alertstatus 25 assigned=DJADMIN
```

## Alertstatus aktualisieren

Den folgenden Befehl ausgeben, um die Alert-ID-Nummer 72 in den Status 'geschlossen' zu ändern und einen Kommentar hinzuzufügen, wie der Alert behoben wurde:

```
update alertstatus 72 status=closed remark="Dateisystem für die aktive Protokolldatei
wurde vergrößert"
```

## Zugehörige Befehle


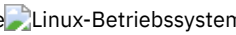
Tabelle 1. Zugehörige Befehle für UPDATE ALERTSTATUS

| Befehl  | Beschreibung  |
|---|---|
| DEFINE ALERTTRIGGER (Alertauslöser definieren)                    | Ordnet angegebene Nachrichten einem Alertauslöser zu.                   |
| DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen) | Entfernt eine Nachrichtennummer, die einen Alert auslösen kann.         |
| QUERY ALERTSTATUS (Status eines Alert abfragen)                   | Zeigt Informationen zu Alerts an, die auf dem Server ausgegeben wurden. |
| QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen) | Zeigt Nachrichtennummern an, die einen Alert auslösen.                  |

| Befehl   | Beschreibung   |
|--|--|
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen) | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an. |
| UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)  | Aktualisiert die Attribute eines oder mehrerer Alertauslöser.                                    |

## UPDATE ADMIN (Administrator aktualisieren)

Dieser Befehl ermöglicht es, das Kennwort oder Kontaktinformationen für einen Administrator zu ändern. Der Administratorname SERVER\_CONSOLE kann jedoch nicht aktualisiert werden.

  Kennwörter für Administratoren müssen nach gewisser Zeit geändert werden, die durch den Befehl SET PASSEXP festgelegt wird. Der Befehl SET PASSEXP hat keine Auswirkungen auf Kennwörter, die sich mit einem Lightweight Directory Access Protocol-Server (LDAP-Server) authentifizieren.

Einschränkung: Die Authentifizierungsmethode für Ihre eigene Benutzer-ID kann nicht aktualisiert werden. Falls erforderlich, muss ein anderer Administrator diese Änderung vornehmen. Außerdem können Sie bei der Aktualisierung eines Kennworts mit dem Befehl UPDATE ADMIN kein Platzhalterzeichen beim Parameter `Administratorname` verwenden.

Administratoren mit dem Namen eines Knotens können während der Ausführung eines Befehls REGISTER NODE erstellt werden. Damit der Knoten und der Administrator mit demselben Namen synchronisiert bleiben, werden die Authentifizierungsmethode und die Einstellung für SSLREQUIRED für den Knoten aktualisiert, damit sie mit dem Administrator übereinstimmen. Wird die Authentifizierungsmethode des Administrators von LOCAL in LDAP geändert und wird kein Kennwort bereitgestellt, wird der Knoten in den Status "LDAP (künftig)" versetzt. Ein Kennwort wird dann bei der nächsten Anmeldung angefordert. Kennwörter zwischen Knoten und Administratoren mit denselben Namen bleiben bei jeder Authentifizierungsänderung synchron.

Sie müssen den Befehl RENAME ADMIN verwenden, um den Namen eines registrierten Administrators zu ändern.

Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol):

- Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.
- Falls eine Benutzer-ID mit Administratorberechtigung mit einem Knotennamen übereinstimmt, dürfen Sie die Authentifizierungsmethode nicht in LDAP aktualisieren. Andernfalls stellen Sie möglicherweise ein nicht erwartetes Verhalten fest, weil automatische Kennwortänderungen dasselbe Kennwort zweimal aktualisieren. Dies hat zur Folge, dass das Kennwort für die Benutzer-ID mit Administratorberechtigung unbekannt ist. Es kann aber auch vorkommen, dass die Kennwortaktualisierungsoperation fehlschlägt.

## Berechtigungsklasse

Zum Ändern des Kennworts oder der Kontaktinformationen eines anderen Administrators ist für diesen Befehl die Systemberechtigung erforderlich. Jeder Administrator kann diesen Befehl ausgeben, um sein Kennwort bzw. seine Kontaktinformationen zu aktualisieren.

## Syntax

```

>>-UPdate Admin-----Administratorname-----+-----+----->
                                     '-Kennwort-'
>-+-----+-----+-----+-----+-----+-----+----->
   '-PASSExp-----Tage-'   '-CONtact-----Text-'
>-+-----+-----+-----+-----+-----+-----+----->
   '-FORCEPwreset-----+No--+-'
                               '-Yes-'
>-+-----+-----+-----+-----+-----+-----+----->
   '-EMAILAddress-----Benutzer-ID@Knoten-'
>-+-----+-----+-----+-----+-----+-----+----->
   |                                     (3)                                     |
   |                                     .-SYNCldapdelete-----No--.         |
   '-AUTHentication-----+LOcal+-----+-----+-----+-----+-----+-----+----->
                               '-LDap--'   '-SYNCldapdelete-----+Yes--+-'
                                               '-No--'
>-+-----+-----+-----+-----+-----+-----+----->

```

```

|          (4)          |
|'-SSLrequired-----+Yes-----+'
|          +-No-----+
|          '-Default-'
|
.-SESSIONSECurity----TRANSitional----.
>-----+----->
|'-SESSIONSECurity----+STRict-----+'
|          '-TRANSitional-'
|
>-----+-----<
|'-ALert-----+Yes-+-'
|          '-No--'

```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.
2. Kennwörter sind bei diesem Befehl optional, wenn Sie nicht die Authentifizierungsmethode von LDAP in LOCAL ändern möchten.
3. Der Parameter SYNCldapdelete gilt nur, wenn ein Administrator, der sich mit einem LDAP-Verzeichnissever authentifiziert, zur lokalen Authentifizierung zurückkehrt.
4. Der Parameter SSLREQUIRED ist veraltet.

## Parameter

Administratorname (Erforderlich)

Gibt den Namen des Administrators an, der aktualisiert werden soll.

Kennwort

Gibt das Kennwort des Administrators an. Dieser Parameter ist in den meisten Fällen optional. Wenn die Authentifizierungsmethode des Administrators von LDAP in LOCAL geändert wird, ist ein Kennwort erforderlich. Wenn ein LDAP-Server für die Authentifizierung von Administratoren verwendet wird, geben Sie bei Verwendung des Befehls UPDATE ADMIN kein Kennwort an.

PASSExp

Gibt die Anzahl der Tage an, die das Kennwort gültig ist. Für die Kennwortablaufdauer kann ein Wert im Bereich von 0 bis 9999 definiert werden. Der Wert 0 bedeutet, dass das Kennwort niemals abläuft. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, wird die Kennwortablaufdauer nicht geändert. Dieser Parameter gilt nicht für Kennwörter, die auf einem LDAP-Verzeichnissever gespeichert werden.

CONtact

Gibt eine Zeichenfolge an, die den Administrator kennzeichnet. Dieser Parameter ist wahlfrei. Die Zeichenfolge in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Sollen zuvor definierte Kontaktinformationen entfernt werden, geben Sie eine Nullzeichenfolge ("" ) an.

FORCEPwreset

Gibt an, ob der Administrator das Kennwort ändern oder zurücksetzen muss. Dieser Parameter ist wahlfrei. Gültige Werte:

No

Gibt an, dass der Administrator bei dem Versuch, sich beim Server anzumelden, das Kennwort nicht ändern bzw. zurücksetzen muss. Die Kennwortablaufdauer wird mit dem Befehl SET PASSEXP definiert.

Yes

Gibt an, dass das Kennwort des Administrators bei der nächsten Anmeldung abläuft. Der Administrator muss das Kennwort dann ändern oder zurücksetzen. Wenn kein Kennwort angegeben wird, wird ein Syntaxfehler empfangen.

Einschränkungen:

- Für Benutzer-IDs mit Administratorberechtigung, die mit einem LDAP-Server authentifiziert werden, wird der Kennwortablauf mithilfe von LDAP-Serverdienstprogrammen definiert. Geben Sie daher nicht FORCEPWRESET=YES an, wenn AUTHENTICATION=LDAP angegeben werden soll.
- Soll eine Benutzer-ID mit Administratorberechtigung für die Authentifizierung mit einem LDAP-Server aktualisiert werden, und haben Sie FORCEPWRESET=YES angegeben, müssen Sie das Kennwort ändern, bevor Sie FORCEPWRESET=NO und AUTHENTICATION=LDAP angeben können.

EMAILAddress

Dieser Parameter wird für zusätzliche Kontaktinformationen verwendet. Die mit diesem Parameter angegebenen Informationen werden von IBM Spectrum Protect nicht verwendet.

AUTHentication

Dieser Parameter bestimmt die Kennwortauthentifizierungsmethode, die von der Administrator-ID verwendet wird (LDAP oder LOCAL).

Local

Gibt an, dass der Administrator die lokale IBM Spectrum Protect-Serverdatenbank verwendet, um Kennwörter für die Authentifizierung zu speichern.

LDap

Gibt an, dass der Administrator einen LDAP-Verzeichnisserver für die Kennwortauthentifizierung verwendet.

SYNCLdapdelete

Dieser Parameter gilt nur, wenn ein Administrator, der sich mit einem LDAP-Server authentifiziert, zur lokalen Authentifizierung zurückkehren möchte.

Yes

Gibt an, dass der Administrator vom LDAP-Server gelöscht wird.

Einschränkung: Sie dürfen nicht den Wert YES angeben. (Der Wert YES ist nur für die Benutzer der vorherigen LDAP-Authentifizierungsmethode gültig, die in Kennwörter und Anmeldeverfahren verwaltet beschrieben wird.)

No

Gibt an, dass der Administrator nicht vom LDAP-Server gelöscht wird. Dies ist der Standardwert.

SSLrequired (veraltet)

Gibt an, ob die Administrator-ID das Protokoll Secure Sockets Layer (SSL) für die Kommunikation zwischen dem IBM Spectrum Protect-Server und dem Client für Sichern/Archivieren verwenden muss. Wenn Sie Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren, müssen Sie die Sitzungen mit SSL oder einer anderen Netzsicherheitsmethode schützen.

Wichtig: Ab IBM Spectrum Protect Version 8.1.2 und Tivoli Storage Manager Version 7.1.8 wird dieser Parameter nicht mehr verwendet. Die durch diesen Parameter aktivierte Validierung wird durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter SESSIONSECURITY durchgesetzt wird. Der Parameter SSLREQUIRED wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

SESSIONSECURITY

Gibt an, ob der Administrator die sichersten Einstellungen verwenden muss, um mit einem IBM Spectrum Protect-Server zu kommunizieren. Dieser Parameter ist wahlfrei.

Sie können einen der folgenden Werte angeben:

STRICT

Gibt an, dass die striktesten Sicherheitseinstellungen für den Administrator durchgesetzt werden. Der Wert STRICT verwendet das sicherste Kommunikationsprotokoll, das verfügbar ist. Dies ist derzeit TLS 1.2. Das TLS 1.2-Protokoll wird für SSL-Sitzungen zwischen dem Server und dem Administrator verwendet. Um anzugeben, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, lesen Sie die Informationen zur Clientoption SSL. Für die Verwendung des Werts STRICT müssen die folgenden Anforderungen erfüllt werden, um sicherzustellen, dass sich der Administrator mit dem Server authentifizieren kann:

- Der Administrator und der Server müssen IBM Spectrum Protect-Software verwenden, die den Parameter SESSIONSECURITY unterstützt.
- Der Administrator muss für die Verwendung des TLS 1.2-Protokolls für SSL-Sitzungen zwischen dem Server und dem Administrator konfiguriert werden.

Administratoren, für die der Wert STRICT definiert ist und die diese Anforderungen nicht erfüllen, können sich nicht mit dem Server authentifizieren.

TRANSITIONAL

Gibt an, dass die vorhandenen Sicherheitseinstellungen für den Administrator durchgesetzt werden. Dies ist der Standardwert. Dieser Wert ist für die temporäre Verwendung bestimmt, während Sie Ihre Sicherheitseinstellungen aktualisieren, um die Anforderungen für den Wert STRICT zu erfüllen.

Ist SESSIONSECURITY=TRANSITIONAL definiert und hat der Administrator nie die Anforderungen für den Wert STRICT erfüllt, authentifiziert sich der Administrator weiterhin mithilfe des Werts TRANSITIONAL. Wenn ein Administrator jedoch die Anforderungen für den Wert STRICT erfüllt, wird der Wert des Parameters SESSIONSECURITY automatisch von TRANSITIONAL in STRICT aktualisiert. Der Administrator kann sich dann nicht mehr mit einer Version des Clients oder mit einem SSL/TLS-Protokoll authentifizieren, die bzw. das die Anforderungen für STRICT nicht erfüllt. Nachdem sich ein Administrator erfolgreich mit einem Kommunikationsprotokoll authentifiziert hat, das mehr Sicherheit bietet, kann sich der Administrator nicht mehr mit einem weniger sicheren Protokoll authentifizieren. Beispiel: Wenn ein Administrator, der nicht SSL verwendet, aktualisiert wird und sich mithilfe von TLS 1.2 erfolgreich authentifiziert, kann sich der Administrator nicht mehr ohne SSL-Protokoll oder mithilfe von TLS 1.1 authentifizieren. Diese Einschränkung gilt auch bei Verwendung von Funktionen wie z. B. Befehlsweiterleitung oder Export zwischen Servern, wenn sich der Administrator beim IBM Spectrum Protect-Server als Administrator von einem anderen Server authentifiziert.

ALert

Gibt an, ob Alerts an die E-Mail-Adresse eines Administrators gesendet werden.

Yes

- No
    - Gibt an, dass Alerts an die E-Mail-Adresse des angegebenen Administrators gesendet werden.
    - Gibt an, dass Alerts nicht an die E-Mail-Adresse des angegebenen Administrators gesendet werden. Dies ist der Standardwert.
- Tipp: Die Alertüberwachung muss aktiviert sein und die E-Mail-Einstellungen müssen korrekt definiert sein, damit Alerts erfolgreich als E-Mail empfangen werden können. Um die aktuellen Einstellungen anzuzeigen, geben Sie den Befehl QUERY MONITORSETTINGS aus.

## Beispiel: Kennwort und Kennwortablaufdauer aktualisieren

Für den Administrator LARRY soll das neue Kennwort SECRETWORD mit einer Kennwortablaufdauer von 120 Tagen vergeben werden. In diesem Beispiel authentifiziert sich der Administrator mit dem IBM Spectrum Protect-Server.

```
update admin larry secretword passexp=120
```

## Beispiel: Alle Administratoren für die Kommunikation mit einem Server unter Verwendung der Sitzungssicherheit 'strict' aktualisieren

Alle Administratoren für die Verwendung der striktesten Sicherheitseinstellungen aktualisieren, um sich mit dem Server zu authentifizieren.

```
update admin * sessionsecurity=strict
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE ADMIN

| Befehl   | Beschreibung   |
|--|--|
| QUERY ADMIN  | Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.                               |
| QUERY STATUS   | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen) | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.                     |
| REGISTER ADMIN   | Definiert einen neuen Administrator, ohne Administratorberechtigung zu erteilen.                                     |
| REGISTER NODE  | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.                              |
| RENAME ADMIN   | Ändert den Namen eines IBM Spectrum Protect-Administrators.  |
| SET PASSEXP  | Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.                                   |
| UPDATE NODE  | Ändert die Attribute, die einem Clientknoten zugeordnet sind.  |

### Zugehörige Tasks:

Tivoli Storage Manager-Objekte benennen

### Zugehörige Verweise:

🔗 Ssl (Clientoption)

## UPDATE BACKUPSET (Aufbewahrungszeitraum einer Sicherungsgruppe aktualisieren)

Mit diesem Befehl kann der Aufbewahrungszeitraum aktualisiert werden, der der Sicherungsgruppe eines Clients zugeordnet ist.

## Berechtigungsklasse

Um diesen Befehl ausgeben zu können, müssen Benutzer die Systemberechtigung oder Maßnahmenberechtigung für die Domäne haben, der der Client-Knoten zugeordnet ist.

## Syntax

```

      .-,-,-----
      V      |
>>-UPDate BACKUPSET-----+Knotenname-----+----->
      '-Knotengruppenname-'

      .-,-,-----
      V      |
>---Sicherungsgruppenname---RETention---+Tage---+----->
      '-NOLimit-'

>+-----+-----+-----+-----+----->
  '-BEGINDate---Datum-'  '-BEGINTime---Zeit-'

>+-----+-----+-----+-----+----->
  '-ENDDate---Datum-'  '-ENDTime---Zeit-'

>+-----+-----+-----+-----+----->
  '-WHERERETention---Tage---+----->
      '-NOLimit-'

      .-WHEREDATAType---ALL-----
>+-----+-----+-----+-----+----->
  |      .-,-,-----
  |      V      |
  '-WHEREDATAType---FILE---+----->
      '-IMAGE-'

>+-----+-----+-----+-----+----->
  '-WHEREDEScRiption---Beschreibung-'

      .-VERSion---Any-----
>+-----+-----+-----+-----+----->
  '-Preview---No---+----->
      '-Yes-'      '-VERSion---Any---+----->
      '-Latest-'

```

## Parameter

### Knotenname oder Knotengruppenname (Erforderlich)

Gibt die Namen der Clientknoten oder Knotengruppen an, deren Daten in der angegebenen Sicherungsgruppe enthalten sind, die aktualisiert werden soll. Sollen mehrere Knoten- und Knotengruppenamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Die angegebenen Knotennamen können Platzhalterzeichen enthalten, aber Knotengruppenamen dürfen keine Platzhalterzeichen enthalten.

### Sicherungsgruppenname (Erforderlich)

Gibt den Namen der Sicherungsgruppe an, die aktualisiert werden soll. Der angegebene Sicherungsgruppenname kann Platzhalterzeichen enthalten. Es können mehrere Sicherungsgruppenamen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden.

### RETention (Erforderlich)

Gibt die aktualisierte Anzahl der Tage an, die die Sicherungsgruppe auf dem Server aufbewahrt werden soll. Sie können eine ganze Zahl von 0 bis 30000 angeben. Gültige Werte:

#### Tage

Gibt die aktualisierte Anzahl der Tage an, die die Sicherungsgruppe aufbewahrt werden soll.

#### NOLimit

Gibt an, dass die Sicherungsgruppe auf dem Server unbegrenzt aufbewahrt wird. Wird NOLIMIT angegeben, werden die Datenträger mit der Sicherungsgruppe vom Server unbegrenzt aufbewahrt, es sei denn, ein Benutzer oder Administrator löscht die Datenträger aus dem Serverspeicher.

Achtung: Die Aktualisierung des Aufbewahrungszeitraums einer Sicherungsgruppe kann dazu führen, dass sie zu einem anderen Zeitpunkt als andere Sicherungsgruppen verfällt, die möglicherweise auf demselben Ausgabedatenträger gespeichert sind. Der Datenträger wird in jedem Fall erst dann für andere Verwendungen verfügbar gemacht, wenn alle Sicherungsgruppen verfallen sind.

### BEGINDate

Gibt das Anfangsdatum an, an dem die zu aktualisierende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum. Dieser Parameter kann mit dem Parameter BEGINTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird ein Anfangsdatum ohne eine Anfangszeit angegeben, lautet die Zeit 24:00 (Mitternacht) an dem angegebenen Datum.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert | Beschreibung | Beispiel |
|------|--------------|----------|
|------|--------------|----------|



| Wert                              | Beschreibung  | Beispiel   |
|-----------------------------------|---|--|
| MM/TT/JJJJ                        | Ein bestimmtes Datum                                      | 09/15/1999   |
| TODAY                             | Das aktuelle Datum  | TODAY  |
| TODAY+Tage <i>oder</i><br>+Tage   | Das aktuelle Datum plus der Anzahl der angegebenen Tage.  | TODAY +3 <i>oder</i> +3.   |
| TODAY-Tage <b>oder</b> -<br>Tage  | Das aktuelle Datum minus der Anzahl der angegebenen Tage. | TODAY-3 <i>oder</i> -3.  |
| EOLM (Ende des<br>letzten Monats) | Der letzte Tag des Vormonats.                             | EOLM   |
| EOLM-Tage                         | Der letzte Tag des Vormonats minus angegebene Tage.       | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses<br>Monats)    | Der erste Tag des aktuellen Monats.                       | BOTM   |
| BOTM+Tage                         | Der erste Tag des aktuellen Monats plus angegebene Tage.  | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

#### BEGINTime

Gibt die Anfangszeit an, zu der die zu aktualisierende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Standardwert ist die aktuelle Uhrzeit. Dieser Parameter kann mit dem Parameter BEGINDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird eine Anfangszeit ohne ein Anfangsdatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Uhrzeit.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert                             | Beschreibung   | Beispiel                      |
|----------------------------------|--|-------------------------------|
| HH:MM:SS                         | Eine bestimmte Uhrzeit   | 10:30:08                      |
| NOW                              | Die aktuelle Uhrzeit   | NOW                           |
| NOW+HH:MM <i>oder</i><br>+HH:MM  | Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum  | NOW+02:00 <i>oder</i> +02:00. |
| NOW-HH:MM <b>oder</b> -<br>HH:MM | Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum | NOW-02:00 <i>oder</i> -02:00. |

#### ENDDate

Gibt das Enddatum an, an dem die zu aktualisierende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter ENDTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird ein Enddatum ohne eine Endzeit angegeben, lautet die Zeit 23:59:59 am angegebenen Enddatum.

Sie können das Datum mit einem der folgenden Werte angeben:

| Wert                              | Beschreibung  | Beispiel   |
|-----------------------------------|---|--|
| MM/TT/JJJJ                        | Ein bestimmtes Datum                                      | 09/15/1999   |
| TODAY                             | Das aktuelle Datum  | TODAY  |
| TODAY+Tage <i>oder</i><br>+Tage   | Das aktuelle Datum plus der Anzahl der angegebenen Tage.  | TODAY +3 <i>oder</i> +3.   |
| TODAY-Tage <i>oder</i> –<br>Tage  | Das aktuelle Datum minus der Anzahl der angegebenen Tage. | TODAY -3 <i>oder</i> -3.   |
| EOLM (Ende des<br>letzten Monats) | Der letzte Tag des Vormonats.                             | EOLM   |
| EOLM-Tage                         | Der letzte Tag des Vormonats minus angegebene Tage.       | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses<br>Monats)    | Der erste Tag des aktuellen Monats.                       | BOTM   |

| Wert      | Beschreibung   | Beispiel  |
|-----------|--|---|
| BOTM+Tage | Der erste Tag des aktuellen Monats plus angegebene Tage. | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren. |

#### ENDTime

Gibt die Endzeit an, zu der die zu aktualisierende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter ENDDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird eine Endzeit ohne ein Enddatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Zeit. Sie können die Uhrzeit mit einem der folgenden Werte angeben:

| Wert                             | Beschreibung   | Beispiel                      |
|----------------------------------|--|-------------------------------|
| HH:MM:SS                         | Eine bestimmte Uhrzeit   | 10:30:08                      |
| NOW                              | Die aktuelle Uhrzeit   | NOW                           |
| NOW+HH:MM <i>oder</i><br>+HH:MM  | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten  | NOW+02:00 <i>oder</i> +02:00. |
| NOW-HH:MM <i>oder</i> -<br>HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten | NOW-02:00 <i>oder</i> -02:00. |

#### WHEREtention

Gibt den Aufbewahrungszeitraum in Tagen an, der der zu aktualisierenden Sicherungsgruppe zugeordnet ist. Gültige Werte:

##### Tage

Gibt an, dass die Sicherungsgruppe, die diese Anzahl Tage aufbewahrt wird, aktualisiert wird.

##### NOLimit

Gibt an, dass die Sicherungsgruppe, die unbegrenzt aufbewahrt wird, aktualisiert wird.

#### WHEREDescription

Gibt die Beschreibung an, die der zu aktualisierenden Sicherungsgruppe zugeordnet ist. Dieser Parameter ist wahlfrei. Für die Beschreibung können Platzhalterzeichen angegeben werden. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

#### WHEREDataType

Gibt an, dass die Sicherungsgruppen mit den angegebenen Typen von Daten aktualisiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert gibt an, dass Sicherungsgruppen für alle Typen von Daten (Dateiebene, Image und Anwendung) aktualisiert werden sollen. Bei der Angabe mehrerer Datentypen muss jeder Datentyp durch ein Komma und ohne Leerzeichen voneinander getrennt werden. Gültige Werte:

##### ALL

Gibt an, dass Sicherungsgruppen für alle Typen von Daten (Dateiebene, Image und Anwendung) aktualisiert werden sollen. Dies ist der Standardwert.

##### FILE

Gibt an, dass eine Sicherungsgruppe auf Dateiebene aktualisiert werden soll. Sicherungsgruppen auf Dateiebene enthalten Dateien und Verzeichnisse, die vom Client für Sichern/Archivieren gesichert wurden.

##### IMAGE

Gibt an, dass eine Imagesicherungsgruppe aktualisiert werden soll. Imagesicherungsgruppen enthalten Images, die mit dem Befehl BACKUP IMAGE des Clients für Sichern/Archivieren erstellt wurden.

#### Preview

Gibt an, ob die Liste der zu aktualisierenden Sicherungsgruppen vorab angezeigt werden soll, ohne die Sicherungsgruppen tatsächlich zu aktualisieren. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

##### No

Gibt an, dass die Sicherungsgruppen aktualisiert werden.

##### Yes

Gibt an, dass der Server die zu aktualisierenden Sicherungsgruppen anzeigt, ohne die Sicherungsgruppen tatsächlich zu aktualisieren.

#### VERSION

Gibt die Version der Sicherungsgruppe an, die aktualisiert werden soll. Sicherungsgruppen mit demselben Präfixnamen werden als verschiedene Versionen derselben Sicherungsgruppe betrachtet. Dieser Parameter ist wahlfrei. Der Standardwert gibt an, dass alle Versionen aktualisiert werden sollen, die den im Befehl angegebenen Kriterien entsprechen. Gültige Werte:

##### Any

Gibt an, dass alle Versionen aktualisiert werden sollen, die den im Befehl angegebenen Kriterien entsprechen.

##### Latest

Gibt an, dass nur die letzte Version der Sicherungsgruppe aktualisiert werden soll. Wenn andere im Befehl angegebene Kriterien (beispielsweise ENDDATE oder WHERERETENTION) die letzte Version der Sicherungsgruppe ausschließen, wird keine Sicherungsgruppe aktualisiert.

## Beispiel: Einen Aufbewahrungszeitraum aktualisieren

Den Aufbewahrungszeitraum aktualisieren, wobei die Beschreibung Healthy Computers lautet. Der Aufbewahrungszeitraum ist der Sicherungsgruppe PERS\_DATA.3099 zugeordnet, die Daten vom Clientknoten JANE enthält. Den Aufbewahrungszeitraum in 70 Tage ändern.

```
update backupset jane pers_data.3099
retention=70 wheredescription="healthy computers"
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE BACKUPSET

| Befehl                  | Beschreibung  |
|-------------------------|---|
| DEFINE BACKUPSET        | Definiert eine zuvor generierte Sicherungsgruppe für einen Server.          |
| DEFINE NODEGROUP        | Definiert eine Gruppe von Knoten.   |
| DEFINE NODEGROUPMEMBER  | Fügt einer Knotengruppe einen Clientknoten hinzu.                           |
| DELETE BACKUPSET        | Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum. |
| DELETE NODEGROUP        | Löscht eine Knotengruppe.   |
| DELETE NODEGROUPMEMBER  | Löscht einen Clientknoten aus einer Knotengruppe.                           |
| GENERATE BACKUPSET      | Generiert eine Sicherungsgruppe mit den Daten eines Clients.                |
| GENERATE BACKUPSETTOC   | Generiert ein Inhaltsverzeichnis für eine Sicherungsgruppe.                 |
| QUERY BACKUPSET         | Zeigt Sicherungsgruppen an.   |
| QUERY BACKUPSETCONTENTS | Zeigt den Inhalt in Sicherungsgruppen an.                                   |
| QUERY NODEGROUP         | Zeigt Informationen zu Knotengruppen an.                                    |
| UPDATE NODEGROUP        | Aktualisiert die Beschreibung einer Knotengruppe.                           |

## UPDATE CLIENTOPT (Folgenummer einer Clientoption aktualisieren)

Mit diesem Befehl kann die Folgenummer einer Clientoption in einer Clientoptionsgruppe aktualisiert werden.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

## Syntax

```
>>-UPDate CLIENTOpt--Optionsgruppenname--Optionsname----->
>--aktuelle_Folgenummer--neue_Folgenummer-----><
```

## Parameter

- Optionsgruppenname (Erforderlich)  
Gibt den Namen der Optionsgruppe an.
- Optionsname (Erforderlich)  
Gibt eine gültige Client-Option an.
- aktuelle\_Folgenummer (Erforderlich)  
Gibt die aktuelle Folgenummer der Option an.
- neue\_Folgenummer (Erforderlich)  
Gibt die neue Folgenummer der Option an.

## Beispiel: Folgenummer einer Clientoption aktualisieren

Um die aktuelle Folgenummer der Clientoption zu aktualisieren, den folgenden Befehl ausgeben:

```
update clientopt eng dateformat 0 9
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE CLIENTOPT

| Befehl           | Beschreibung  |
|------------------|---|
| COPY CLOPTSET    | Kopiert eine Clientoptionsgruppe.                       |
| DEFINE CLIENTOPT | Fügt einer Clientoptionsgruppe eine Clientoption hinzu. |
| DELETE CLIENTOPT | Löscht eine Clientoption aus einer Clientoptionsgruppe. |
| DELETE CLOPTSET  | Löscht eine Clientoptionsgruppe.                        |
| QUERY CLOPTSET   | Zeigt Informationen über eine Clientoptionsgruppe an.   |

## UPDATE CLOPTSET (Beschreibung einer Clientoptionsgruppe aktualisieren)

Mit diesem Befehl kann die Beschreibung für eine Clientoptionsgruppe aktualisiert werden.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, der der Clientknoten zugeordnet ist.

## Syntax

```
>>-UPDate CLOptset--Optionsgruppenname----->>  
>--DESCRiption--===Beschreibung-----><
```

## Parameter

Optionsgruppenname (Erforderlich)

Gibt den Namen der Optionsgruppe an.

DESCRiption (Erforderlich)

Gibt eine Beschreibung der Clientoptionsgruppe an. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält.

## Beispiel: Beschreibung einer Clientoptionsgruppe aktualisieren

Aktualisieren Sie die Beschreibung für die Clientoptionsgruppe mit dem Namen ENG.

```
update cloptset eng description="unix"
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE CLOPTSET

| Befehl           | Beschreibung  |
|------------------|---|
| COPY CLOPTSET    | Kopiert eine Clientoptionsgruppe.                       |
| DEFINE CLIENTOPT | Fügt einer Clientoptionsgruppe eine Clientoption hinzu. |
| DEFINE CLOPTSET  | Definiert eine Clientoptionsgruppe.                     |
| DELETE CLIENTOPT | Löscht eine Clientoption aus einer Clientoptionsgruppe. |
| DELETE CLOPTSET  | Löscht eine Clientoptionsgruppe.                        |
| QUERY CLOPTSET   | Zeigt Informationen über eine Clientoptionsgruppe an.   |

| Befehl           | Beschreibung  |
|------------------|---|
| UPDATE CLIENTOPT | Aktualisiert die Folgenummer einer Clientoption in einer Clientoptionsgruppe. |

## UPDATE COLLOGROUP (Kollokationsgruppe aktualisieren)

Verwenden Sie diesen Befehl, um die Beschreibung einer Kollokationsgruppe zu ändern.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-UPDate COLLOGGroup--Gruppenname----->
>--DEscription===--Beschreibung-----<<
```

### Parameter

Gruppenname

Gibt den Namen der Kollokationsgruppe an, deren Beschreibung aktualisiert werden soll.

DEscription (Erforderlich)

Gibt eine Beschreibung der Kollokationsgruppe an. Dieser Parameter ist erforderlich. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Enthält die Beschreibung Leerzeichen, schließen Sie die gesamte Beschreibung in Anführungszeichen ein.

### Beispiel: Eine Kollokationsgruppe aktualisieren

Die Kollokationsgruppe GROUP1 mit einer neuen Beschreibung aktualisieren.

```
update colloggroup group1 "Personalabteilung"
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE COLLOGROUP

| Befehl              | Beschreibung  |
|---------------------|---|
| DEFINE COLLOGROUP   | Definiert eine Kollokationsgruppe.  |
| DEFINE COLLOCMEMBER | Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.                                     |
| DEFINE STGPOOL      | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.                            |
| DELETE COLLOGROUP   | Löscht eine Kollokationsgruppe.   |
| DELETE COLLOCMEMBER | Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.                                     |
| MOVE NODEDATA       | Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen. |
| QUERY COLLOGROUP    | Zeigt Informationen zu Kollokationsgruppen an.  |
| QUERY NODE          | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.                             |
| QUERY NODEDATA      | Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.                               |
| QUERY STGPOOL       | Zeigt Informationen zu Speicherpools an.  |
| REMOVE NODE         | Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.              |
| UPDATE STGPOOL      | Ändert die Attribute eines Speicherpools.   |

## UPDATE COPYGROUP (Kopiengruppe aktualisieren)

Mit diesem Befehl kann eine Sicherungs- oder Archivierungskopiengruppe aktualisiert werden. Um Clients die Verwendung der aktualisierten Kopiengruppe zu ermöglichen, muss die Maßnahmengruppe aktiviert werden, die die Kopiengruppe enthält.

Tipp: Der Befehl UPDATE COPYGROUP schlägt fehl, wenn ein Kopiespeicherpool als Zielort angegeben wird.

Der Befehl UPDATE COPYGROUP liegt in zwei unterschiedlichen Formaten vor, und zwar abhängig davon, ob eine Sicherungskopiengruppe oder eine Archivierungskopiengruppe aktualisiert werden soll. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für UPDATE COPYGROUP

| Befehl              | Beschreibung  |
|---------------------|---|
| ACTIVATE POLICYSET  | Wertet eine Maßnahmengruppe aus und aktiviert sie.  |
| ASSIGN DEFMGMTCLASS | Ordnet eine Verwaltungsklasse als Standardklasse für eine angegebene Maßnahmengruppe zu.                                      |
| COPY MGMTCLASS      | Erstellt eine Kopie einer Verwaltungsklasse.  |
| DEFINE COPYGROUP    | Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse. |
| DEFINE MGMTCLASS    | Definiert eine Verwaltungsklasse.   |
| DELETE COPYGROUP    | Löscht eine Sicherungs- oder Archivierungskopiengruppe aus einer Maßnahmendomäne und Maßnahmengruppe.                         |
| DELETE MGMTCLASS    | Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe.                     |
| EXPIRE INVENTORY    | Startet die Verfallsverarbeitung für den Datenträgerbestandsverfall manuell.  |
| QUERY COPYGROUP     | Zeigt die Attribute einer Kopiengruppe an.  |
| QUERY MGMTCLASS     | Zeigt Informationen zu Verwaltungsklassen an.   |

- UPDATE COPYGROUP (Sicherungskopiengruppe aktualisieren)  
Mit diesem Befehl kann eine definierte Sicherungskopiengruppe aktualisiert werden.
- UPDATE COPYGROUP (Definierte Archivierungskopiengruppe aktualisieren)  
Mit diesem Befehl kann eine definierte Archivierungskopiengruppe aktualisiert werden.

## UPDATE COPYGROUP (Sicherungskopiengruppe aktualisieren)

Mit diesem Befehl kann eine definierte Sicherungskopiengruppe aktualisiert werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Kopiengruppe gehört.

### Syntax

```
>>-UPDate COpYgroup----->
>--Domänennname--Name_der_Maßnahmengruppe--Klassennamen----->
>--+-----+--+-----+----->
  '-STANDARD-'   '-Type-----Backup-'
>--+-----+--+-----+----->
  '-DESTination-----Poolname-'   '-FREQuency-----Tage-'
>--+-----+--+-----+----->
  '-VERExists-----+Anzahl---'
                        '-NOLimit-'
```

```

>----->
  '-VERDeleted-----+Anzahl--+'
                        '-NOLimit-'

>----->
  '-RETEExtra-----+Tage-----+'  '-RETOOnly-----+Tage-----+'
                        '-NOLimit-'          '-NOLimit-'

>----->
  '-MODE-----+MODified+++'
                        '-ABSolute-'

>----->
  '-SERialization-----+SHRSTatic--+'
                        +-STatic-----+
                        +-SHRDYnamic-+
                        '-DYnamic----+'

>-----<
  '-TOCDestination-----+Poolname---+'

```

## Parameter

### Domänenname (Erforderlich)

Gibt die Maßnahmendomäne an, zu der die Kopiengruppe gehört.

### Name\_der\_Maßnahmengruppe (Erforderlich)

Gibt die Maßnahmengruppe an, zu der die Kopiengruppe gehört. Eine Kopiengruppe in der AKTIVEN Maßnahmengruppe kann nicht aktualisiert werden.

### Klassenname (Erforderlich)

Gibt die Verwaltungsklasse an, zu der die Kopiengruppe gehört.

### STANDARD

Gibt die Kopiengruppe an, die STANDARD lauten muss. Dieser Parameter ist wahlfrei.

### Type=Backup

Gibt an, dass eine Sicherungskopiengruppe aktualisiert werden soll. Dieser Parameter ist wahlfrei.

### DESTINATION

Gibt den primären Speicherpool an, in dem der Server anfänglich Sicherungsdaten speichert. Dieser Parameter ist wahlfrei. Ein Kopienspeicherpool kann nicht als Zielort angegeben werden.

### FREQUENCY

Gibt an, wie oft der Server eine Datei sichern kann. Dieser Parameter ist wahlfrei. Der Server sichert eine Datei nur, wenn die angegebene Anzahl Tage seit der letzten Sicherung verstrichen ist. Der Wert für den Parameter FREQUENCY wird nur bei einer vollständigen Teilsicherung verwendet. Dieser Wert wird bei einer selektiven Sicherung oder einer partiellen Teilsicherung ignoriert. Zulässige Werte sind ganze Zahlen von 0 bis 9999. Der Wert 0 bedeutet, daß der Server eine Datei unabhängig vom Datum der letzten Sicherung sichern kann.

### VERExists

Gibt die maximale Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die sich momentan im Client-Dateisystem befinden. Dieser Parameter ist wahlfrei.

Wird der Grenzwert durch eine Teilsicherung überschritten, verfällt die älteste Sicherungsversion, die im Serverspeicher vorhanden ist. Gültige Werte:

### Zahl

Gibt die Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die sich momentan im Client-Dateisystem befinden. Zulässige Werte sind ganze Zahlen von 1 bis 9999.

Tipp: Um sicherzustellen, dass Dateien nach einem Malwarevorfall, wie z. B. einer Ransomware-Attacke, wiederhergestellt werden können, geben Sie einen Wert von mindestens 2 an. Bevorzugte Werte sind 3, 4 oder höher.

### NOLimit

Gibt an, daß der Server alle Sicherungsversionen aufbewahren soll.

Die Anzahl der Sicherungsversionen, die aufbewahrt werden sollen, wird so lange durch diesen Parameter gesteuert, bis Versionen den Aufbewahrungszeitraum überschreiten, der durch den Parameter RETEXTRA angegeben ist.

### VERDeleted

Gibt die maximale Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die nach der Sicherung mit dem Server aus dem Client-Dateisystem gelöscht wurden. Dieser Parameter ist wahlfrei.

Löscht ein Benutzer eine Datei aus dem Clientdateisystem, ändert der Server bei der nächsten Teilsicherung die aktive Sicherungsversion der Datei in eine inaktive Version und markiert die ältesten Versionen, die diese Anzahl überschreiten, als verfallen. Das Verfallsdatum der übrigen Versionen wird durch den Aufbewahrungszeitraum bestimmt, der mit dem Parameter RETEXTRA oder RETONLY angegeben wurde. Gültige Werte:

#### Anzahl

Gibt die Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die nach der Sicherung aus dem Client-Dateisystem gelöscht werden. Es kann ein Wert von 0 bis 9999 angegeben werden.

#### NOLimit

Gibt an, dass der Server alle Sicherungsversionen für Dateien, die nach der Sicherung aus dem Clientdateisystem gelöscht werden, aufbewahren soll.

#### RETEExtra

Gibt die Anzahl der Tage an, die der Server eine Sicherungsversion aufbewahrt, nachdem diese Version inaktiv wurde. Die Version einer Datei wird inaktiv, wenn der Client eine aktuellere Sicherungsversion speichert oder wenn der Client die Datei aus der Datenstation löscht und dann eine vollständige Teilsicherung durchführt. Der Server löscht inaktive Versionen auf der Basis des Aufbewahrungszeitraums, auch wenn die Anzahl der inaktiven Versionen die durch den Parameter VEREXISTS oder VERDELETED erlaubte Anzahl nicht überschreitet. Dieser Parameter ist wahlfrei. Gültige Werte:

#### Tage

Gibt die Anzahl Tage an, die inaktive Sicherungsversionen aufbewahrt werden sollen. Zulässige Werte sind ganze Zahlen von 0 bis 9999.

Tipp: Um sicherzustellen, dass Dateien nach einem Malwarevorfall, wie z. B. einer Ransomware-Attacke, wiederhergestellt werden können, geben Sie einen Wert von mindestens 14 Tagen an. Der bevorzugte Wert ist 30 oder mehr Tage.

#### NOLimit

Gibt an, dass inaktive Sicherungsversionen unbegrenzt aufbewahrt werden sollen.

Wird NOLIMIT angegeben, löscht der Server überzählige Sicherungsversionen auf der Basis des Parameters VEREXISTS (wenn die Datei noch im Client-Dateisystem vorhanden ist) oder auf der Basis des Parameters VERDELETED (wenn die Datei nicht mehr im Client-Dateisystem vorhanden ist).

#### RETOOnly

Gibt die Anzahl Tage an, die die letzte Sicherungsversion einer Datei aufbewahrt werden soll, die aus dem Client-Dateisystem gelöscht wurde. Dieser Parameter ist wahlfrei. Gültige Werte:

#### Tage

Gibt die Anzahl Tage an, die die letzte verbleibende inaktive Kopie einer Datei aufbewahrt werden soll. Zulässige Werte sind ganze Zahlen von 0 bis 9999.

Tipp: Um sicherzustellen, dass Dateien nach einem Malwarevorfall, wie z. B. einer Ransomware-Attacke, wiederhergestellt werden können, geben Sie einen Wert von mindestens 30 Tagen an.

#### NOLimit

Gibt an, dass die letzte verbleibende inaktive Version einer Datei unbegrenzt aufbewahrt werden soll.

Wird NOLIMIT angegeben, wird die letzte verbleibende Sicherungsversion unbegrenzt von dem Server aufbewahrt, es sei denn, ein Benutzer oder Administrator löscht die Datei aus dem Server-Speicher.

#### MODE

Gibt an, ob der Server eine Datei nur sichert, wenn sich die Datei seit der letzten Sicherung geändert hat oder wenn ein Client eine Sicherung anfordert. Dieser Parameter ist wahlfrei. Gültige Werte:

#### MODified

Gibt an, daß die Datei nur gesichert wird, wenn sie sich seit der letzten Sicherung geändert hat. Eine Datei wird als geändert angesehen, wenn folgende Bedingungen gelten:

- Das Datum der letzten Änderung hat sich geändert.
- Die Dateigröße hat sich geändert.
- Der Dateieigner hat sich geändert.
- Die Dateiberechtigungen haben sich geändert.

#### ABSolute

Gibt an, daß die Datei unabhängig davon gesichert wird, ob sie geändert wurde.

Der Wert für MODE wird nur für vollständige Teilsicherungen verwendet. Dieser Wert wird bei einer partiellen Teilsicherung oder einer selektiven Sicherung ignoriert.

#### SERialization

Gibt an, wie der Server Dateien oder Verzeichnisse verarbeitet, wenn sie während der Sicherungsverarbeitung geändert werden. Dieser Parameter ist wahlfrei. Gültige Werte:

#### SHRStatic

Gibt an, daß der Server eine Datei oder ein Verzeichnis nur sichert, wenn die Datei oder das Verzeichnis während der Sicherung nicht geändert wird. Der Server versucht bis zu viermal, eine Sicherung durchzuführen, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wurde. Wird die Datei oder das Verzeichnis während jedes Sicherungsversuchs geändert, sichert der Server die Datei oder das Verzeichnis nicht.



## Static

Gibt an, daß der Server eine Datei oder ein Verzeichnis nur sichert, wenn die Datei oder das Verzeichnis während der Sicherung nicht geändert wird. Der Server versucht nur einmal, die Sicherung durchzuführen.

Plattformen, die die Option STATIC nicht unterstützen, nehmen den Standardwert SHRSTATIC an.

## SHRDynamic

Gibt an, daß der Server die Datei oder das Verzeichnis während des letzten Sicherungsversuchs sichert, auch wenn die Datei oder das Verzeichnis während der Sicherung geändert wird. Der Server versucht bis zu viermal, eine Sicherung durchzuführen, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wurde.

## Dynamic

Gibt an, daß der Server eine Datei oder ein Verzeichnis beim ersten Versuch sichert, auch wenn die Datei oder das Verzeichnis während der Sicherungsverarbeitung geändert wird.

Wichtig: Die Werte SHRDYNAMIC und DYNAMIC sind mit Vorsicht zu verwenden. IBM Spectrum Protect bestimmt anhand dieser Werte, ob eine Datei oder ein Verzeichnis gesichert wird, während Änderungen vorgenommen werden. Aus diesem Grund ist die Sicherungsversion möglicherweise nur eine Sicherung mit grober Übereinstimmung. Eine Sicherung mit grober Übereinstimmung gibt den aktuellen Inhalt der Datei oder des Verzeichnisses nicht korrekt wieder, da sie einige, aber nicht alle Änderungen enthält. Wird eine Datei, die eine Sicherung mit grober Übereinstimmung enthält, zurückgeschrieben, ist die Datei möglicherweise nicht brauchbar. Dies ist von der Anwendung abhängig, die die Datei verwendet. Ist eine Sicherung mit grober Übereinstimmung nicht akzeptabel, definieren Sie für SERIALIZATION den Wert SHRSTATIC oder STATIC, damit IBM Spectrum Protect nur dann eine Sicherungsversion erstellt, wenn die Datei oder das Verzeichnis nicht geändert wird.

## TOCDestination

Gibt den primären Speicherpool an, in dem ein Inhaltsverzeichnis für jede NDMP-Sicherungs- oder Sicherungsgruppenoperation anfänglich gespeichert wird, für die ein Inhaltsverzeichnis generiert wird. Dieser Parameter ist wahlfrei. Ein Kopierspeicherpool kann nicht als Zielort angegeben werden. Der als Zielort angegebene Speicherpool muss das Datenformat NATIVE oder NONBLOCK haben. Um Mountverzögerungen zu vermeiden, stellen Sie sicher, dass der Speicherpool die Einheitenklasse DISK oder DEVTYPE=FILE hat. Die Generierung eines Inhaltsverzeichnisses ist eine Option für NDMP-Sicherungsoperationen, wird aber nicht für andere Imagesicherungsoperationen unterstützt.

Um einen vorhandenen Zielort für das Inhaltsverzeichnis aus der Kopiergruppe zu entfernen, geben Sie eine leere Zeichenfolge ("" ) für diesen Wert an.

Wird die Erstellung eines Inhaltsverzeichnisses (TOC) für eine Sicherungsoperation angefordert, die NDMP verwendet, und ist das Image an eine Verwaltungsklasse gebunden, deren Sicherungskopiergruppe keinen Zielort für das Inhaltsverzeichnis angibt, hängt das Ergebnis von dem TOC-Parameter für die Sicherungsoperation ab.

- Bei TOC=PREFERRED (Standardwert) wird die Sicherung ohne Erstellung eines Inhaltsverzeichnisses fortgesetzt.
- Bei TOC=YES schlägt die gesamte Sicherung fehl, da kein Inhaltsverzeichnis erstellt werden kann.

## Beispiel: Eine Sicherungskopiergruppe aktualisieren

Die Sicherungskopiergruppe STANDARD in der Maßnahmendomäne EMPLOYEE\_RECORDS, Maßnahmengruppe VACATION, Verwaltungsklasse ACTIVEFILES aktualisieren. Den Zielort in DISKPOOL ändern, mit einem Mindestintervall von sieben Tagen zwischen Sicherungen, unabhängig davon, ob die Dateien geändert wurden. Bis zu drei Sicherungsversionen aufbewahren, während eine Datei noch in einem Client-Dateisystem vorhanden ist.

```
update copygroup employee_records vacation
activefiles type=backup destination=diskpool
frequency=7 verexists=3 mode=absolute
```

## UPDATE COPYGROUP (Definierte Archivierungskopiergruppe aktualisieren)

Mit diesem Befehl kann eine definierte Archivierungskopiergruppe aktualisiert werden.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Kopiergruppe gehört.

## Syntax

```
>>-UPDate CCopygroup----->
```

```
>--Domänenname--Name_der_Maßnahmengruppe--Klassenname----->
```

```

>--+-----+---Type---+---Archive----->
  '-STANDARD-'

>--+-----+-----+-----+----->
  '-DESTination---+---Poolname-' '-FREQuency---+---Cmd-'

>--+-----+-----+-----+----->
  '-RETVer---+---Tage---+-' '-MODE---+---ABSolute-'
    '-NOLimit-'

>--+-----+-----+-----+----->
  '-RETMin---+---Tage---'

>--+-----+-----+-----+-----><
  '-SERialization---+---SHRStatic---+-'
    '+-STatic-----+
    '+-SHRDYnamic-+
    '-DYnamic----'

```

## Parameter

Domänenname (Erforderlich)

Gibt die Maßnahmendomäne an, zu der die Kopiengruppe gehört.

Name\_der\_Maßnahmengruppe (Erforderlich)

Gibt die Maßnahmengruppe an, zu der die Kopiengruppe gehört. Eine Kopiengruppe in der AKTIVEN Maßnahmengruppe kann nicht aktualisiert werden.

Klassenname (Erforderlich)

Gibt die Verwaltungsklasse an, zu der die Kopiengruppe gehört.

STANDARD

Gibt die Kopiengruppe an, die STANDARD lauten muss. Dieser Parameter ist wahlfrei.

Type=Archive (Erforderlich)

Gibt an, dass eine Archivierungskopiengruppe aktualisiert werden soll. Dieser Parameter ist erforderlich.

DESTination

Gibt den primären Speicherpool an, in dem der Server anfänglich die Archivierungskopie speichert. Dieser Parameter ist wahlfrei. Ein Kopierspeicherpool kann nicht als Zielort angegeben werden.

FREQuency=Cmd

Gibt die Kopienhäufigkeit an, die CMD lauten muss. Dieser Parameter ist wahlfrei.

RETVer

Gibt die Anzahl Tage an, die eine Archivierungskopie aufbewahrt werden soll. Dieser Parameter ist wahlfrei. Gültige Werte:

Tage

Gibt die Anzahl Tage an, die eine Archivierungskopie aufbewahrt werden soll. Sie können eine ganze Zahl von 0 bis 30000 angeben.

Tipp: Um sicherzustellen, dass Ihre Daten nach einem Malwarevorfall, wie z. B. einer Ransomware-Attacke, wiederhergestellt werden können, geben Sie einen Wert von mindestens 30 Tagen an.

NOLimit

Gibt an, dass eine Archivierungskopie unbegrenzt aufbewahrt werden soll.

Wird NOLIMIT angegeben, werden Archivierungskopien von dem Server unbegrenzt aufbewahrt, es sei denn, ein Benutzer oder Administrator löscht die Datei aus dem Serverspeicher.

Der Wert des Parameters RETVER kann Auswirkungen auf die Verwaltungsklasse haben, mit der der Server ein archiviertes Verzeichnis verbindet. Wenn der Client die Option ARCHMC nicht verwendet, verbindet der Server Verzeichnisse, die archiviert werden, mit der Standardverwaltungsklasse. Verfügt die Standardverwaltungsklasse über keine Archivierungskopiengruppe, verbindet der Server Verzeichnisse, die archiviert werden, mit der Verwaltungsklasse mit dem kürzesten Aufbewahrungszeitraum.

MODE=ABSolute

Gibt an, dass eine Datei immer archiviert wird, wenn der Client dies anfordert. Der Parameter MODE muss den Wert ABSOLUTE haben. Dieser Parameter ist wahlfrei.

RETMin

Gibt die Mindestanzahl von Tagen an, die eine Archivierungskopie aufbewahrt werden soll, nachdem sie archiviert wurde. Dieser Parameter ist wahlfrei. Der Standardwert ist 365.

SERialization

Gibt an, wie der Server Dateien verarbeitet, die während der Archivierung geändert werden. Dieser Parameter ist wahlfrei. Gültige Werte:

SHRStatic

Gibt an, daß der Server keine Datei archiviert, die gerade geändert wird. Der Server versucht bis zu viermal, eine Archivierung durchzuführen, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wurde. Wenn die Datei während des Archivierungsversuchs geändert wird, archiviert der Server die Datei nicht.

#### Static

Gibt an, daß der Server keine Datei archiviert, die gerade geändert wird. Wenn eine Datei während des Archivierungsversuchs geändert wird, archiviert der Server die Datei nicht.

Plattformen, die die Option STATIC nicht unterstützen, nehmen den Standardwert SHRSTATIC an.

#### SHRDynamic

Gibt an, daß der Server die Datei während des letzten Archivierungsversuchs archiviert, auch wenn die Datei während der Archivierung geändert wird. Der Server versucht bis zu viermal, die Datei zu archivieren, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wurde.

#### Dynamic

Gibt an, daß der Server eine Datei beim ersten Versuch archiviert, auch wenn sie während der Archivierungsverarbeitung geändert wird.

Wichtig: Die Werte SHRDYNAMIC und DYNAMIC sind mit Vorsicht zu verwenden. IBM Spectrum Protect bestimmt anhand dieser Werte, ob eine Datei archiviert wird, während Änderungen vorgenommen werden. Aus diesem Grund ist die Archivierungskopie möglicherweise nur eine Sicherung mit grober Übereinstimmung. Eine Sicherung mit grober Übereinstimmung gibt den aktuellen Inhalt der Datei nicht korrekt wieder, da sie einige, aber nicht alle Änderungen enthält. Wird eine Datei, die eine Sicherung mit grober Übereinstimmung enthält, abgerufen, ist die Datei möglicherweise nicht brauchbar. Dies ist von der Anwendung abhängig, die die Datei verwendet. Ist eine Sicherung mit grober Übereinstimmung nicht akzeptabel, definieren Sie für SERIALIZATION den Wert SHRSTATIC oder STATIC, damit IBM Spectrum Protect nur dann eine Archivierungskopie erstellt, wenn die Datei nicht geändert wird.

Tipp: Gehen Sie bei der Auswahl von Werten für die Aufbewahrungsdauer für primäre Speicherpools, die den Typ RECLAMATIONTYPE=SNAPLOCK haben, mit Vorsicht vor. Datenträger in Speicherpools mit diesem Typ können erst gelöscht werden, wenn die Daten ihrer Aufbewahrungsdauer verstrichen sind.

## Beispiel: Mehrere Elemente einer Kopiengruppe aktualisieren

Die Archivierungskopiengruppe STANDARD in der Maßnahmendomäne EMPLOYEE\_RECORDS, Maßnahmengruppe VACATION, Verwaltungsklasse ACTIVEFILES aktualisieren. Den Zielort in TAPEPOOL ändern. Archivierungskopien 190 Tage aufbewahren.

```
update copygroup employee_records vacation
activefiles standard type=archive
destination=tapepool retver=190
```

## UPDATE DATAMOVER (Einheit zum Versetzen von Daten aktualisieren)

Verwenden Sie diesen Befehl, um die Definition einer Einheit zum Versetzen von Daten zu aktualisieren oder eine Einheit zum Versetzen von Daten abzuhängen, wenn die Hardware gewartet wird.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-UPDate DATAMover--Name_der_Einheit_zum_Versetzen_von_Daten-->
>--+-----+-----+-----+-----+-----+-----+----->
  '-HLAddress---Adresse-' '-LLAddress----TCP-Anschluss-'
>--+-----+-----+-----+-----+-----+-----+----->
  '-USERid----Benutzer-ID-' '-PASsword----Kennwort-'
>--+-----+-----+-----+-----+-----+-----+-----<
  '-ONLine----+Yes-+-'
                '-No--'
```

### Parameter

Name\_der\_Einheit\_zum\_Versetzen\_von\_Daten (Erforderlich)  
Gibt den Namen der Einheit zum Versetzen von Daten an.

#### HLAddress

Gibt entweder die neue numerische IP-Adresse oder den neuen Domännennamen an, die für den Zugriff auf den NAS-Dateiserver verwendet werden. Dieser Parameter ist wahlfrei.

#### LLAddress

Gibt die neue TCP-Anschlussnummer für den Zugriff auf den NAS-Dateiserver für NDMP-Sitzungen (NDMP = Network Data Management Protocol) an. Dieser Parameter ist wahlfrei.

#### USERid

Gibt die Benutzer-ID eines Benutzers an, der berechtigt ist, eine NDMP-Sitzung mit dem NAS-Dateiserver einzuleiten. Geben Sie beispielsweise die Verwaltungs-ID eines NetApp-Dateiservers ein. Dieser Parameter ist wahlfrei.

#### PASSword

Gibt das neue Kennwort der Benutzer-ID für die Anmeldung beim NAS-Dateiserver an. Dieser Parameter ist wahlfrei.

#### ONLine

Gibt an, ob die Einheit zum Versetzen von Daten für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei.

#### Yes

Gibt an, dass die Einheit zum Versetzen von Daten für die Verwendung verfügbar ist.

#### No

Gibt an, dass die Einheit zum Versetzen von Daten nicht für die Verwendung verfügbar ist.

Achtung: Wird ein Kassettenarchiv durch die Verwendung eines Pfads von einer Einheit zum Versetzen von Daten zu dem Kassettenarchiv gesteuert, und ist die Einheit zum Versetzen von Daten offline, kann der Server nicht auf das Kassettenarchiv zugreifen. Wird der Server angehalten und erneut gestartet, während die Einheit zum Versetzen von Daten offline ist, wird das Kassettenarchiv nicht initialisiert.

## Beispiel: IP-Adresse für eine Einheit zum Versetzen von Daten aktualisieren

Die Einheit zum Versetzen von Daten für den Knoten NAS1 aktualisieren. Die numerische IP-Adresse von 9.67.97.103 in 9.67.97.109 ändern.

```
update datamover nas1 hladdress=9.67.97.109
```

## Beispiel: Domänenname für eine Einheit zum Versetzen von Daten aktualisieren

Die Einheit zum Versetzen von Daten für den Knoten NAS1 aktualisieren. Die numerische IP-Adresse von 9.67.97.109 in den Domännennamen NETAPP2.TUCSON.IBM.COM ändern.

```
update datamover nas1 hladdress=netapp2.tucson.ibm.com
```

## Zugehörige Befehle



Tabelle 1. Zugehörige Befehle für UPDATE DATAMOVER

| Befehl           | Beschreibung  |
|------------------|---|
| DEFINE DATAMOVER | Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server.     |
| DEFINE PATH      | Definiert einen Pfad von einer Quelle zu einem Ziel.                                    |
| DELETE DATAMOVER | Löscht eine Einheit zum Versetzen von Daten.  |
| QUERY DATAMOVER  | Zeigt Definitionen der Einheit zum Versetzen von Daten an.                              |
| REGISTER NODE    | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest. |
| UPDATE NODE      | Ändert die Attribute, die einem Clientknoten zugeordnet sind.                           |

## UPDATE DEVCLASS (Attribute einer Einheitenklasse aktualisieren)

Mit diesem Befehl kann eine definierte Einheitenklasse aktualisiert werden.

Anmerkung: Die Einheitenklasse DISK wird von IBM Spectrum Protect vordefiniert und kann mit dem Befehl UPDATE DEVCLASS nicht geändert werden.

  Wenn Sie eine Einheitenklasse für Einheiten aktualisieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in UPDATE DEVCLASS - z/OS Media-Server (Einheitenklasse für z/OS Media-Server aktualisieren).

Die Syntax und Parameterbeschreibungen werden entsprechend des Einheitentyps zur Verfügung gestellt. Die Syntax- und Parameterinformationen sind in der folgenden Reihenfolge aufgeführt.

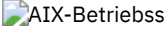
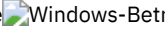


- UPDATE DEVCLASS (Einheitenklasse 3590 aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse 3592 aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse 4MM aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse 8MM aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse CENTERA aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse DLT aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse ECARTRIDGE aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse FILE aktualisieren)
-   UPDATE DEVCLASS (Einheitenklasse GENERICTAPE aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse LTO aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse NAS aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse REMOVABLEFILE aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse SERVER aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse VOLSAFE aktualisieren)

Tabelle 1. Zugehörige Befehle für UPDATE DEVCLASS

| Befehl           | Beschreibung  |
|------------------|---|
| BACKUP DEVCONFIG | Sichert IBM Spectrum Protect-Einheitendaten in einer Datei.   |
| DEFINE DEVCLASS  | Definiert eine Einheitenklasse.                               |
| DEFINE LIBRARY   | Definiert ein automatisiertes oder manuelles Kassettenarchiv. |
| DELETE DEVCLASS  | Löscht eine Einheitenklasse.                                  |
| QUERY DEVCLASS   | Zeigt Informationen zu Einheitenklassen an.                   |
| QUERY DIRSPACE   | Zeigt Informationen zu Verzeichnissen FILE an.                |
| UPDATE LIBRARY   | Ändert die Attribute eines Kassettenarchivs.                  |

## UPDATE DEVCLASS (Einheitenklasse 3590 aktualisieren)

Verwenden Sie die Einheitenklasse 3590, wenn Sie 3590-Bandeinheiten verwenden.

  Wenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in UPDATE DEVCLASS (Einheitenklasse 3590 für z/OS Media-Server aktualisieren).

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-UPDate DEVclass--Einheitenklassenname----->
>--+-----+----->
  '-LIBRARY---Kassettenarchivname-'
>--+-----+----->
  '-FORMAT---+DRIVE---+' '-ESTCAPacity---Größe-'
      +-3590B---+
      +-3590C---+
      +-3590E-B-+
      +-3590E-C-+
      +-3590H-B-+
      '-3590H-C-'
>--+-----+----->
  '-PREFIX---+ADSM-----+'
      '-Banddatenträgerpräfix-'
>--+-----+----->
  '-MOUNTRetention---Minuten-' '-MOUNTWait---Minuten-'
```

```
>-----<
'-MOUNTLimit-----+--DRIVES--+'
      +-Anzahl-+
      '-0-----'
```

## Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an.

LIBRARY

Gibt den Namen des definierten Kassettenarchivobjekts an, das die Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können.

Dieser Parameter ist wahlfrei.

Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Geben Sie stattdessen das Format an, das die Laufwerke verwenden.

In den folgenden Tabellen sind die Aufzeichnungsformate, die geschätzten Kapazitäten und die Optionen der Aufzeichnungsformate für 3590-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für 3590

| Format   | Geschätzte Kapazität  | Beschreibung   |
|--|---|--|
| DRIVE  | –   | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| 3590B  | 10,0 GB   | Dekomprimiertes (Basis-)Format   |
| 3590C  | Siehe Anmerkung<br>20,0 GB  | Komprimiertes Format   |
| 3590E-B  | 10,0 GB   | Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format   |
| 3590E-C  | Siehe Anmerkung<br>20,0 GB  | Komprimiertes Format, ähnlich dem 3590C-Format   |
| 3590H-B  | 30,0 GB (J-Kassette - Standardlänge)<br>60,0 GB (K-Kassette - erweiterte Länge)                     | Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format   |
| 3590H-C  | Siehe Anmerkung<br>60,0 GB (J-Kassette - Standardlänge)<br>120,0 GB (K-Kassette - erweiterte Länge) | Komprimiertes Format, ähnlich dem 3590C-Format   |
| Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann die tatsächliche Kapazität abhängig von der Effektivität der Komprimierung größer als der aufgelistete Wert sein. |   |  |

Tabelle 2. Auswahl des Aufzeichnungsformats für 3590-Einheiten

| Einheit | Format |       |         |         |         |         |
|---------|--------|-------|---------|---------|---------|---------|
|         | 3590B  | 3590C | 3590E-B | 3590E-C | 3590H-B | 3590H-C |
|         |        |       |         |         |         |         |

| Einheit        | Format          |                 |                 |                 |                 |                 |
|----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
|                | 3590B           | 3590C           | 3590E-B         | 3590E-C         | 3590H-B         | 3590H-C         |
| 3590Ultra-SCSI | Lesen/Schreiben | Lesen/Schreiben | ---             | ---             | ---             | ---             |
| 3590E          | Lesen/Schreiben | Lesen/Schreiben | Lesen/Schreiben | Lesen/Schreiben | Lesen/Schreiben | Lesen/Schreiben |
| 3590H          | Lesen           | Lesen           | Lesen           | Lesen           |                 |                 |
|                | Lesen           | Lesen           |                 |                 |                 |                 |

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger mit sequenziellem Zugriff an, die durch diese Einheitenklasse kategorisiert werden. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:  
AB.CD2.E
- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

## MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.



### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

## UPDATE DEVCLASS (Einheitenklasse 3592 aktualisieren)

  Wenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in UPDATE DEVCLASS (Einheitenklasse 3592 für z/OS Media-Server aktualisieren).

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-UPDate DEVclass--Einheitenklassenname----->
>+-----+----->
  '-LIBRARY---Kassettenarchivname- '
>+-----+----->
  '-LBProtect----+-READWrite+- '
      +-WRITEOnly+-
      '-No----- '
>+-----+----->
  '-SCALECapacity----+-100+- '  '-FORMAT----+-DRIVE----- '
      +-90--+          +-3592-----+
      '-20--'          +-3592C-----+
                          +-3592-2----+
                          +-3592-2C--+
                          +-3592-3----+
                          +-3592-3C--+
                          +-3592-4----+
                          +-3592-4C--+
                          +-3592-5----+
                          +-3592-5C--+
                          +-3592-5A--+
                          '-3592-5AC-'
>+-----+----->
  '-ESTCapacity----Größe- '
>+-----+----->
  '-PREFIX----+-ADSM-----+- '
      '-Banddatenträgerpräfix- '
>+-----+----->
  '-MOUNTRetention----Minuten- '  '-MOUNTWait----Minuten- '
```



```

>-----+-----+-----+-----+----->
  '-MOUNTLimit-----+DRIVES--+'
                        +-Anzahl-+
                        '-0-----'

>-----+-----+-----+-----+-----<
  | (1) (2) |
  '-----DRIVEEncryption-----+ON-----+'
                                     +-ALLOW-----+
                                     +-EXTERNAL--+
                                     '-OFF-----'

```

#### Anmerkungen:

1. Sie können nicht WORM=Yes in Verbindung mit DRIVEENCRYPTION=ON angeben.
2. Laufwerkverschlüsselung wird nur für 3592-Laufwerke der Generation 2 oder höher unterstützt.

## Parameter

### Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

### LIBRARY

Gibt den Namen des definierten Kassettenarchivobjekts an, das die Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können.

Dieser Parameter ist wahlfrei.

Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

### LBProtect

Gibt an, ob der Schutz logischer Blöcke verwendet wird, um die Integrität von Daten sicherzustellen, die auf Band gespeichert sind. Wenn LBPROTECT auf READWRITE oder WRITEONLY gesetzt ist, verwendet der Server dieses Feature des Bandlaufwerks für den Schutz logischer Blöcke und generiert CRC-Zugriffsschutzinformationen für jeden Datenblock, der auf Band geschrieben wird. Der Server überprüft auch die CRC-Zugriffsschutzinformationen, wenn Daten von dem Band gelesen werden.

Die folgenden Werte sind gültig:

#### READWrite

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect und dem Bandlaufwerk erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen. Der Wert READWRITE hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

Wird der Parameter LBPROTECT auf READWRITE gesetzt, müssen Sie nicht den Parameter CRCDATA in einer Speicherpooldefinition angeben, da der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust bereitstellt.

#### WRITEOnly

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk nur für Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Für Leseoperationen überprüfen der Server und das Bandlaufwerk nicht die CRC-Informationen. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect zum Generieren der CRC-Informationen und für das Bandlaufwerk zum Berechnen und Vergleichen der CRC-Werte für Schreiboperationen erforderlich ist. Der Wert WRITEONLY hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

#### No

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen nicht aktiviert ist. Der Server aktiviert jedoch den Schutz logischer Blöcke bei Schreiboperationen für einen sich füllenden Datenträger, der bereits über Daten mit dem Schutz logischer Blöcke verfügt.

Einschränkung: Der Schutz logischer Blöcke wird nur für IBM® 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher unterstützt.

In Technote 1634851, Additional information on the Tivoli Storage Manager LBProtect option, wird erläutert, wann der Parameter LBProtect zu verwenden ist.

## SCALECAPacity

Gibt den Prozentsatz der Datenträgerkapazität an, der zum Speichern von Daten verwendet werden kann. Dieser Parameter ist wahlfrei. Gültige Werte sind 20, 90 oder 100.

Wird für SCALECAPacity der Wert 100 angegeben, wird die maximale Speicherkapazität zur Verfügung gestellt. Wird der Wert 20 angegeben, wird die schnellste Zugriffszeit zur Verfügung gestellt.

Anmerkung: Der Wert für SCALECAPacity wird wirksam, wenn Daten zum ersten Mal auf einen Datenträger geschrieben werden. Alle Aktualisierungen an der Einheitenklasse für SCALECAPacity haben erst dann Auswirkungen auf Datenträger, auf die bereits Daten geschrieben wurden, wenn die Datenträger wieder in den Arbeitsdatenträgerstatus versetzt werden.

## FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Geben Sie stattdessen das Format an, das die Laufwerke verwenden.

In der folgenden Tabelle sind die Aufzeichnungsformate, die geschätzten Kapazitäten und die Optionen der Aufzeichnungsformate für 3592-Einheiten aufgelistet.

Tipp: Der Formatname wird beispielsweise als 3592-X, 3592-XC, 3592-XA oder 3592-XAC angegeben. Dabei gibt X die Laufwerkgeneration, C ein komprimiertes Format und A ein Archivierungslaufwerk an.

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für 3592

| Format  | Geschätzte Kapazität | Beschreibung   |
|---|----------------------|--|
| DRIVE   | –                    | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| 3592  | 300 GB               | Dekomprimiertes (Basis-)Format   |
| 3592C   | Siehe Anmerkung.     | Komprimiertes Format   |
| 3592-2  | 500 GB               | JA-Bänder mit dekomprimiertem (Basis-)Format   |
|   | 700 GB               | JB-Bänder mit dekomprimiertem (Basis-)Format   |
| 3592-2C   | 1,5 TB               | JA-Bänder mit komprimiertem Format   |
|   | 2,1 TB               | JB-Bänder mit komprimiertem Format   |
| 3592-3  | 640 GB               | JA-Bänder mit dekomprimiertem (Basis-)Format   |
|   | 1 TB                 | JB-Bänder mit dekomprimiertem (Basis-)Format   |
| 3592-3C   | 1,9 TB               | JA-Bänder mit komprimiertem Format   |
|   | 3 TB                 | JB-Bänder mit komprimiertem Format   |
| 3592-4  | 400 GB               | JK-Bänder mit dekomprimiertem (Basis-)Format   |
|   | 1,5 TB               | JB-Bänder mit dekomprimiertem (Basis-)Format   |
|   | 3,1 TB               | JC-Bänder mit dekomprimiertem (Basis-)Format   |
| 3592-4C   | 1,2 TB               | JK-Bänder mit komprimiertem Format   |
|   | 4,4 TB               | JB-Bänder mit komprimiertem Format   |
|   | 9,4 TB               | JC-Bänder mit komprimiertem Format   |
| 3592-5<br>(Für IBM TS1150 Modell<br>3592 E08-Laufwerke<br>mit Produkt-ID<br>03592E08) | 900 GB               | JK-Bänder mit dekomprimiertem (Basis-)Format   |
|   | 7000 GB              | JC/JY-Bänder mit dekomprimiertem (Basis-)Format  |
|   | 2000 GB              | JL-Bänder mit dekomprimiertem (Basis-)Format   |
|   | 10.000 GB            | JD/JZ-Bänder mit dekomprimiertem (Basis-)Format  |

| Format   | Geschätzte Kapazität                               | Beschreibung   |
|--|--|--|
| 3592-5C<br><br>(Für IBM TS1150 Modell<br>3592 E08-Laufwerke<br>mit Produkt-ID<br>03592E08)   | Hängt von der<br>Komprimierbarkeit der<br>Daten ab | JK-Bänder mit komprimiertem Format<br><br>JC/JY-Bänder mit komprimiertem Format<br><br>JL-Bänder mit komprimiertem Format<br><br>JD/JZ-Bänder mit komprimiertem Format |
| 3592-5A<br><br>(Für IBM TS1155 Modell<br>3592 55F-Laufwerke<br>mit Produkt-ID<br>0359255F)   | 3000 GB<br><br>15.000 GB                           | JL-Bänder mit dekomprimiertem (Basis-)Format<br><br>JD/JZ-Bänder mit dekomprimiertem (Basis-)Format  |
| 3592-5AC<br><br>(Für IBM TS1155 Modell<br>3592 55F-Laufwerke<br>mit Produkt-ID<br>0359255F)  | Hängt von der<br>Komprimierbarkeit der<br>Daten ab | JL-Bänder mit komprimiertem Format<br><br>JD/JZ-Bänder mit komprimiertem Format  |
| Anmerkung: Verwendet dieses Format die Komprimierungsfunktion für Bandlaufwerke, kann je nach Effektivität der Komprimierung die tatsächliche Kapazität von der geschätzten Kapazität abweichen. |  |  |

Wichtig: Um eine optimale Leistung zu erzielen, sollte das Mischen von Laufwerken verschiedener Generationen in einem einzelnen SCSI-Kassettenarchiv vermieden werden.

Spezielle Konfigurationen sind auch erforderlich, wenn verschiedene Generationen von 3592-Laufwerken in 349x- und ACSLS-Kassettenarchiven gemischt werden.

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

#### DRIVEEncryption

Gibt an, ob die Laufwerkverschlüsselung zulässig ist. Dieser Parameter ist wahlfrei.

Die Aktualisierung dieses Parameters wirkt sich nur auf leere Datenträger aus. War ein Datenträger, der gefüllt wurde, zuvor verschlüsselt, oder ist der Datenträger nicht verschlüsselt, und wird der Parameter DRIVEENCRYPTION aktualisiert, behält der Datenträger seinen ursprünglichen verschlüsselten oder nicht verschlüsselten Status. Der Datenträger behält außerdem seinen ursprünglichen Schlüsselverwaltungsstatus.

#### ON

Gibt an, dass IBM Spectrum Protect der Schlüsselmanager für die Laufwerkverschlüsselung ist und die Laufwerkverschlüsselung für leere Speicherpooldatenträger nur erlaubt, wenn das Anwendungsverfahren aktiviert ist. (Andere Typen von Datenträgern, wie beispielsweise Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger, werden nicht verschlüsselt.) Wird ON angegeben und entweder das Kassettenarchivverfahren oder das Systemverfahren der Verschlüsselung aktiviert, ist die Laufwerkverschlüsselung nicht zulässig, und Sicherungsoperationen schlagen fehl.

#### ALLOW

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Die Laufwerkverschlüsselung für leere Datenträger ist jedoch erlaubt, wenn entweder das Kassettenarchivverfahren oder das Systemverfahren der Verschlüsselung aktiviert ist.

#### EXTERNAL

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Verwenden Sie diese Einstellung mit einer Verschlüsselungsmethodik, die von einem anderen Anbieter zur Verfügung gestellt wird und die mit

dem Anwendungsverfahren der Verschlüsselung verwendet wird, das für das Laufwerk aktiviert ist. Geben Sie EXTERNAL an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect nicht inaktiviert. Geben Sie dagegen ALLOW an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect inaktiviert.

OFF

Gibt an, dass die Laufwerkverschlüsselung nicht zulässig ist. Wird entweder das Kassettenarchivverfahren oder das Systemverfahren der Verschlüsselung aktiviert, schlagen Sicherungen fehl. Wird das Anwendungsverfahren aktiviert, inaktiviert IBM Spectrum Protect die Verschlüsselung, und die Ausführung von Sicherungen wird versucht.

## UPDATE DEVCLASS (Einheitenklasse 4MM aktualisieren)

Verwenden Sie die Einheitenklasse 4MM, wenn Sie 4-mm-Bandeinheiten verwenden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-UPDate DEVclass--Einheitenklassenname----->
>+-----+----->
  '-LIBRARY----Kassettenarchivname- '
>+-----+----->
  '-FORMAT----+DRIVE+-'  '-ESTCAPacity----Größe- '
      +-DDS1--+
      +-DDS1C--+
      +-DDS2--+
      +-DDS2C--+
      +-DDS3--+
      +-DDS3C--+
      +-DDS4--+
      +-DDS4C--+
      +-DDS5--+
      +-DDS5C--+
      +-DDS6--+
      '-DDS6C- '
>+-----+----->
  '-PREFIX----+ADSM-----+- '
      '-Banddatenträgerpräfix- '
>+-----+----->
  '-MOUNTWait---Minuten- '  '-MOUNTRetention----Minuten- '
>+-----+-----<
  '-MOUNTLimit-----+DRIVES+- '
      +-Anzahl+-
      '-0----- '

```

### Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an.

LIBRARY

Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten 4-mm-Bandlaufwerke enthält. Dieser Parameter ist wahlfrei. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Geben Sie stattdessen das Format an, das die Laufwerke verwenden.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für 4-mm-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für 4-mm-Bänder

| Format   | Geschätzte Kapazität                                      | Beschreibung   |
|--|---|--|
| DRIVE  | –   | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| DDS1   | 1,3 GB (60 Meter)<br>2,0 GB (90 Meter)                    | Dekomprimiertes Format, gilt nur für 60-Meter-Bänder und 90-Meter-Bänder   |
| DDS1C  | Siehe Anmerkung<br>1,3 GB (60 Meter)<br>2,0 GB (90 Meter) | Komprimiertes Format, gilt nur für 60-Meter-Bänder und 90-Meter-Bänder   |
| DDS2   | 4,0 GB  | Dekomprimiertes Format, gilt nur für 120-Meter-Bänder  |
| DDS2C  | Siehe Anmerkung<br>8,0 GB                                 | Komprimiertes Format, gilt nur für 120-Meter-Bänder  |
| DDS3   | 12,0 GB   | Dekomprimiertes Format, gilt nur für 125-Meter-Bänder  |
| DDS3C  | Siehe Anmerkung<br>24,0 GB                                | Komprimiertes Format, gilt nur für 125-Meter-Bänder  |
| DDS4   | 20,0 GB   | Dekomprimiertes Format, gilt nur für 150-Meter-Bänder  |
| DDS4C  | Siehe Anmerkung<br>40,0 GB                                | Komprimiertes Format, gilt nur für 150-Meter-Bänder  |
| DDS5   | 36 GB   | Dekomprimiertes Format bei Verwendung von DAT 72-Datenträgern  |
| DDS5C  | Siehe Anmerkung<br>72 GB                                  | Komprimiertes Format bei Verwendung von DAT 72-Datenträgern  |
| DDS6   | 80 GB   | Dekomprimiertes Format bei Verwendung von DAT 160-Datenträgern   |
| DDS6C  | Siehe Anmerkung<br>160 GB                                 | Komprimiertes Format bei Verwendung von DAT 160-Datenträgern   |
| Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann die tatsächliche Kapazität abhängig von der Effektivität der Komprimierung größer als der aufgelistete Wert sein. |   |  |

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger mit sequenziellem Zugriff an, die durch diese Einheitenklasse kategorisiert werden. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: K (Kilobyte), M (Megabyte), G (Gigabyte) oder T (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

Für weitere Informationen zur geschätzten Standardkapazität für 4-mm-Bänder siehe Tabelle 1.

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

## UPDATE DEVCLASS (Einheitenklasse 8MM aktualisieren)

Verwenden Sie die Einheitenklasse 8MM, wenn Sie 8-mm-Bandeinheiten verwenden.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-UPDate DEVclass--Einheitenklassenname----->
>+-----+----->
  '-LIBRARY---Kassettenarchivname-'
>+-----+----->
  '-FORMAT---+DRIVE+-'  '-ESTCAPacity---Größe-'
      +-8200--+
      +-8200C+
      +-8500--+
      +-8500C+
      +-8900--+
      +-AIT----+
      +-AITC--+
      +-M2-----+
      +-M2C---+
      +-SAIT--+
      +-SAITC+
      +-VXA2--+
      +-VXA2C+
      +-VXA3--+
      '-VXA3C-'
>+-----+----->
  '-PREFIX---+ADSM-----+-'
      '-Banddatenträgerpräfix-'
>+-----+----->
  '-MOUNTRetention---Minuten-'  '-MOUNTWait---Minuten-'
>+-----+-----<
  '-MOUNTLimit-----+DRIVES+-'
      +-Anzahl+
      '-0-----'
```

## Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

LIBRARY

Gibt den Namen des definierten Kassettenarchivobjekts an, das die 8-mm-Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können. Weitere Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Geben Sie stattdessen das Format an, das die Laufwerke verwenden.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für 8-mm-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformat und geschätzte Standardkapazität für 8-mm-Band

| Format         |                      | Beschreibung  |
|----------------|----------------------|---|
| Datenträgertyp | Geschätzte Kapazität |   |
| DRIVE          | –                    | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |



| <b>Format</b>   |   | <b>Beschreibung</b>  |
|---|---|--|
| <b>Datenträgertyp</b>   | <b>Geschätzte Kapazität</b>   |  |
| 8200  | 2,3 GB  | Dekomprimiertes (Standard) Format, verwendet 112-Meter-Standardbandkassetten   |
| 8200C   | Siehe Anmerkung<br>3,5 GB<br>4,6 GB   | Komprimiertes Format, verwendet 112-Meter-Standardbandkassetten  |
| 8500<br>15 m<br>15 m<br>15 m<br>54 m<br>54 m<br>54 m<br>112 m<br>112 m<br>112 m<br>160 m XL               | Siehe Anmerkung<br>600 MB<br>600 MB<br>600 MB<br>2,35 GB<br>2,35 GB<br>2,35 GB<br>5 GB oder 10,0 GB<br>5 GB oder 10,0 GB<br>5 GB oder 10,0 GB<br>7 GB | Laufwerke (Lesen/Schreiben)<br>Eliant 820 (LS)<br>Exabyte 8500/8500C (LS)<br>Exabyte 8505 (LS)<br>Eliant 820 (LS)<br>Exabyte 8500/8500C (LS)<br>Exabyte 8505 (LS)<br>Eliant 820 (LS)<br>Exabyte 8500/8500C (LS)<br>Exabyte 8505 (LS)<br>Eliant 820 (LS)    |
| 8500C<br>15 m<br>15 m<br>15 m<br>54 m<br>54 m<br>54 m<br>112 m<br>112 m<br>112 m<br>160 m XL              | Siehe Anmerkung<br>1,2 GB<br>1,2 GB<br>1,2 GB<br>4,7 GB<br>4,7 GB<br>4,7 GB<br>5 GB oder 10,0 GB<br>5 GB oder 10,0 GB<br>5 GB oder 10,0 GB<br>7 GB    | Laufwerke (Lesen/Schreiben)<br>Eliant 820 (LS)<br>Exabyte 8500/8500C (LS)<br>Exabyte 8505 (LS)<br>Eliant 820 (LS)<br>Exabyte 8500/8500C (LS)<br>Exabyte 8505 (LS)<br>Eliant 820 (LS)<br>Exabyte 8500/8500C (LS)<br>Exabyte 8505 (LS)<br>Eliant 820 (LS)    |
| 8900<br>15 m<br>54 m<br>112 m<br>160 m XL<br>22 m<br>125 m<br>170 m                                       | Siehe Anmerkung<br>----2,5 GB<br>-40 GB   | Laufwerk (Lesen/Schreiben)<br>Mammoth 8900 (L)<br>Mammoth 8900 (L)<br>Mammoth 8900 (L)<br>Mammoth 8900 (L)<br>Mammoth 8900 (LS)<br>Mammoth 8900 (LS mit Upgrade)<br>Mammoth 8900 (LS)  |
| AIT<br>SDX1-25C<br>SDX1-35C<br>SDX2-36C<br>SDX2-50C<br>SDX3-100C<br>SDX3X-150C<br>SDX4-200C<br>SDX5-400C  | Siehe Anmerkung<br>25 GB<br>35 GB<br>36 GB50 GB<br>100 GB150 GB200 GB400 GB   | Laufwerk<br>AIT-, AIT2- und AIT3-Laufwerke<br>AIT-, AIT2- und AIT3-Laufwerke<br>AIT2- und AIT3-Laufwerke<br>AIT2- und AIT3-Laufwerke<br>AIT3-, AIT4- und AIT5-Laufwerke<br>AIT3-Ex-, AIT4- und AIT5-Laufwerke<br>AIT4- und AIT5-Laufwerke<br>AIT5-Laufwerk |
| AITC<br>SDX1-25C<br>SDX1-35C<br>SDX2-36C<br>SDX2-50C<br>SDX3-100C<br>SDX3X-150C<br>SDX4-200C<br>SDX5-400C | Siehe Anmerkung<br>50 GB<br>91 GB<br>72 GB130 GB<br>260 GB<br>390 GB<br>520 GB<br>1040 GB   | Laufwerk<br>AIT-, AIT2- und AIT3-Laufwerke<br>AIT-, AIT2- und AIT3-Laufwerke<br>AIT2- und AIT3-Laufwerke<br>AIT2- und AIT3-Laufwerke<br>AIT3-, AIT4- und AIT5-Laufwerke<br>AIT3-Ex-, AIT4- und AIT5-Laufwerke<br>AIT4- und AIT5-Laufwerke<br>AIT5-Laufwerk |

| <b>Format</b>  |  | <b>Beschreibung</b>   |
|--|--|---|
| <b>Datenträgertyp</b>  | <b>Geschätzte Kapazität</b>                            |   |
| M2<br>75 m<br>150 m<br>225 m   | Siehe Anmerkung<br><br>20,0 GB40,0 GB60,0 GB           | Laufwerk (Lesen/Schreiben)<br><br>Mammoth II (LS)<br>Mammoth II (LS)<br>Mammoth II (LS) |
| M2C<br>75 m<br>150 m<br>225 m  | Siehe Anmerkung<br><br>50,0 GB<br>100,0 GB<br>150,0 GB | Laufwerk (Lesen/Schreiben)<br><br>Mammoth II (LS)<br>Mammoth II (LS)<br>Mammoth II (LS) |
| SAIT   | Siehe Anmerkung<br><br>500 GB                          | Laufwerk (Lesen/Schreiben)<br><br>Sony SAIT1-500 (LS)                                   |
| SAITC  | Siehe Anmerkung<br><br>1300 GB (1,3 TB)                | Laufwerk (Lesen/Schreiben)<br><br>Sony SAIT1-500 (LS)                                   |
| VXA2<br>V6 (62 m)<br>V10 (124 m)<br>V17 (170 m)  | Siehe Anmerkung<br><br>20 GB40 GB60 GB                 | Laufwerk (Lesen/Schreiben)<br><br>VXA-2   |
| VXA2C<br>V6 (62 m)<br>V10 (124 m)<br>V17 (170 m)   | Siehe Anmerkung<br><br>40 GB80 GB120 GB                | Laufwerk (Lesen/Schreiben)<br><br>VXA-2   |
| VXA3<br>X6 (62 m)<br>X10 (124 m)<br>X23 (230 m)  | Siehe Anmerkung<br><br>40 GB86 GB<br>160 GB            | Laufwerk (Lesen/Schreiben)<br><br>VXA-3   |
| VXA3C<br>X6 (62 m)<br>X10 (124 m)<br>X23 (230 m)   | Siehe Anmerkung<br><br>80 GB172 GB<br>320 GB           | Laufwerk (Lesen/Schreiben)<br><br>VXA-3   |
| <p>Anmerkung: Die tatsächlichen Kapazitäten können abhängig von den verwendeten Kassetten und Laufwerken variieren.</p> <ul style="list-style-type: none"> <li>• Für das AITC- und SAITC-Format ist das normale Komprimierungsverhältnis 2,6:1.</li> <li>• Für das M2C-Format ist das normale Komprimierungsverhältnis 2,5:1.</li> </ul> |  |   |

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

Für weitere Informationen zur geschätzten Standardkapazität für 8-mm-Bänder siehe Tabelle 1.

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist,

verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist AD5M.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

## Beispiel: Den Grenzwert für Ladeanforderungen und die Kapazität einer 8-mm-Einheitenklasse aktualisieren

Die Einheitenklasse 8MMTAPE aktualisieren. Den Grenzwert für Ladeanforderungen in 3 und die geschätzte Kapazität in 10 GB ändern.

```
update devclass 8mmtape mountlimit=3 estcapacity=10G
```

## Beispiel: Die Ladedauer einer 8-mm-Einheitenklasse aktualisieren

---

Für die 8-mm-Einheitenklasse 8MMTAPE soll eine Ladedauer von 15 Minuten definiert werden.

```
update devclass 8mmtape mountretention=15
```

## UPDATE DEVCLASS (Einheitenklasse CENTERA aktualisieren)

---

Verwenden Sie die Einheitenklasse CENTERA, wenn Sie EMC Centera-Speichereinheiten verwenden. Der Einheitentyp CENTERA verwendet Dateien als Datenträger zum sequenziellen Speichern von Daten. Er ähnelt der Einheitenklasse FILE.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
>>-UPDate DEVclass--Einheitenklassenname----->
                                     (1)
>--HLAddress-----IP-Adresse?PEA-Datei----->
>+-----+----->
  '-MINCAPacity-----Größe---'
>+-----+-----<
  '-MOUNTLimit-----Anzahl---'
```

Anmerkungen:

1. Für jede Centera-Einheitenklasse müssen Sie eine IP-Adresse angeben. Ein PEA-Dateiname und -Pfad (PEA = Pool Entry Authorization) sind jedoch optional, und die PEA-Dateispezifikation muss auf die IP-Adresse folgen. Verwenden Sie das Zeichen "?", um den PEA-Dateinamen und -Pfad von der IP-Adresse zu trennen.

## Parameter

---


Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

HLAddress

Gibt eine IP-Adresse für die Centera-Speichereinheit und optional den Namen und Pfad einer PEA-Datei (PEA = Pool Entry Authorization) an. Geben Sie die IP-Adresse in Schreibweise mit Trennzeichen an (beispielsweise 9.10.111.222). Eine Centera-Einheit kann mehrere IP-Adressen haben. Sie müssen jedoch nur eine Adresse als Wert für diesen Parameter angeben.

 AIX-Betriebssysteme Bei dem PEA-Dateinamen und -Pfadnamen muss die Groß-/Kleinschreibung beachtet werden.

Werden Name und Pfad einer PEA-Datei angehängt, stellen Sie sicher, dass die Datei in einem Verzeichnis auf dem System gespeichert wird, auf dem der IBM Spectrum Protect-Server ausgeführt wird. Verwenden Sie das Zeichen "?", um den PEA-Dateinamen und -Pfad von der IP-Adresse oder den IP-Adressen zu trennen. Beispiel:  Windows-Betriebssysteme

```
HLADDRESS=9.10.111.222?c:\controlFiles\TSM.PEA
```

 AIX-Betriebssysteme

```
HLADDRESS=9.10.111.222?/user/ControlFiles/TSM.PEA
```

Geben Sie nur einen PEA-Dateinamen und Pfad für jede Einheitenklassendefinition an. Geben Sie zwei verschiedene Centera-Einheitenklassen an, die auf dieselbe Centera-Speichereinheit zeigen, und enthalten die Einheitenklassendefinitionen verschiedene PEA-Dateinamen und -Pfade, verwendet der Server die PEA-Datei, die im Einheitenklassenparameter HLADDRESS angegeben ist, der zuerst zum Öffnen der Centera-Speichereinheit verwendet wurde.

Anmerkung:

1. Der Server schließt während der Installation keine PEA-Datei ein. Wenn Sie keine PEA-Datei erstellen, verwendet der Server das Centera-Standardprofil, mit dem es Anwendungen erlaubt werden kann, Daten auf einer Centera-Speichereinheit zu lesen, zu schreiben, zu löschen und abzufragen. Um eine genauere Steuerung zu ermöglichen, erstellen Sie eine PEA-Datei mit der Befehlszeilenschnittstelle, die von EMC Centera zur Verfügung gestellt wird. Ausführliche Informationen zur Centera-Authentifizierung und -Berechtigung befinden sich im EMC Centera *Programmer's Guide*.
2. Sie können den PEA-Dateinamen und -Pfad auch in einer Umgebungsvariablen unter Verwendung der Syntax `CENTERA_PEA_LOCATION=Dateipfad_ Dateiname` angeben. Der mit dieser Umgebungsvariablen angegebene PEA-Dateiname und -Pfad gilt für alle Centera-Cluster. Wird diese Variable verwendet, müssen Sie keinen PEA-Dateinamen und -Pfad mit dem Parameter `HLADDRESS` angeben.
3. Die Aktualisierung der Einheitenklasse mit einem neuen oder geänderten PEA-Dateinamen und einer neuen oder geänderten Position kann einen Neustart des Servers erfordern, wenn auf die durch die IP-Adresse identifizierte Centera-Speichereinheit bereits in der aktuellen Instanz des Servers zugegriffen wurde.

#### MINCAPacity

Gibt die neue Mindestgröße für Centera-Datenträger an, die einem Speicherpool in dieser Einheitenklasse zugeordnet sind. Dieser Wert stellt das Mindestdatenvolumen dar, das auf einem Centera-Datenträger gespeichert wird, bevor der Server den Datenträger als voll kennzeichnet. Centera-Datenträger akzeptieren weiterhin Daten, bis das Mindestdatenvolumen gespeichert wurde. Dieser Parameter ist wahlfrei.

#### Größe

Dieser Wert muss als ganze Zahl gefolgt von einem **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte) angegeben werden. Der zulässige Mindestwert ist 1 MB (`MINCAPACITY=1M`). Der zulässige Maximalwert ist 128 GB (`MINCAPacity=128G`).

#### MOUNTLimit

Gibt die neue maximale Anzahl der Sitzungen an, die auf die Centera-Einheit zugreifen. Dieser Parameter ist wahlfrei. Sie können eine beliebige Zahl von 0 aufwärts angeben; die Summe aller Grenzwerte für Ladeanforderungen für alle Einheitenklassen, die derselben Centera-Einheit zugeordnet sind, darf jedoch die maximale Anzahl der von Centera erlaubten Sitzungen nicht überschreiten.

## UPDATE DEVCLASS (Einheitenklasse DLT aktualisieren)

Verwenden Sie die Einheitenklasse DLT, wenn Sie DLT-Bandeinheiten verwenden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-UPDate DEVclass--Einheitenklassenname----->
>--+-----+----->
  '-LIBRARY----Kassettenarchivname- '
>--+-----+----->
  '-FORMAT-----+DRIVE-----'  '-ESTCAPacity----Größe- '
      +-DLT1-----+
      +-DLT1C-----+
      +-DLT10-----+
      +-DLT10C-----+
      +-DLT15-----+
      +-DLT15C-----+
      +-DLT20-----+
      +-DLT20C-----+
      +-DLT35-----+
      +-DLT35C-----+
      +-DLT40-----+
      +-DLT40C-----+
      +-DLT2-----+
      +-DLT2C-----+
      +-DLT4-----+
      +-DLT4C-----+
      +-SDLT-----+
      +-SDLTC-----+
      +-SDLT320---+
      +-SDLT320C--+
      +-SDLT600---+
```

```

++SDLT600C++
+-DLTS4-----+
'-DLTS4C-----'

>+-----+-----+-----+-----+----->
'-PREFIX-----+ADSM-----+-'
  '-Banddatenträgerpräfix-'

>+-----+-----+-----+-----+----->
'-MOUNTRetention-----Minuten-' '-MOUNTWait-----Minuten-'

>+-----+-----+-----+-----+-----<
'-MOUNTLimit-----+DRIVES+-+'
      +-Anzahl+
      '-0-----'

```

## Parameter

### Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

### LIBRARY

Gibt den Namen des definierten Kassettenarchivobjekts an, das die DLT-Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

### FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Geben Sie stattdessen das Format an, das die Laufwerke verwenden.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für DLT-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformat und geschätzte Standardkapazität für DLT

| Format | Geschätzte Kapazität | Beschreibung   |
|--------|----------------------|--|
| DRIVE  | –                    | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| DLT1   | 40,0 GB              | Dekomprimiertes Format, verwendet nur CompacTape III- oder CompacTape IV-Kassetten   |
| DLT1C  | Siehe 1.<br>80,0 GB  | Komprimiertes Format, verwendet nur CompacTape III- und CompacTape IV-Kassetten  |
| DLT10  | 10,0 GB              | Dekomprimiertes Format, verwendet nur CompacTape III- oder CompacTape IV-Kassetten   |
| DLT10C | Siehe 1.<br>20,0 GB  | Komprimiertes Format, verwendet nur CompacTape III- und CompacTape IV-Kassetten  |
| DLT15  | 15,0 GB              | Dekomprimiertes Format, verwendet nur CompacTape IIIxt- oder CompacTape IV-Kassetten (nicht CompacTape III)<br>Anmerkung: Gültig für DLT2000XT-, DLT4000- und DLT7000-Laufwerke  |
| DLT15C | Siehe 1.<br>30,0 GB  | Komprimiertes Format, verwendet nur CompacTape IIIxt- oder CompacTape IV-Kassetten (nicht CompacTape III)<br>Gültig für DLT2000XT-, DLT4000- und DLT7000-Laufwerke   |
| DLT20  | 20,0 GB              | Dekomprimiertes Format, verwendet nur CompacTape IV-Kassetten<br>Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke   |

| <b>Format</b>  | <b>Geschätzte Kapazität</b> | <b>Beschreibung</b>   |
|--|-----------------------------|---|
| DLT20C   | Siehe 1.<br>40,0 GB         | Komprimiertes Format, verwendet nur CompactTape IV-Kassetten<br>Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke |
| DLT35  | 35,0 GB                     | Dekomprimiertes Format, verwendet nur CompactTape IV-Kassetten<br>Gültig für DLT7000- und DLT8000-Laufwerke         |
| DLT35C   | Siehe 1.<br>70,0 GB         | Komprimiertes Format, verwendet nur CompactTape IV-Kassetten<br>Gültig für DLT7000- und DLT8000-Laufwerke           |
| DLT40  | 40,0 GB                     | Dekomprimiertes Format, verwendet CompactTape IV-Kassetten<br>Gültig für DLT8000-Laufwerk                           |
| DLT40C   | Siehe 1.<br>80,0 GB         | Komprimiertes Format, verwendet CompactTape IV-Kassetten<br>Gültig für DLT8000-Laufwerk                             |
| DLT2   | 80,0 GB                     | Dekomprimiertes Format, verwendet Quantum DLT VS1-Banddatenträger   |
| DLT2C  | Siehe 1.<br>160,0 GB        | Komprimiertes Format, verwendet Quantum DLT VS1-Banddatenträger   |
| DLT4   | 160,0 GB                    | Dekomprimiertes Format, verwendet Quantum DLTtape VS1-Kassetten.<br>Gültig für Quantum DLT-V4-Laufwerk              |
| DLT4C  | Siehe 1.<br>320,0 GB        | Komprimiertes Format, verwendet Quantum DLTtape VS1-Kassetten.<br>Gültig für Quantum DLT-V4-Laufwerk                |
| SDLT<br>Siehe 2.   | 100,0 GB                    | Dekomprimiertes Format, verwendet Super DLT Tape 1-Kassetten<br>Gültig für Super DLT-Laufwerk                       |
| SDLTC<br>Siehe 2.  | Siehe 1.<br>200,0 GB        | Komprimiertes Format, verwendet Super DLT Tape 1-Kassetten<br>Gültig für Super DLT-Laufwerk                         |
| SDLT320<br>Siehe 2.  | 160,0 GB                    | Dekomprimiertes Format, verwendet Quantum SDLT I-Datenträger<br>Gültig für Super DLT-Laufwerk                       |
| SDLT320C<br>Siehe 2.   | Siehe 1.<br>320,0 GB        | Komprimiertes Format, verwendet Quantum SDLT I-Datenträger<br>Gültig für Super DLT-Laufwerk                         |
| SDLT600  | 300,0 GB                    | Dekomprimiertes Format, verwendet SuperDLTtape-II-Datenträger<br>Gültig für Super DLT-Laufwerk                      |
| SDLT600C   | Siehe 1.<br>600,0 GB        | Komprimiertes Format, verwendet SuperDLTtape-II-Datenträger<br>Gültig für Super DLT-Laufwerk                        |
| DLTS4  | 800 GB                      | Dekomprimiertes Format, verwendet Quantum DLT S4-Datenträger.<br>Gültig für ein DLT-S4-Laufwerk                     |
| DLTS4C   | Siehe 1.<br>1,6 TB          | Komprimiertes Format, verwendet Quantum DLT S4-Datenträger.<br>Gültig für ein DLT-S4-Laufwerk                       |
| <b>Anmerkung:</b><br>1. Je nach Effektivität der Komprimierung kann die tatsächliche Kapazität größer als der aufgeführte Wert sein.<br>2. IBM Spectrum Protect unterstützt kein Kassettenarchiv, das sowohl Backward Read Compatible (BRC) SDLT- als auch Non-Backward Read Compatible (NBRC) SDLT-Laufwerke enthält. |                             |   |

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

Für weitere Informationen zu geschätzten Kapazitäten siehe Tabelle 1.

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

DRIVES



Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl



Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

## UPDATE DEVCLASS (Einheitenklasse ECARTRIDGE aktualisieren)

Verwenden Sie die Einheitenklasse ECARTRIDGE, wenn Sie StorageTek-Laufwerke wie beispielsweise StorageTek T9840 oder T10000 verwenden.

  Wenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in UPDATE DEVCLASS (Einheitenklasse ECARTRIDGE für z/OS Media-Server aktualisieren).

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-UPDate DEVclass--Einheitenklassenname----->
>--+-----+----->
  '-LIBRARY----Kassettenarchivname- '
>--+-----+----->
  '-LBProtect----+READWrite-+- '
    +-WRITEOnly-+
    '-No----- '
>--+-----+----->
  '-FORMAT----+DRIVE-----+' '-ESTCAPacity----Größe- '
    +-T9840C----+
    +-T9840C-C--+
    +-T9840D----+
    +-T9840D-C--+
    +-T10000A----+
    +-T10000A-C+
    +-T10000B----+
    +-T10000B-C+
    +-T10000C----+
    +-T10000C-C+
    +-T10000D----+
    '-T10000D-C- '
>--+-----+----->
  '-PREFIX----+ADSM-----+'
    '-Banddatenträgerpräfix- '
>--+-----+----->
  '-MOUNTRetention----+Minuten- ' '-MOUNTWait----+Minuten- '
>--+-----+----->
  '-MOUNTLimit----+DRIVES-+- '
    +-Anzahl-+
    '-0----- '
>--+-----+-----<
  | (1) (2) |
  '------DRIVEEncryption----+ON-----+'
    +-ALLOW----+
    +-EXTERNAL-+
```

Anmerkungen:

1. Sie können die Laufwerkverschlüsselung nur für Oracle StorageTek T10000B-Laufwerke mit dem Formatwert DRIVE, T10000B oder T10000B-C, für Oracle StorageTek T10000C-Laufwerke mit dem Formatwert DRIVE, T10000C oder T10000C-C und für Oracle StorageTek T10000D-Laufwerke mit dem Formatwert DRIVE, T10000D und T10000D-C verwenden.
2. Sie können nicht WORM=YES in Verbindung mit DRIVEENCRYPTION=ON angeben.

## Parameter

### Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

### LIBRARY

Gibt den Namen des definierten Kassettenarchivobjekts mit den ECARTRIDGE-Bandlaufwerken an, die von dieser Einheitenklasse verwendet werden können. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

### LBProtect

Gibt an, ob der Schutz logischer Blöcke verwendet wird, um die Integrität von Daten sicherzustellen, die auf Band gespeichert sind. Wenn LBPROTECT auf READWRITE oder WRITEONLY gesetzt ist, verwendet der Server dieses Feature des Bandlaufwerks für den Schutz logischer Blöcke und generiert CRC-Zugriffsschutzinformationen für jeden Datenblock, der auf Band geschrieben wird. Der Server überprüft auch die CRC-Zugriffsschutzinformationen, wenn Daten von dem Band gelesen werden.

Die folgenden Werte sind gültig:

#### READWRITE

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect und dem Bandlaufwerk erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen. Der Wert READWRITE hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

Wird der Parameter LBPROTECT auf READWRITE gesetzt, müssen Sie nicht den Parameter CRCDATA in einer Speicherpooldefinition angeben, da der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust bereitstellt.

#### WRITEONLY

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk nur für Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Für Leseoperationen überprüfen der Server und das Bandlaufwerk nicht die CRC-Informationen. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect zum Generieren der CRC-Informationen und für das Bandlaufwerk zum Berechnen und Vergleichen der CRC-Werte für Schreiboperationen erforderlich ist. Der Wert WRITEONLY hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

#### No

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen nicht aktiviert ist. Der Server aktiviert jedoch den Schutz logischer Blöcke bei Schreiboperationen für einen sich füllenden Datenträger, der bereits über Daten mit dem Schutz logischer Blöcke verfügt.

Einschränkung: Der Schutz logischer Blöcke wird nur auf Oracle StorageTek T10000C- und Oracle StorageTek T10000D-Laufwerken unterstützt.

### FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Geben Sie stattdessen das Format an, das die Laufwerke verwenden.

Wichtig: Wird DRIVE für eine Einheitenklasse angegeben, die über inkompatible Einheiten mit sequenziellem Zugriff verfügt, müssen Datenträger in Einheiten geladen werden, die in dem Format lesen oder schreiben können, das beim ersten Laden des Datenträgers eingerichtet wurde. Dies kann zu Verzögerungen führen, wenn die einzige Einheit mit sequenziellem Zugriff, die auf den Datenträger zugreifen kann, bereits im Gebrauch ist.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für ECARTRIDGE-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für ECARTRIDGE-Bänder

| Format | Geschätzte Kapazität | Beschreibung |
|--------|----------------------|--------------|
|--------|----------------------|--------------|

| Format   | Geschätzte Kapazität | Beschreibung   |
|--|----------------------|--|
| DRIVE  | –                    | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| T9840C   | 40 GB                | Dekomprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840C-C   | 80 GB                | Komprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840D   | 75 GB                | Dekomprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840D-C   | 150 GB               | Komprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette   |
| T10000A  | 500 GB               | Dekomprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette  |
| T10000A-C  | 1 TB                 | Komprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette  |
| T10000B  | 1 TB                 | Dekomprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette   |
| T10000B-C  | 2 TB                 | Komprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette   |
| T10000C  | 5 TB                 | Dekomprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000C-C  | 10 TB                | Komprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000D  | 8 TB                 | Dekomprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000D-C  | 15 TB                | Komprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| Anmerkungen:   |                      |  |
| <ul style="list-style-type: none"> <li>• Einige Formate verwenden die Datenkomprimierung über Hardware mittels Bandlaufwerk. Je nach Effektivität der Komprimierung kann die tatsächliche Kapazität doppelt so groß (oder größer) sein wie der aufgeführte Wert.</li> <li>• T10000A-Laufwerke können nur das T10000A-Format lesen und schreiben. T10000B-Laufwerke können das T10000A-Format lesen, aber nicht schreiben. T10000C-Laufwerke können die T10000A- und T10000B-Formate lesen, aber nicht schreiben. T10000D-Laufwerke können die T10000A-, T10000B- und T10000C-Formate lesen, aber nicht schreiben.</li> </ul> |                      |  |

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

Für weitere Informationen zur geschätzten Standardkapazität von Magnetbandkassetten siehe Tabelle 1.

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

#### DRIVEEncryption

Gibt an, ob die Laufwerkverschlüsselung zulässig ist. Dieser Parameter ist wahlfrei.

Einschränkung:

1. Sie können die Laufwerkverschlüsselung nur für die folgenden Laufwerke verwenden:

- Oracle StorageTek T10000B-Laufwerke, die den Formatwert DRIVE, T10000B oder T10000B-C haben
  - Oracle StorageTek T10000C-Laufwerke, die den Formatwert DRIVE, T10000C oder T10000C-C haben
  - Oracle StorageTek T10000D-Laufwerke, die den Formatwert DRIVE, T10000D oder T10000D-C haben
2. Sie können nicht IBM Spectrum Protect als Schlüsselmanager für die Laufwerkverschlüsselung von WORM-Datenträgern angeben (WORM - Write Once Read Many). (Die Angabe von WORM=YES in Verbindung mit DRIVEENCRYPTION=ON wird nicht unterstützt.)
  3. Ist die Verschlüsselung für eine Einheitenklasse aktiviert und ist die Einheitenklasse einem Speicherpool zugeordnet, sollte der Speicherpool nicht einen Arbeitsdatenträgerpool mit anderen Einheitenklassen gemeinsam nutzen, die nicht verschlüsselt werden können. Ist ein Band verschlüsselt und soll das Band in einem Laufwerk verwendet werden, das nicht verschlüsselt werden kann, müssen Sie das Band manuell mit einem neuen Kennsatz versehen, bevor es in diesem Laufwerk verwendet werden kann.

#### ON

Gibt an, dass IBM Spectrum Protect der Schlüsselmanager für die Laufwerkverschlüsselung ist und die Laufwerkverschlüsselung für leere Speicherpooldatenträger nur erlaubt, wenn das Anwendungsverfahren aktiviert ist. (Andere Typen von Datenträgern werden nicht verschlüsselt. Beispielsweise werden Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger nicht verschlüsselt.) Wird ON angegeben und ein anderes Verschlüsselungsverfahren aktiviert, ist die Laufwerkverschlüsselung nicht zulässig, und Sicherungsoperationen schlagen fehl.

#### ALLOW

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Die Laufwerkverschlüsselung für leere Datenträger ist jedoch zulässig, wenn ein anderes Verschlüsselungsverfahren aktiviert ist.

#### EXTERNAL

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Verwenden Sie diese Einstellung mit einer Verschlüsselungsmethodik, die von einem anderen Anbieter zur Verfügung gestellt wird und die mit dem Anwendungsverfahren der Verschlüsselung verwendet wird, das für das Laufwerk aktiviert ist. Geben Sie EXTERNAL an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect nicht inaktiviert. Geben Sie dagegen ALLOW an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect inaktiviert.

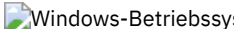
#### OFF


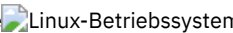
Gibt an, dass die Laufwerkverschlüsselung nicht zulässig ist. Wird ein anderes Verschlüsselungsverfahren aktiviert, schlagen Sicherungen fehl. Wird das Anwendungsverfahren aktiviert, inaktiviert IBM Spectrum Protect die Verschlüsselung, und die Ausführung von Sicherungen wird versucht.

## UPDATE DEVCLASS (Einheitenklasse FILE aktualisieren)

Verwenden Sie die Einheitenklasse FILE, wenn Dateien im Magnetplattenspeicher als Datenträger verwendet werden, die Daten sequenziell speichern (wie auf Band).

  Die Einheitenklasse FILE unterstützt keine Kassettenarchive EXTERNAL.

 Die Einheitenklasse FILE unterstützt keine Kassettenarchive EXTERNAL.

  Wenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in UPDATE DEVCLASS (Einheitenklasse FILE für z/OS Media-Server aktualisieren).

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-UPDate DEVclass--Einheitenklassenname----->
>--+-----+-----+-----+----->
  '-MOUNTLimit----Anzahl-'   '-MAXCAPacity----Größe-'
>--+-----+-----+-----+----->
  |           .-,'-----'. |
  |           v               |
  '-DIRectory----Verzeichnisname+-'
>--+-----+-----+-----+-----><
```

'-SHAREd-----+No--+-'  
'-Yes-'

## Parameter


---

### Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

### MOUNTLimit

Gibt die maximale Anzahl von Dateien an, die gleichzeitig für die Ein- und Ausgabe geöffnet sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

 Wird die Einheitenklasse mit einem Speicheragenten gemeinsam genutzt (durch Angabe des Parameters SHARED=YES), werden Laufwerke definiert oder gelöscht, um eine Übereinstimmung mit dem Wert für MOUNTLIMIT zu erreichen.



Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

### MAXCAPacity

Gibt die maximale Größe einer Datenspeicherdatei an, die durch diese Einheitenklasse kategorisiert wird. Dieser Parameter ist wahlfrei.

Dieser Wert muss als ganze Zahl gefolgt von einem K (Kilobyte), M (Megabyte), G (Gigabyte) oder T (Terabyte) angegeben werden. Die Mindestgröße ist 1 MB (MAXCAPACITY=1M). Wenn Sie eine Einheitenklasse FILE für Datenbanksicherungsdatenträger definieren, geben Sie einen Wert für MAXCAPACITY an, der für die Größe der Datenbank angemessen ist und der die Anzahl der Datenbankdatenträger minimiert.



MAXCAPACITY=5G gibt beispielsweise an, dass die maximale Kapazität eines Datenträgers in dieser Einheitenklasse 5 Gigabyte beträgt. Der angegebene Wert muss kleiner-gleich der maximal unterstützten Größe einer Datei im Zieldateisystem sein.

  Keinen Wert für MAXCAPACITY größer als 640 MB definieren, wenn diese Datei für die REMOVABLEFILE CD-Unterstützung bestimmt ist. Ein Wert, der kleiner als der verwendbare Speicherbereich (650 MB) einer CD ist, ermöglicht eine Eins-zu-Eins-Übereinstimmung zwischen Dateien aus der Einheitenklasse FILE und Kopien, die sich auf CD befinden.

### DIRectory



Gibt die Verzeichnisposition(en) der in dieser Einheitenklasse verwendeten Dateien an. Schließen Sie die gesamte Liste der Verzeichnisse in Anführungszeichen ein und verwenden Sie Kommas, um einzelne Verzeichnisnamen voneinander zu trennen. Sonderzeichen (z. B. Leerzeichen) sind in Verzeichnisnamen zulässig. Die Verzeichnisliste "abc def,xyz" enthält beispielsweise zwei Verzeichnisse: abc def und xyz. Dieser Parameter ist wahlfrei.


Durch die Angabe eines oder mehrerer Verzeichnisnamen werden die Positionen angegeben, an denen der Server die Dateien speichert, die Speicherdatenträger für diese Einheitenklasse darstellen.

  Bei der Verarbeitung des Befehls erweitert der Server den oder die angegebenen Verzeichnisnamen in die vollständig qualifizierte Form (beginnend beim Stammverzeichnis).

Wichtig: Wenn Sie Speicheragenten für den gemeinsamen Zugriff auf FILE-Datenträger verwenden, müssen Sie mit dem Befehl DEFINE PATH einen Pfad für jeden Speicheragenten definieren. Die Pfaddefinition enthält die Verzeichnisnamen, die vom Speicheragenten für den Zugriff auf jedes Verzeichnis verwendet werden.

Wenn der Server später einen Arbeitsdatenträger zuordnen muss, erstellt er eine neue Datei in einem dieser Verzeichnisse. (Der Server kann ein beliebiges der Verzeichnisse auswählen, in dem neue Arbeitsdatenträger erstellt werden sollen.) Bei Arbeitsdatenträgern, die zum Speichern von Clientdaten verwendet werden, hat die durch den Server erstellte Datei die Dateinamenerweiterung .bfs. Bei Arbeitsdatenträgern, auf denen Exportdaten gespeichert werden, wird die Dateinamenerweiterung .exp verwendet.

  Wenn Sie beispielsweise eine Einheitenklasse mit dem Verzeichnis tsmstor definieren und der Server einen Arbeitsdatenträger in dieser Einheitenklasse benötigt, um Exportdaten zu speichern, könnte der Name der Datei, die der Server erstellt, tsmstor\00566497.exp lauten.

 Wenn Sie beispielsweise eine Einheitenklasse mit dem Verzeichnis c:\server definieren und der Server einen Arbeitsdatenträger in dieser Einheitenklasse benötigt, um Exportdaten zu speichern, könnte der Name der Datei, die der Server erstellt, c:\server\00566497.exp lauten.

Tipp: Geben Sie mehrere Verzeichnisse für eine Einheitenklasse an, stellen Sie sicher, dass die Verzeichnisse separaten Dateisystemen zugeordnet sind. Bei Speicherbereichsauslöserfunktionen und Berechnungen des Speicherbereichs im

Speicherpool wird der Speicherbereich berücksichtigt, der in jedem Verzeichnis verbleibt. Wenn Sie mehrere Verzeichnisse für eine Einheitenklasse angeben und sich die Verzeichnisse in demselben Dateisystem befinden, berechnet der Server den Speicherbereich durch Hinzufügen von Werten, die den Speicherbereich darstellen, der in jedem Verzeichnis verbleibt. Diese Speicherbereichsberechnungen sind ungenau. Anstatt einen Speicherpool mit ausreichend Speicherbereich für eine Operation auszuwählen, kann der Server den falschen Speicherpool auswählen und frühzeitig über keinen Speicherbereich mehr verfügen. Bei Speicherbereichsauslösern kann eine ungenaue Berechnung zu einem Fehler bei der Erweiterung des Speicherbereichs führen, der in einem Speicherpool verfügbar ist. Ein Fehler bei der Erweiterung des Speicherbereichs in einem Speicherpool ist eine der Bedingungen, die zur Inaktivierung eines Auslösers führen kann. Wird ein Auslöser inaktiviert, da der Speicherbereich in einem Speicherpool nicht erweitert wurde, können Sie den Auslöser erneut aktivieren, indem Sie den folgenden Befehl ausgeben: `update spacetrigger stg`. Es sind keine weiteren Änderungen an dem Speicherbereichsauslöser erforderlich.

Einschränkung: Soll eine Verzeichnisliste geändert werden, müssen Sie die vollständige Liste ersetzen.

#### SHAREd

Gibt an, dass diese Einheitenklasse FILE von dem Server und von einem oder mehreren Speicheragenten gemeinsam genutzt wird. Zur Vorbereitung der gemeinsamen Nutzung wird automatisch ein Kassettenarchiv zusammen mit einer Anzahl von Laufwerken definiert, die dem Wert für MOUNTLIMIT entspricht, der der Einheitenklasse zugeordnet ist. Sind das Kassettenarchiv und die Laufwerke vorhanden und wird der Wert für MOUNTLIMIT geändert, können entweder Laufwerke erstellt werden, um einen neuen höheren Wert für MOUNTLIMIT zu erreichen, oder Laufwerke gelöscht werden, um einen neuen niedrigeren Wert zu erreichen.

## Speicheragenten, die FILE-Datenträger verwenden

Sie müssen sicherstellen, dass Speicheragenten auf neu erstellte FILE-Datenträger zugreifen können. Für den Zugriff auf FILE-Datenträger ersetzen Speicheragenten Namen aus der Verzeichnisliste in der Einheitenklassendefinition durch die Namen in der Verzeichnisliste für die zugeordnete Pfaddefinition. Der folgende Abschnitt verdeutlicht die Bedeutung übereinstimmender Einheitenklassen und Pfade, um sicherzustellen, dass Speicheragenten auf neu erstellte FILE-Datenträger zugreifen können.

Beispiel: Sie möchten folgende drei Verzeichnisse für ein FILE-Kassettenarchiv verwenden:

#### Windows-Betriebssysteme

- c:\server
- d:\server
- e:\server

#### AIX-Betriebssysteme

- /usr/tivoli1
- /usr/tivoli2
- /usr/tivoli3

#### Linux-Betriebssysteme

- /opt/tivoli1
- /opt/tivoli2
- /opt/tivoli3

1. Sie verwenden den folgenden Befehl, um ein FILE-Kassettenarchiv mit dem Namen CLASSA mit einem Laufwerk mit dem Namen CLASSA1 auf SERVER1 zu definieren:

#### Windows-Betriebssysteme

```
define devclass classa devtype=file
directory="c:\server,d:\server,e:\server"
shared=yes mountlimit=1
```


#### AIX-Betriebssysteme

```
define devclass classa devtype=file
directory="/usr/tivoli1,/usr/tivoli2,/usr/tivoli3"
shared=yes mountlimit=1
```

#### Linux-Betriebssysteme


```
define devclass classa devtype=file
directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
shared=yes mountlimit=1
```

2. Sie wollen, dass der Speicheragent STA1 das FILE-Kassettenarchiv verwenden kann. Daher definieren Sie folgenden Pfad für Speicheragent STA1:

-  Windows-Betriebssysteme


```
define path server1 stal srctype=server desttype=drive device=file
directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
\\192.168.1.10\e\server" library=classa
```

In diesem Szenario ersetzt der Speicheragent STA1 den Verzeichnisnamen c:\server durch den Verzeichnisnamen \\192.168.1.10\c\server, um auf FILE-Datenträger zuzugreifen, die sich in dem Verzeichnis c:\server auf dem Server befinden.

-  AIX-Betriebssysteme

```
define path server1 stal srctype=server desttype=drive device=file
directory="/usr/ibm1,/usr/ibm2,/usr/ibm3" library=classa
```


In diesem Szenario ersetzt der Speicheragent STA1 den Verzeichnisnamen /usr/tivoli1 durch den Verzeichnisnamen /usr/ibm1, um auf FILE-Datenträger zuzugreifen, die sich in dem Verzeichnis /usr/tivoli1 auf dem Server befinden.

-  Linux-Betriebssysteme

```
define path server1 stal srctype=server desttype=drive device=file
directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
```


In diesem Szenario ersetzt der Speicheragent STA1 den Verzeichnisnamen /opt/tivoli1 durch den Verzeichnisnamen /opt/ibm1/, um auf FILE-Datenträger zuzugreifen, die sich in dem Verzeichnis /opt/tivoli1 auf dem Server befinden.

Die Ergebnisse sind wie folgt:

-  Windows-Betriebssysteme FILE-Datenträger c:\server\file1.dsm wird durch SERVER1 erstellt. Wenn Sie das erste Verzeichnis für die Einheitenklassen später mit folgendem Befehl ändern:

```
update devclass classa directory="c:\otherdir,d:\server,e:\server"
```

kann SERVER1 weiterhin auf FILE-Datenträger c:\server\file1.dsm zugreifen, der Speicheragent STA1 jedoch nicht, weil in der PATH-Verzeichnisliste kein übereinstimmender Verzeichnisname mehr vorhanden ist. Ist kein Verzeichnisname in der Verzeichnisliste verfügbar, die der Einheitenklasse zugeordnet ist, kann der Speicheragent den Zugriff auf einen FILE-Datenträger in diesem Verzeichnis verlieren. Obwohl der Server zum Lesen noch auf den Datenträger zugreifen kann, kann der fehlgeschlagene Zugriff des Speicheragenten auf den FILE-Datenträger dazu führen, dass Operationen nur auf einem LAN-Pfad wiederholt werden können oder dass sie fehlschlagen.

-  AIX-Betriebssysteme Wird der FILE-Datenträger /usr/tivoli1/file1.dsm auf SERVER1 erstellt und wird der Befehl

```
update devclass classa directory="/usr/otherdir,/usr/tivoli2,
/usr/tivoli3"
```

ausgegeben, kann SERVER1 weiterhin auf FILE-Datenträger /usr/tivoli1/file1.dsm zugreifen, der Speicheragent STA1 jedoch nicht, weil in der PATH-Verzeichnisliste kein übereinstimmender Verzeichnisname mehr vorhanden ist. Ist kein Verzeichnisname in der Verzeichnisliste verfügbar, die der Einheitenklasse zugeordnet ist, kann der Speicheragent den Zugriff auf einen FILE-Datenträger in diesem Verzeichnis verlieren. Obwohl der Server zum Lesen noch auf den Datenträger zugreifen kann, kann der fehlgeschlagene Zugriff des Speicheragenten auf den FILE-Datenträger dazu führen, dass Operationen nur auf einem LAN-Pfad wiederholt werden können oder dass sie fehlschlagen.

-  Linux-Betriebssysteme Wird der FILE-Datenträger /opt/tivoli1/file1.dsm auf SERVER1 erstellt und wird der Befehl

```
update devclass classa directory="/opt/otherdir,/opt/tivoli2,
/opt/tivoli3"
```

ausgegeben, kann SERVER1 weiterhin auf FILE-Datenträger /opt/tivoli1/file1.dsm zugreifen, der Speicheragent STA1 jedoch nicht, weil in der PATH-Verzeichnisliste kein übereinstimmender Verzeichnisname mehr vorhanden ist. Ist kein Verzeichnisname in der Verzeichnisliste verfügbar, die der Einheitenklasse zugeordnet ist, kann der Speicheragent den Zugriff auf einen FILE-Datenträger in diesem Verzeichnis verlieren. Obwohl der Server zum Lesen noch auf den Datenträger zugreifen kann, kann der fehlgeschlagene Zugriff des Speicheragenten auf den FILE-Datenträger dazu führen, dass Operationen nur auf einem LAN-Pfad wiederholt werden können oder dass sie fehlschlagen.

## Beispiel: Eine Einheitenklasse FILE für die gemeinsame Nutzung aktualisieren

---

Eine FILE-Einheitenklasse (mit dem Namen PLAINFILES) für die gemeinsame Benutzung mit einem IBM Spectrum Protect-Speicheragenten vorbereiten.

```
update devclass plainfiles shared=yes
```

## Beispiel: Die Kapazität einer Einheitenklasse FILE aktualisieren

---



Für die Einheitenklasse FILE mit dem Namen STORFILES soll eine maximale Kapazität von 25 MB definiert werden.

```
update devclass storfiles maxcap=25m
```



## Beispiel: Einer Einheitenklasse FILE ein Verzeichnis hinzufügen

Die FILE-Einheitenklasse CLASSA aktualisieren, indem ein Verzeichnis, /usr/otherdir, zur Verzeichnisliste hinzugefügt wird. Die Verzeichnisse /opt/tivoli2 und /opt/tivoli3 wurden angegeben, als die Einheitenklasse zuerst definiert wurde.

```
update devclass classa
directory="/opt/tivoli2,/opt/tivoli3,/usr/otherdir"
```



## Beispiel: Einer Einheitenklasse FILE ein Verzeichnis hinzufügen

Die FILE-Einheitenklasse CLASSA aktualisieren, indem ein Verzeichnis, /usr/otherdir, zur Verzeichnisliste hinzugefügt wird. Die Verzeichnisse /usr/tivoli2 und /usr/tivoli3 wurden angegeben, als die Einheitenklasse zuerst definiert wurde.

```
update devclass classa
directory="/usr/tivoli2,/usr/tivoli3,/usr/otherdir"
```



## Beispiel: Einer Einheitenklasse FILE ein Verzeichnis hinzufügen

Die FILE-Einheitenklasse CLASSA aktualisieren, indem ein Verzeichnis, c:\otherdir, zur Verzeichnisliste hinzugefügt wird. Die Verzeichnisse d:\server und e:\server wurden angegeben, als die Einheitenklasse zuerst definiert wurde.

```
update devclass classa
directory="d:\server,e:\server,c:\otherdir"
```



## UPDATE DEVCLASS (Einheitenklasse GENERICTAPE aktualisieren)

Verwenden Sie die Einheitenklasse GENERICTAPE für Bandlaufwerke, die von Einheitentreibern des Betriebssystems unterstützt werden.

Bei Verwendung dieses Einheitentyps erkennt der Server weder den Einheitentyp noch das Kassettenaufzeichnungsformat. Wenn ein E/A-Fehler auftritt, sind die Fehlerinformationen weniger ausführlich im Vergleich zu den Fehlerinformationen für einen bestimmten Einheitentyp (z. B. 8MM), da der Server den Einheitentyp nicht erkennt. Bei der Definition von Einheiten für den Server dürfen keine verschiedenen Einheitentypen in demselben Einheitentyp gemischt werden.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-UPDate DEVclass--Einheitenklassenname----->
>--+-----+----->
  '-LIBRARY---Kassettenarchivname-'
>--+-----+----->
  '-ESTCAPacity---Größe-'  '-MOUNTRetention---Minuten-'
>--+-----+-----<
  '-MOUNTWait---Minuten-'  '-MOUNTLimit---+DRIVES-+-'
                              +-Anzahl-+
                              '-0-----'
```

## Parameter

#### Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

#### LIBRARY

Gibt den Namen des definierten Kassettenarchivobjekts an, das die Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können.

Dieser Parameter ist wahlfrei.

Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Geben Sie eine dem verwendeten Bandlaufwerk entsprechende Kapazität an.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

## UPDATE DEVCLASS (Einheitenklasse LTO aktualisieren)

Verwenden Sie die Einheitenklasse LTO, wenn Sie LTO-Bandeinheiten verwenden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-UPDate DEVclass--Einheitenklassenname----->
>--+-----+----->
  '-LIBRARY---Kassettenarchivname-'
>--+-----+----->
  '-LBProtect---+READWrite+-'
                    +-WRITEOnly+
                    '-No-----'
>--+-----+-----+----->
  '-FORMAT---+DRIVE---+' '-ESTCAPacity---Größe-'
                    +-ULTRIUM---+
                    +-ULTRIUMC---+
                    +-ULTRIUM2---+
                    +-ULTRIUM2C--+
                    +-ULTRIUM3---+
                    +-ULTRIUM3C--+
                    +-ULTRIUM4---+
                    +-ULTRIUM4C--+
                    +-ULTRIUM5---+
                    +-ULTRIUM5C--+
                    +-ULTRIUM6---+
                    '-ULTRIUM6C-'
>--+-----+----->
  '-PREFIX---+ADSM-----+'
                    '-Banddatenträgerpräfix-'
>--+-----+-----+----->
  '-MOUNTRetention---Minuten-' '-MOUNTWait---Minuten-'
>--+-----+----->
  '-MOUNTLimit---+DRIVES+-'
                    +-Anzahl+
                    '-0-----'
>--+-----+-----><
  | (1) (2) |
  '-----DRIVEEncryption---+ON-----+'
                                +-ALLOW---+
                                +-EXTERNAL+
                                '-OFF-----'
```

Anmerkungen:

1. Sie können nicht DRIVEENCRYPTION=ON angeben, wenn Ihre Laufwerke WORM-Datenträger verwenden (WORM - Write Once Read Many).
2. Laufwerkverschlüsselung wird nur für Ultrium 4-, Ultrium 5- und Ultrium 6-Laufwerke und -Datenträger unterstützt.

### Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRARY

Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten LTO-Bandlaufwerke enthält. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

#### LBProtect

Gibt an, ob der Schutz logischer Blöcke verwendet wird, um die Integrität von Daten sicherzustellen, die auf Band gespeichert sind. Wenn LBPROTECT auf READWRITE oder WRITEONLY gesetzt ist, verwendet der Server dieses Feature des Bandlaufwerks für den Schutz logischer Blöcke und generiert CRC-Zugriffsschutzinformationen für jeden Datenblock, der auf Band geschrieben wird. Der Server überprüft auch die CRC-Zugriffsschutzinformationen, wenn Daten von dem Band gelesen werden.

Die folgenden Werte sind gültig:

#### READWrite

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect und dem Bandlaufwerk erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen. Der Wert READWRITE hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

Wird der Parameter LBPROTECT auf READWRITE gesetzt, müssen Sie nicht den Parameter CRCDATA in einer Speicherpooldefinition angeben, da der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust bereitstellt.

#### WRITEOnly

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk nur für Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Für Leseoperationen überprüfen der Server und das Bandlaufwerk nicht die CRC-Informationen. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect zum Generieren der CRC-Informationen und für das Bandlaufwerk zum Berechnen und Vergleichen der CRC-Werte für Schreiboperationen erforderlich ist. Der Wert WRITEONLY hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

#### No

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen nicht aktiviert ist. Der Server aktiviert jedoch den Schutz logischer Blöcke bei Schreiboperationen für einen sich füllenden Datenträger, der bereits über Daten mit dem Schutz logischer Blöcke verfügt.

Einschränkung: Der Schutz logischer Blöcke wird nur auf IBM® LTO5-Laufwerken und unterstützten LTO6-Laufwerken unterstützt.

#### FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Geben Sie stattdessen das Format an, das die Laufwerke verwenden.

Gehen Sie wie folgt vor, wenn alle Laufwerke von Ultrium-Einheiten auf Ultrium 2-Einheiten migriert werden:

- Löschen Sie alle vorhandenen Ultrium-Laufwerkdefinitionen und die Pfade, die ihnen zugeordnet sind.
- Definieren Sie die neuen Ultrium 2-Laufwerke und Pfade.

Sollen verschiedene Generationen von LTO-Datenträgern und -laufwerken gemischt werden, sind die folgenden Einschränkungen zu beachten.

Tabelle 1. Lese-/Schreibfunktionalität verschiedener Generationen von LTO-Laufwerken

| Laufwerke                 | Datenträger der Generation 1 | Datenträger der Generation 2 | Datenträger der Generation 3 | Datenträger der Generation 4 | Datenträger der Generation 5 | Datenträger der Generation 6 |
|---------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|
| Generation 1              | Lesen und schreiben          | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             |
| Generation 2              | Lesen und schreiben          | Lesen und schreiben          | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             |
| Generation 3 <sup>1</sup> | Nur lesen                    | Lesen und schreiben          | Lesen und schreiben          | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             |
| Generation 4 <sup>2</sup> | nicht zutreffend             | Nur lesen                    | Lesen und schreiben          | Lesen und schreiben          | nicht zutreffend             | nicht zutreffend             |
| Generation 5 <sup>3</sup> | nicht zutreffend             | nicht zutreffend             | Nur lesen                    | Lesen und schreiben          | Lesen und schreiben          | nicht zutreffend             |
| Generation 6 <sup>4</sup> | nicht zutreffend             | nicht zutreffend             | nicht zutreffend             | Nur lesen                    | Lesen und schreiben          | Lesen und schreiben          |

| Laufwerke   | Datenträger der Generation 1 | Datenträger der Generation 2 | Datenträger der Generation 3 | Datenträger der Generation 4 | Datenträger der Generation 5 | Datenträger der Generation 6 |
|---|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|
| <p><sup>1</sup> In einem Kassettenarchiv mit einem Laufwerk der Generation 3 müssen alle Arbeitsdatenträger der Generation 1 entnommen werden und alle Speicherpooldatenträger der Generation 1 müssen in "schreibgeschützt" aktualisiert werden.</p> <p><sup>2</sup> In einem Kassettenarchiv mit einem Laufwerk der Generation 4 müssen alle Arbeitsdatenträger der Generation 2 entnommen werden und alle Speicherpooldatenträger der Generation 2 müssen in "schreibgeschützt" aktualisiert werden.</p> <p><sup>3</sup> In einem Kassettenarchiv mit einem Laufwerk der Generation 5 müssen alle Arbeitsdatenträger der Generation 3 entnommen werden und alle Speicherpooldatenträger der Generation 3 müssen in "schreibgeschützt" aktualisiert werden.</p> <p><sup>4</sup> In einem Kassettenarchiv mit einem Laufwerk der Generation 6 müssen alle Arbeitsdatenträger der Generation 4 entnommen werden und alle Speicherpooldatenträger der Generation 4 müssen in "schreibgeschützt" aktualisiert werden.</p> |                              |                              |                              |                              |                              |                              |

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für LTO-Einheiten aufgelistet:

Tabelle 2. Aufzeichnungsformat und geschätzte Standardkapazität für LTO

| Format   | Geschätzte Kapazität       | Beschreibung   |
|--|----------------------------|--|
| DRIVE  | -                          | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| ULTRIUM  | 100 GB                     | Dekomprimiertes Format, verwendet Ultrium-Kassetten  |
| ULTRIUMC   | Siehe Anmerkung<br>200 GB  | Komprimiertes Format, verwendet Ultrium-Kassetten  |
| ULTRIUM2   | 200 GB                     | Dekomprimiertes (Standard) Format, verwendet Ultrium 2-Kassetten   |
| ULTRIUM2C  | Siehe Anmerkung<br>400 GB  | Komprimiertes Format, verwendet Ultrium 2-Kassetten  |
| ULTRIUM3   | 400 GB                     | Dekomprimiertes (Standard) Format, verwendet Ultrium 3-Kassetten   |
| ULTRIUM3C  | Siehe Anmerkung<br>800 GB  | Komprimiertes Format, verwendet Ultrium 3-Kassetten  |
| ULTRIUM4   | 800 GB                     | Dekomprimiertes (Standard) Format, verwendet Ultrium 4-Kassetten   |
| ULTRIUM4C  | Siehe Anmerkung<br>1,6 TB  | Komprimiertes Format, verwendet Ultrium 4-Kassetten  |
| ULTRIUM5   | 1,5 TB                     | Dekomprimiertes (Standard-)Format, verwendet Ultrium 5-Kassetten   |
| ULTRIUM5C  | Siehe Anmerkung<br>3,0 TB  | Komprimiertes Format, verwendet Ultrium 5-Kassetten  |
| ULTRIUM6   | 2,5 TB                     | Dekomprimiertes (Standard) Format, verwendet Ultrium 6-Kassetten   |
| ULTRIUM6C  | Siehe Anmerkung<br>6,25 TB | Komprimiertes Format, verwendet Ultrium 6-Kassetten  |
| Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann die tatsächliche Kapazität abhängig von der Effektivität der Komprimierung größer als der aufgelistete Wert sein. |                            |  |

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger mit sequenziellem Zugriff an, die durch diese Einheitenklasse kategorisiert werden. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

Für weitere Informationen zu geschätzten Kapazitäten siehe Tabelle 2.

#### PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das

diese Einheitenklasse versorgt.

0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

#### DRIVEEncryption

Gibt an, ob die Laufwerkverschlüsselung zulässig ist. Dieser Parameter ist wahlfrei. Laufwerkverschlüsselung wird nur für Ultrium 4-, Ultrium 5- und Ultrium 6-Laufwerke und -Datenträger unterstützt.

Einschränkung: Ist die Verschlüsselung für eine Einheitenklasse aktiviert und ist die Einheitenklasse einem Speicherpool zugeordnet, sollte der Speicherpool nicht einen Arbeitsdatenträgerpool mit anderen Einheitenklassen gemeinsam nutzen, die nicht verschlüsselt werden können. Ist ein Band verschlüsselt und soll das Band in einem Laufwerk verwendet werden, das nicht verschlüsselt werden kann, müssen Sie das Band manuell mit einem neuen Kennsatz versehen, bevor es in diesem Laufwerk verwendet werden kann.

ON

Gibt an, dass IBM Spectrum Protect der Schlüsselmanager für die Laufwerkverschlüsselung ist und die Laufwerkverschlüsselung für leere Speicherpooldatenträger nur erlaubt, wenn das Anwendungsverfahren aktiviert ist. (Andere Typen von Datenträgern werden nicht verschlüsselt. Beispielsweise werden Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger nicht verschlüsselt.) Wird ON angegeben und ein anderes Verschlüsselungsverfahren aktiviert, ist die Laufwerkverschlüsselung nicht zulässig, und Sicherungsoperationen schlagen fehl.

Anmerkung: Sie können nicht IBM Spectrum Protect als Schlüsselmanager für die Laufwerkverschlüsselung von WORM-Datenträgern angeben (WORM - Write Once Read Many). (Wenn Sie WORM-Datenträger verwenden, können Sie nicht DRIVEENCRYPTION=ON angeben.)

ALLOW

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Die Laufwerkverschlüsselung für leere Datenträger ist jedoch zulässig, wenn ein anderes Verschlüsselungsverfahren aktiviert ist.

EXTERNAL

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Verwenden Sie diese Einstellung mit einer Verschlüsselungsmethodik, die von einem anderen Anbieter zur Verfügung gestellt wird und die mit dem Anwendungsverfahren der Verschlüsselung verwendet wird, das für das Laufwerk aktiviert ist. Geben Sie EXTERNAL an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect nicht inaktiviert. Geben Sie dagegen ALLOW an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect inaktiviert.

OFF

Gibt an, dass die Laufwerkverschlüsselung nicht zulässig ist. Wird ein anderes Verschlüsselungsverfahren aktiviert, schlagen Sicherungen fehl. Wird das Anwendungsverfahren aktiviert, inaktiviert IBM Spectrum Protect die Verschlüsselung, und die Ausführung von Sicherungen wird versucht.

## Beispiel: Den Grenzwert für Ladeanforderungen für eine Einheitenklasse LTO aktualisieren

---



Die Einheitenklasse LTOTAPE aktualisieren. Den Grenzwert für Ladeanforderungen in 2 ändern.

```
update devclass ltotape mountlimit=2
```

## UPDATE DEVCLASS (Einheitenklasse NAS aktualisieren)

---

Verwenden Sie die Einheitenklasse NAS (Network Attached Storage), wenn Sie NDMP-Operationen zum Sichern von NAS-Dateiservern verwenden (NDMP - Network Data Management Protocol). Die Einheitenklasse ist für Laufwerke bestimmt, die der NAS-Dateiserver für Sicherungen unterstützt.

  Die Einheitenklasse NAS unterstützt keine Kassettenarchive EXTERNAL.

 Die Einheitenklasse NAS unterstützt keine Kassettenarchive EXTERNAL.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
>>-UPDate DEVclass--Einheitenklassenname----->>
```

```

>+-----+-----+----->
  '-LIBRARY-----Kassettenarchivname-'
>+-----+-----+----->
  '-MOUNTRetention-----0-'  '-MOUNTWait-----Minuten-'
>+-----+-----+-----+----->
  '-MOUNTLimit-----+-----DRIVES+-'  '-ESTCAPacity-----Größe-'
                   +-Anzahl+
                   '-0-----'
>+-----+-----+-----<
  '-PREFIX-----Banddatenträgerpräfix-'

```

## Parameter

---

### Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

### LIBRARY

Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten SCSI-Bandlaufwerke enthält. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

### MOUNTRetention=0

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Null (0) ist der einzige unterstützte Wert für Einheitenklassen mit DEVType=NAS.

### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

### Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: K (Kilobyte), M (Megabyte), G (Gigabyte) oder T (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

### PREFIX



Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

```
AB.CD2.E
```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

## Beispiel: Die geschätzte Kapazität für eine Einheitenklasse NAS aktualisieren

Die Einheitenklasse NASTAPE aktualisieren. Die geschätzte Kapazität in 200 GB ändern.

```
update devclass nastape library=naslib estcapacity=200G
```

## UPDATE DEVCLASS (Einheitenklasse REMOVABLEFILE aktualisieren)

Verwenden Sie die Einheitenklasse REMOVABLEFILE für Einheiten für austauschbare Datenträger, die als lokale, entfernbare Dateisysteme angeschlossen sind.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-UPDate DEVclass--Einheitenklassenname----->
>--+-----+----->
  '-LIBRARY----Kassettenarchivname- '
>--+-----+--+-----+----->
  '-MAXCAPacity----Größe- '  '-MOUNTRetention----Minuten- '
>--+-----+--+-----+-----<
  '-MOUNTWait----Minuten- '  '-MOUNTLimit----+DRIVES-+- '
                               +-Anzahl-+
                               '-0-----'
```

### Parameter

Einheitenklassenname (Erforderlich)



Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

LIBRARY

Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten Laufwerke für austauschbare Datenträger enthält. Dieser Parameter ist wahlfrei. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

MAXCAPacity

Gibt die maximale Größe der Datenträger an, die für einen Speicherpool definiert sind, der durch diese Einheitenklasse kategorisiert wird. Dieser Parameter ist wahlfrei.

  Da der Server nur eine Datei pro physischen austauschbaren Datenträger öffnet, ist die Kapazität so zu wählen, dass diese eine Datei die Datenträgerkapazität vollständig nutzt.

Dieser Wert muss als ganze Zahl gefolgt von einem K (Kilobyte), M (Megabyte), G (Gigabyte) oder T (Terabyte) angegeben werden.

MAXCAPACITY=5M gibt beispielsweise an, dass die maximale Kapazität eines Datenträgers in dieser Einheitenklasse 5 MB beträgt. Der zulässige Mindestwert ist 1 MB (d. h. MAXCAPACITY=1M).

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

## UPDATE DEVCLASS (Einheitenklasse SERVER aktualisieren)

---

Verwenden Sie die Einheitenklasse SERVER, um Speicherdatenträger oder Dateien zu verwenden, die auf einem anderen IBM Spectrum Protect-Server archiviert sind.

### Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

---

```
>>-UPDdate DEVclass--Einheitenklassenname----->
>--+-----+--+-----+----->
  '-SERVERName-----Servername-' '-MAXCAPacity-----Größe-'
>--+-----+-----+----->
  '-PREFIX-----+ADSM-----+'
                   '-Banddatenträgerpräfix-'
```

```

>----->
'-RETRYPeriod-----Minuten--'

>----->
'-RETRYInterval-----Sekunden--'

>----->
'-MOUNTRetention-----Minuten-'

>-----<
'-MOUNTLimit-----Anzahl--+'
'-1-----'

```

## Parameter

---

Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

SERVERName

Gibt den Namen des Servers an. Der Parameter SERVERNAME muss einem definierten Server entsprechen.

Anmerkung: Wird der Servername (SERVERNAME) eines vorhandenen Servers durch einen neuen Namen ersetzt, kann auf die Daten der Datenträger unter dem alten Servernamen (SERVERNAME) mit dieser Einheitenklasse nicht mehr zugegriffen werden.

MAXCAPacity

Gibt die maximale Größe für Objekte bei der Erstellung auf dem Zielserver an. Dieser Parameter ist wahlfrei.

Dieser Wert muss als ganze Zahl gefolgt von einem **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte) angegeben werden. Der zulässige Mindestwert ist 1 MB (MAXCAPACITY=1M).

PREFIX

Gibt den Anfangsabschnitt des Archivierungsdateinamens der höheren Ebene auf dem Zielserver an. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:  
                   AB.CD2.E
- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Archivierungsdateinamens der höheren Ebene, der das Standardpräfix verwendet, ist ADSM.volume1.

RETRYPeriod

Gibt den Wiederholungszeitraum in Minuten an. Der Wiederholungszeitraum ist das Intervall, während dem der Server versucht, eine Verbindung zu einem Zielserver herzustellen, falls ein Übertragungsfehler vermutet wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

RETRYInterval

Gibt das Wiederholungsintervall in Sekunden an. Das Wiederholungsintervall gibt an, wie oft Wiederholungen in einer bestimmten Zeitperiode erfolgen. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 1 bis 9999 angeben.

MOUNTRetention

Gibt die Anzahl Minuten an, die eine inaktive Verbindung mit dem Zielserver aufrechterhalten werden soll, bevor die Verbindung geschlossen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTLimit

Gibt die maximal zulässige Anzahl gleichzeitig stattfindender Sitzungen zwischen dem Quellenserver und dem Zielserver an. Alle Versuche, auf mehr Sitzungen zuzugreifen als mit dem Grenzwert für Ladeanforderung angegeben sind, haben das Warten des Anforderers zur Folge. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 1 bis 4096 angeben.

Gültige Werte:

Zahl

Gibt die maximal zulässige Anzahl gleichzeitig stattfindender Sitzungen zwischen dem Quellenserver und dem Zielservers an.

1

Gibt die Anzahl der gleichzeitig stattfindenden Sitzungen zwischen dem Quellenserver und dem Zielservers an.

## UPDATE DEVCLASS (Einheitenklasse VOLSAFE aktualisieren)

Verwenden Sie den Einheitentyp VOLSAFE, um mit StorageTek VolSafe-Datenträgern und -Laufwerken zu arbeiten. Diese Technologie verwendet Datenträger, die nicht überschrieben werden können. Verwenden Sie diese Datenträger daher nicht für kurzfristige Sicherungen von Clientdateien, der Serverdatenbank oder von Exportbändern.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-UPDate DEVclass--Einheitenklassenname----->
>--+-----+----->
  '-LIBRARY----Kassettenarchivname- '
>--+-----+-----+----->
  '-FORMAT-----+DRIVE-----+ ' '-ESTCAPacity----Größe- '
      +-9840-----+
      +-9840-C-----+
      +-T9840C-----+
      +-T9840C-C--+
      +-T9840D-----+
      +-T9840D-C--+
      +-T10000A-----+
      +-T10000A-C+
      +-T10000B-----+
      +-T10000B-C+
      +-T10000C-----+
      +-T10000C-C+
      +-T10000D-----+
      '-T10000D-C- '
>--+-----+----->
  '-PREFIX-----+ADSM-----+-'
      '-Banddatenträgerpräfix- '
>--+-----+-----+----->
  '-MOUNTRetention----Minuten- ' '-MOUNTWait----Minuten- '
>--+-----+-----+-----><
  '-MOUNTLimit-----+DRIVES+-+ '
      +-Anzahl+
      '-0-----'
```

### Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRARY

Gibt den Namen des definierten Kassettenarchivobjekts an, das die VolSafe-Laufwerke enthält, die von dieser Einheitenklasse verwendet werden können. Sind Laufwerke in einem Kassettenarchiv VolSafe-aktiviert, müssen alle Laufwerke in dem Kassettenarchiv VolSafe-aktiviert sein. Für weitere Informationen zum Einheitentyp VolSafe siehe DEFINE DEVCLASS (Einheitenklasse VOLSAFE definieren).

FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

Achtung: Wird DRIVE für eine Einheitenklasse angegeben, die über inkompatible Einheiten mit sequenziellem Zugriff verfügt, müssen Datenträger in Einheiten geladen werden, die in dem Format lesen oder schreiben können, das beim ersten Laden des

Datenträgers eingerichtet wurde. Dies kann zu Verzögerungen führen, wenn die einzige Einheit mit sequenziellem Zugriff, die auf den Datenträger zugreifen kann, bereits im Gebrauch ist.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für VolSafe-Einheiten aufgelistet:

**Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für VOLSAFE-Bänder**

| Format    | Geschätzte Kapazität | Beschreibung   |
|-----------|----------------------|--|
| DRIVE     | –                    | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| 9840      | 20 GB                | Dekomprimiertes (Standard) Format, verwendet eine 20-GB-Kassette mit 270 Meter Band  |
| 9840-C    | 80 GB                | Komprimiertes LZ-1 Enhanced-Format (4:1), verwendet eine 80-GB-Kassette mit 270 Meter Band   |
| T9840C    | 40 GB                | Dekomprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840C-C  | 80 GB                | Komprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840D    | 75 GB                | Dekomprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840D-C  | 150 GB               | Komprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette   |
| T10000A   | 500 GB               | Dekomprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette  |
| T10000A-C | 1 TB                 | Komprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette  |
| T10000B   | 1 TB                 | Dekomprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette   |
| T10000B-C | 2 TB                 | Komprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette   |
| T10000C   | 5 TB                 | Dekomprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000C-C | 10 TB                | Komprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000D   | 8 TB                 | Dekomprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000D-C | 15 TB                | Komprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: **K** (Kilobyte), **M** (Megabyte), **G** (Gigabyte) oder **T** (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

Für weitere Informationen zur geschätzten Standardkapazität von Magnetbandkassetten siehe Tabelle 1.

#### PREFIX

Gibt den Anfangsabschnitt des Archivierungsdateinamens der höheren Ebene auf dem Zielsystem an. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

AB.CD2.E

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,\$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Archivierungsdateinamens der höheren Ebene, der das Standardpräfix verwendet, ist ADSM.volume1.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

#### MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

 AIX-Betriebssysteme  Linux-Betriebssysteme

## UPDATE DEVCLASS - z/OS Media-Server (Einheitenklasse für z/OS Media-Server aktualisieren)

Mit diesem Befehl können Sie eine Einheitenklasse aktualisieren. Eine begrenzte Gruppe von Einheitenklassentypen ist für Einheiten verfügbar, auf die über einen z/OS Media-Server zugegriffen wird.

- UPDATE DEVCLASS (Einheitenklasse 3590 für z/OS Media-Server aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse 3592 für z/OS Media-Server aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse ECARTRIDGE für z/OS Media-Server aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse FILE für z/OS Media-Server aktualisieren)

Tabelle 1. Zugehörige Befehle für UPDATE DEVCLASS

| Befehl                              | Beschreibung  |
|-------------------------------------|---|
| BACKUP DEVCONFIG                    | Sichert IBM Spectrum Protect-Einheitendaten in einer Datei.   |
| DEFINE DEVCLASS (z/OS Media-Server) | Definiert eine Einheitenklasse für die Verwendung von Speicher, der von einem z/OS Media-Server verwaltet wird. |
| DEFINE LIBRARY                      | Definiert ein automatisiertes oder manuelles Kassettenarchiv.   |
| DELETE DEVCLASS                     | Löscht eine Einheitenklasse.  |
| QUERY DEVCLASS                      | Zeigt Informationen zu Einheitenklassen an.   |
| UPDATE LIBRARY                      | Ändert die Attribute eines Kassettenarchivs.  |

## UPDATE DEVCLASS (Einheitenklasse 3590 für z/OS Media-Server aktualisieren)

Mit diesem Befehl können Sie eine Einheitenklasse aktualisieren, die Sie definiert haben, um mit einem z/OS Media-Server auf 3590-Einheiten zuzugreifen. Die Einheitenklasse, die sich auf Speicher für den z/OS Media-Server bezieht, erfordert eine Kassettenarchivdefinition des Typs ZOSMEDIA.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```

(1) (2)
>>-UPDate DEVclass--Einheitenklassenname----->
>--+-----+----->
  '-LIBRARY---Kassettenarchivname-'
>--+-----+----->
  '-FORMAT---+DRIVE---+' '-ESTCAPacity---Größe-'
      +-3590B---+
      +-3590C---+
      +-3590E-B-+
      +-3590E-C-+
      +-3590H-B-+
      '-3590H-C-'
>--+-----+----->
  '-COMPRESSION---+Yes-+-'
      '-No--'
>--+-----+----->
  '-MOUNTRetention---Minuten-' '-MOUNTWait---Minuten-'
>--+-----+----->
  '-MOUNTLimit---+DRIVES-+' '-EXPIration---jjjttt-'
      +-Anzahl-+
      '-0-----'
>--+-----+----->
  '-RETention---Tage-' '-PROtection---+No-----+-'
      +-Yes-----+
      '-Automatic-'

```

```
>-----<
'-UNIT---Einheitenname-'
```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.
2. Der Parameter PREFIX kann mit diesem Befehl nicht aktualisiert werden. Sie müssen eine Einheitenklasse mit dem Wert erstellen, der für den Parameter PREFIX erforderlich ist.

## Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

LIBRARY

Gibt den Namen eines Kassettenarchivs an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde. Das Kassettenarchiv und die Bandlaufwerke, die von dieser Einheitenklasse verwendet werden können, werden von dem z/OS Media-Server gesteuert.

Dieser Parameter ist wahlfrei.

Informationen zum Definieren eines Kassettenarchivs befinden sich unter dem Befehl DEFINE LIBRARY.

FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

In der folgenden Tabelle sind die Optionen der Aufzeichnungsformate für 3590-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate für 3590

| Format   | Beschreibung   |
|--|--|
| 3590B  | Dekomprimiertes (Basis-)Format                           |
| 3590C  | Komprimiertes Format                                     |
| 3590E-B  | Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format |
| 3590E-C  | Komprimiertes Format, ähnlich dem 3590C-Format           |
| 3590H-B  | Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format |
| 3590H-C  | Komprimiertes Format, ähnlich dem 3590C-Format           |
| Anmerkung: Wenn das Format die Datenkomprimierung über Hardware mittels Bandlaufwerk verwendet, kann die tatsächliche Kapazität je nach Effektivität der Komprimierung zunehmen. |  |

ESTCAPACITY

Gibt die geschätzte Kapazität für die Datenträger mit sequenziellem Zugriff an, die durch diese Einheitenklasse kategorisiert werden. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn die geschätzte Standardkapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist. Der Wert bestimmt nicht das auf dem Datenträger gespeicherte Datenvolumen. Der Server verwendet den Wert, um die Belegung zu schätzen, bevor ein Datenträger gefüllt ist. Wenn ein Datenträger voll ist, wird für die Berechnung der Belegung das tatsächlich auf dem Band gespeicherte Datenvolumen verwendet.

Geben Sie den Wert als ganze Zahl mit einem der folgenden Einheitenanzeiger an: K (KB), M (MB), G (GB) oder T (TB). Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt. Der zulässige Mindestwert ist 100 KB (ESTCAPACITY=100K).

COMPRESSION

Gibt an, ob die Dateikomprimierung für diese Einheitenklasse verwendet wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

Yes

Gibt an, dass die Daten der Banddatenträger komprimiert werden.

No

Gibt an, dass die Daten der Banddatenträger nicht komprimiert werden.

MOUNTRETENTION

Gibt die Anzahl Minuten an, die ein inaktiver Banddatenträger beibehalten wird, bevor er entladen wird. Die Zeitspanne für die Ladedauer beginnt nach Ablauf des Inaktivitätszeitlimits. Dieser Parameter ist wahlfrei. Geben Sie eine Zahl von 0 bis 9999 an.



Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

#### MOUNTWait

Gibt die maximale Anzahl Minuten an, die der z/OS Media-Server auf das Laden eines Datenträgers wartet. Wird auf die Ladeanforderung nicht innerhalb der angegebenen Zeit geantwortet, schlägt die Ladeanforderung fehl. Ist eine Einheit erfolgreich zugeordnet und wird die Anforderung zum Öffnen der Einheit nicht innerhalb der angegebenen Zeit ausgeführt, wird die Anforderung zum Öffnen der Einheit beendet und die Ladeanforderung schlägt fehl.

Dieser Parameter ist wahlfrei. Geben Sie eine Zahl von 1 bis 9999 an.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Sie können einen der folgenden Werte angeben:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt. Sie können eine Zahl von 0 bis 4096 angeben.

#### 0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können.

#### EXPIration

Gibt das Verfallsdatum an, das in den Bandkennsätzen für diese Einheitenklasse angegeben wird. Dieser Parameter ist wahlfrei.

Geben Sie das Datum an, an dem der Server das Band nicht mehr benötigt. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Geben Sie das Verfallsdatum im Format *jjjjtt* an (vier Stellen für das Jahr und drei Stellen für den Tag). Beispielsweise wird der 7. Januar 2014 als 2014007 angegeben (der siebte Tag des Jahres 2014).

Wenn Sie den Parameter EXPIRATION angeben, können Sie nicht den Parameter RETENTION angeben.

#### RETention

Gibt die Anzahl Tage an, die das Band aufbewahrt werden soll. Dieser Parameter ist wahlfrei.

Geben Sie die Anzahl der Tage (1 - 9999) an, die der Server das Band voraussichtlich verwenden wird. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Wenn Sie den Parameter RETENTION angeben, können Sie nicht den Parameter EXPIRATION angeben.

Tipp: Sie können für diesen Parameter den Wert null angeben. Dieser Wert sollte jedoch nur angegeben werden, wenn auch ein Wert für den Parameter EXPIRATION angegeben werden soll. Sie können keinen Wert für den Parameter EXPIRATION angeben, wenn Sie einen Wert ungleich null für den Parameter RETENTION angeben.

#### PROtection

Gibt an, ob das RACF-Programm (falls installiert) Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Wenn Schutz zur Verfügung gestellt wird, werden RACF-Profile bei der ersten Verwendung der Datenträger erstellt. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

#### No

Gibt an, dass das RACF-Programm keine Datenträger schützt, die dieser Einheitenklasse zugeordnet sind.

#### Yes

Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Für die Datenträger werden RACF-Profile erstellt, wenn der Server die Datenträger zum ersten Mal verwendet; die Profile werden jedoch nicht gelöscht, wenn Datenträger auf dem Server gelöscht werden. Die Profile müssen manuell gelöscht werden.

Tipp: Sind sensible Daten auf den Datenträgern gespeichert, die dieser Einheitenklasse zugeordnet sind, verwenden Sie PROTECTION=YES und löschen Sie RACF-Profile manuell nur nach dem Entfernen der Banddatenträger.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

#### Automatic

Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. RACF-Profile werden für Datenträger erstellt, wenn der Server zum ersten Mal die Datenträger verwendet. RACF-Profile werden gelöscht, wenn Datenträger auf dem Server gelöscht werden.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

Wichtig: Wird PROTECTION=AUTOMATIC angegeben, wird beim Löschen eines Datenträgers sein RACF-Profil gelöscht. Der Datenträger ist daher nicht mehr durch das RACF-Programm geschützt. Andere Benutzer können auf die Daten auf diesen Datenträgern zugreifen.

Wenn Sie PROTECTION=AUTOMATIC angeben, gibt der z/OS Media-Server RACROUTE-Befehle aus, um Profile zu löschen, wenn ein Datenträger auf dem Server gelöscht wird. Die ausgegebenen Löschbefehle sind von den aktuellen Systemwerten für TAPEVOL und TAPEDSN abhängig. Wenn die Systemeinstellungen geändert werden, löscht der z/OS Media-Server vorhandene Profile möglicherweise nicht.

Ändern Sie nicht die Einstellung in PROTECTION=AUTOMATIC für eine Einheitenklasse, für die PROTECTION=NO definiert wurde. Es können Datenträger ohne Profile vorhanden sein, und es werden Fehlernachrichten generiert, wenn diese Datenträger gelöscht werden. Wenn ein anderer Wert für PROTECTION erforderlich ist, definieren Sie eine neue Einheitenklasse.

Die Erstellung und das Löschen von Profilen erfolgen aufgrund der Schutzeinstellungen, wenn der Datenträger zum ersten Mal verwendet und wenn er gelöscht wird. Der Server erstellt keine Profile für Datenträger, die er bereits verwendet hat. Wenn für den Schutz AUTOMATIC angegeben ist, versucht der Server, Profile zu löschen, wenn Datenträger gelöscht werden.

Die Dokumentation zu dem RACF-Programm enthält ausführliche Informationen zu den Einstellungen für TAPEVOL und TAPEDSN und zu den Profilen, die erstellt werden, wenn diese Einstellungen aktiv sind.

#### UNIT

Gibt einen privaten Einheitennamen für eine Gruppe von Bandeinheiten an, die 3590-Band unterstützen. Dieser Parameter ist wahlfrei. Der Einheitenname kann bis zu 8 Zeichen umfassen.

## UPDATE DEVCLASS (Einheitenklasse 3592 für z/OS Media-Server aktualisieren)

---

Mit diesem Befehl können Sie eine Einheitenklasse aktualisieren, die Sie definiert haben, um mit einem z/OS Media-Server auf 3592-Einheiten zuzugreifen. Die Einheitenklasse, die sich auf Speicher für den z/OS Media-Server bezieht, erfordert eine Kassettenarchivdefinition des Typs ZOSMEDIA.

### Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

---

```

                                     (1) (2)
>>-UPDate DEVclass--Einheitenklassenname----->
>--+-----+-----+----->
  '-LIBRARY----ZOSMEDIA-Speicherarchiv-'
>--+-----+-----+----->
  '-FORMAT----+DRIVE---+ '-ESTCAPacity----Größe-'
      +-3592----+
      +-3592C---+
      +-3592-2--+
      +-3592-2C-+
      +-3592-3--+
      +-3592-3C-+
```

```

    +-3592-4--+
    '-3592-4C-'

>+-----+----->
  '-COMPression----+Yes-+'
                          '-No--'

>+-----+-----+----->
  '-MOUNTRetention---Minuten-' '-MOUNTWait----Minuten-'

>+-----+-----+----->
  '-MOUNTLimit-----+DRIVES-+' '-EXPIration----jjjjttt-'
                          +-Anzahl+
                          '-0-----'

>+-----+-----+----->
  '-RETention---Tage-' '-PROtection---+No-----+'
                                   +-Yes-----+
                                   '-Automatic-'

>+-----+-----<
  '-UNIT---Einheitenname-'

```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.
2. Der Parameter PREFIX kann mit diesem Befehl nicht aktualisiert werden. Sie müssen eine Einheitenklasse mit dem Wert erstellen, der für den Parameter PREFIX erforderlich ist.

## Parameter

**Einheitenklassenname (Erforderlich)**

Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

**LIBRARY**

Gibt den Namen eines Kassettenarchivs an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde. Das Kassettenarchiv und die Bandlaufwerke, die von dieser Einheitenklasse verwendet werden können, werden von dem z/OS Media-Server gesteuert.

Dieser Parameter ist wahlfrei.

Informationen zum Definieren eines Kassettenarchivs befinden sich unter dem Befehl DEFINE LIBRARY.

**FORMAT**

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

Die folgende Tabelle enthält die Aufzeichnungsformate.

Tabelle 1. Aufzeichnungsformate für 3592

| Format  | Beschreibung   |
|---------|--|
| 3592    | Dekomprimiertes (Basis-)Format   |
| 3592C   | Komprimiertes Format   |
| 3592-2  | Dekomprimiertes (Basis) Format, ähnlich dem 3592-Format  |
| 3592-C  | Komprimiertes Format, ähnlich dem 3592C-Format   |
| 3592-3  | Dekomprimiertes (Basis) Format, ähnlich dem 3592-Format  |
| 3592-3C | Komprimiertes Format, ähnlich dem 3592C-Format   |
| 3592-4  | Dekomprimiertes (Basis) Format, ähnlich dem 3592-Format  |
| 3592-4C | Komprimiertes Format, ähnlich dem 3592C-Format   |
| DRIVE   | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |

| Format   | Beschreibung |
|--|--------------|
| Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann je nach Effektivität der Komprimierung die tatsächliche Kapazität von dem aufgelisteten Wert abweichen. |              |

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet. Um optimale Ergebnisse zu erzielen, mischen Sie nicht Generationen von Laufwerken in demselben Kassettenarchiv. Enthält ein Kassettenarchiv gemischte Generationen, können Datenträgerfehler auftreten. Beispielsweise können Laufwerke der Generation 1 und Generation 2 keine Datenträger der Generation 3 lesen. Falls möglich, führen Sie für alle Laufwerke ein Upgrade auf 3592 Generation 3 durch. Kann nicht für alle Laufwerke ein Upgrade auf 3592 Generation 3 durchgeführt werden, müssen Sie eine spezielle Konfiguration verwenden.

#### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn die geschätzte Standardkapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist. Der Wert bestimmt nicht das auf dem Datenträger gespeicherte Datenvolumen. Der Server verwendet den Wert, um die Belegung zu schätzen, bevor ein Datenträger gefüllt ist. Wenn ein Datenträger voll ist, wird für die Berechnung der Belegung das tatsächlich auf dem Band gespeicherte Datenvolumen verwendet.

Geben Sie den Wert als ganze Zahl mit einem der folgenden Einheitenanzeiger an: **K** (KB), **M** (MB), **G** (GB) oder **T** (TB). Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt. Der zulässige Mindestwert ist 100 KB (ESTCAPACITY=100K).

#### COMPression

Gibt an, ob die Dateikomprimierung für diese Einheitenklasse verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Sie können einen der folgenden Werte angeben:

Yes

Gibt an, dass die Daten der Banddatenträger komprimiert werden.

No

Gibt an, dass die Daten der Banddatenträger nicht komprimiert werden.

#### MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Banddatenträger beibehalten wird, bevor er entladen wird. Die Zeitspanne für die Ladedauer beginnt nach Ablauf des Inaktivitätszeitlimits. Dieser Parameter ist wahlfrei. Geben Sie eine Zahl von 0 bis 9999 an.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

#### MOUNTWait

Gibt die maximale Anzahl Minuten an, die der z/OS Media-Server auf das Laden eines Datenträgers wartet. Wird auf die Ladeanforderung nicht innerhalb der angegebenen Zeit geantwortet, schlägt die Ladeanforderung fehl. Ist eine Einheit erfolgreich zugeordnet und wird die Anforderung zum Öffnen der Einheit nicht innerhalb der angegebenen Zeit ausgeführt, wird die Anforderung zum Öffnen der Einheit beendet und die Ladeanforderung schlägt fehl.

Dieser Parameter ist wahlfrei. Geben Sie eine Zahl von 1 bis 9999 an.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

#### MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Sie können einen der folgenden Werte angeben:

#### DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

#### Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das

diese Einheitenklasse versorgt. Sie können eine Zahl von 0 bis 4096 angeben.

0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können.

#### EXPIration

Gibt das Verfallsdatum an, das in den Bandkennsätzen für diese Einheitenklasse angegeben wird. Dieser Parameter ist wahlfrei.

Geben Sie das Datum an, an dem der Server das Band nicht mehr benötigt. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Geben Sie das Verfallsdatum im Format *jjjjtt* an (vier Stellen für das Jahr und drei Stellen für den Tag). Beispielsweise wird der 7. Januar 2014 als 2014007 angegeben (der siebte Tag des Jahres 2014).

Wenn Sie den Parameter EXPIRATION angeben, können Sie nicht den Parameter RETENTION angeben.

#### RETention

Gibt die Anzahl Tage an, die das Band aufbewahrt werden soll. Dieser Parameter ist wahlfrei.

Geben Sie die Anzahl der Tage (1 - 9999) an, die der Server das Band voraussichtlich verwenden wird. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Wenn Sie den Parameter RETENTION angeben, können Sie nicht den Parameter EXPIRATION angeben.

Tipp: Sie können für diesen Parameter den Wert null angeben. Dieser Wert sollte jedoch nur angegeben werden, wenn auch ein Wert für den Parameter EXPIRATION angegeben werden soll. Sie können keinen Wert für den Parameter EXPIRATION angeben, wenn Sie einen Wert ungleich null für den Parameter RETENTION angeben.

#### PROtection

Gibt an, ob das RACF-Programm (falls installiert) Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Wenn Schutz zur Verfügung gestellt wird, werden RACF-Profile bei der ersten Verwendung der Datenträger erstellt. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass das RACF-Programm keine Datenträger schützt, die dieser Einheitenklasse zugeordnet sind.

Yes

Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Für die Datenträger werden RACF-Profile erstellt, wenn der Server die Datenträger zum ersten Mal verwendet; die Profile werden jedoch nicht gelöscht, wenn Datenträger auf dem Server gelöscht werden. Die Profile müssen manuell gelöscht werden.

Tipp: Sind sensible Daten auf den Datenträgern gespeichert, die dieser Einheitenklasse zugeordnet sind, verwenden Sie PROTECTION=YES und löschen Sie RACF-Profile manuell nur nach dem Entfernen der Banddatenträger.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

#### Automatic

Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. RACF-Profile werden für Datenträger erstellt, wenn der Server zum ersten Mal die Datenträger verwendet. RACF-Profile werden gelöscht, wenn Datenträger auf dem Server gelöscht werden.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

Wichtig: Wird PROTECTION=AUTOMATIC angegeben, wird beim Löschen eines Datenträgers sein RACF-Profil gelöscht. Der Datenträger ist daher nicht mehr durch das RACF-Programm geschützt. Andere Benutzer können auf die Daten auf diesen Datenträgern zugreifen.

Wenn Sie PROTECTION=AUTOMATIC angeben, gibt der z/OS Media-Server RACROUTE-Befehle aus, um Profile zu löschen, wenn ein Datenträger auf dem Server gelöscht wird. Die ausgegebenen Löschbefehle sind von den aktuellen Systemwerten für TAPEVOL und TAPEDSN abhängig. Wenn die Systemeinstellungen geändert werden, löscht der z/OS Media-Server vorhandene Profile möglicherweise nicht.

Ändern Sie nicht die Einstellung in PROTECTION=AUTOMATIC für eine Einheitenklasse, für die PROTECTION=NO definiert wurde. Es können Datenträger ohne Profile vorhanden sein, und es werden Fehlernachrichten generiert, wenn diese Datenträger gelöscht werden. Wenn ein anderer Wert für PROTECTION erforderlich ist, definieren Sie eine neue Einheitenklasse.

Die Erstellung und das Löschen von Profilen erfolgen aufgrund der Schutzeinstellungen, wenn der Datenträger zum ersten Mal verwendet und wenn er gelöscht wird. Der Server erstellt keine Profile für Datenträger, die er bereits verwendet hat. Wenn für den Schutz AUTOMATIC angegeben ist, versucht der Server, Profile zu löschen, wenn Datenträger gelöscht werden.

Die Dokumentation zu dem RACF-Programm enthält ausführliche Informationen zu den Einstellungen für TAPEVOL und TAPEDSN und zu den Profilen, die erstellt werden, wenn diese Einstellungen aktiv sind.

#### UNIT

Gibt einen privaten Einheitennamen für eine Gruppe von Bandeinheiten an, die 3592-Band unterstützen. Dieser Parameter ist wahlfrei. Dieser Name darf maximal 8 Zeichen lang sein.

## UPDATE DEVCLASS (Einheitenklasse ECARTRIDGE für z/OS Media-Server aktualisieren)

Mit diesem Befehl können Sie eine Einheitenklasse aktualisieren, die Sie definiert haben, um mit einem z/OS Media-Server auf StorageTek-Laufwerke, wie z. B. StorageTek T9840 oder T10000, zuzugreifen. Die Einheitenklasse, die sich auf Speicher für den z/OS Media-Server bezieht, erfordert eine Kassettenarchivdefinition des Typs ZOSMEDIA.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
(1) (2)
>>-UPDate DEVclass--Einheitenklassenname----->
>--+-----+-----+----->
' -LIBRARY----ZOSMEDIA-Speicherarchiv-'
>--+-----+-----+----->
' -FORMAT-----+DRIVE-----' ' -ESTCAPacity----Größe-'
      +-T9840C----+
      +-T9840C-C--+
      +-T9840D----+
      +-T9840D-C--+
      +-T10000A----+
      +-T10000A-C--+
      +-T10000B----+
      +-T10000B-C--+
      +-T10000C----+
      +-T10000C-C--+
      +-T10000D----+
      +-T10000D-C-'
>--+-----+-----+----->
' -MOUNTRetention---Minuten-' ' -MOUNTWait----Minuten-'
>--+-----+-----+----->
' -MOUNTLimit-----+DRIVES--+ ' -COMpression-----+Yes--+ '
      +-Anzahl+          ' -No-- '
      +-0-----+
>--+-----+-----+----->
' -EXPIration----jjjjttt-' ' -RETention----Tage-'
>--+-----+-----+----->
' -PROtection-----+No-----+ '
      +-Yes-----+
      +-Automatic-'
>--+-----+-----+-----><
' -UNIT---Einheitenname-'
```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.

2. Der Parameter PREFIX kann mit diesem Befehl nicht aktualisiert werden. Sie müssen eine Einheitenklasse mit dem Wert erstellen, der für den Parameter PREFIX erforderlich ist.

## Parameter

### Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

### LIBRARY

Gibt den Namen eines Kassettenarchivs an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde. Das Kassettenarchiv und die Bandlaufwerke, die von dieser Einheitenklasse verwendet werden können, werden von dem z/OS Media-Server gesteuert.

Dieser Parameter ist wahlfrei.

Informationen zum Definieren eines Kassettenarchivs befinden sich unter dem Befehl DEFINE LIBRARY.

### FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Die folgende Tabelle enthält die Aufzeichnungsformate.

Tabelle 1. Aufzeichnungsformate für ECARTRIDGE-Bänder

| Format    | Geschätzte Kapazität | Beschreibung   |
|-----------|----------------------|--|
| DRIVE     | -                    | Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. DRIVE ist der Standardwert.<br>Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen. |
| T9840C    | 40 GB                | Dekomprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840C-C  | 80 GB                | Komprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840D    | 75 GB                | Dekomprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette   |
| T9840D-C  | 150 GB               | Komprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette   |
| T10000A   | 500 GB               | Dekomprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette  |
| T10000A-C | 1 TB                 | Komprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette  |
| T10000B   | 1 TB                 | Dekomprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette   |
| T10000B-C | 2 TB                 | Komprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette   |
| T10000C   | 5 TB                 | Dekomprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000C-C | 10 TB                | Komprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000D   | 8 TB                 | Dekomprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |
| T10000D-C | 15 TB                | Komprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette  |

#### Anmerkung:

- Einige Formate verwenden eine Komprimierungsfunktion der Bandlaufwerkhardware. Je nach Effektivität der Komprimierung kann die tatsächliche Kapazität doppelt so groß (oder größer) sein wie der aufgeführte Wert.
- T10000A-Laufwerke können nur das T10000A-Format lesen und schreiben. T10000B-Laufwerke können das T10000A-Format lesen, aber nicht schreiben. T10000C-Laufwerke können die T10000A- und T10000B-Formate lesen, aber nicht schreiben. T10000D-Laufwerke können die T10000A-, T10000B- und T10000C-Formate lesen, aber nicht schreiben.

### ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger mit sequenziellem Zugriff an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn die geschätzte Standardkapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist. Der Wert bestimmt nicht das auf dem Datenträger gespeicherte Datenvolumen. Der Server verwendet den Wert, um die Belegung zu schätzen, bevor ein Datenträger gefüllt ist. Wenn ein Datenträger voll ist, wird für die Berechnung der Belegung das tatsächlich auf dem Band gespeicherte Datenvolumen verwendet.

Geben Sie den Wert als ganze Zahl mit einem der folgenden Einheitenanzeiger an: **K** (KB), **M** (MB), **G** (GB) oder **T** (TB). Beispiel: Geben Sie mit dem Parameter `ESTCAPACITY=9G` an, dass die geschätzte Kapazität 9 GB beträgt. Der zulässige Mindestwert ist 100 KB (`ESTCAPACITY=100K`).

#### **MOUNTRetention**

Gibt die Anzahl Minuten an, die ein inaktiver Banddatenträger beibehalten wird, bevor er entladen wird. Die Zeitspanne für die Ladedauer beginnt nach Ablauf des Inaktivitätszeitlimits. Dieser Parameter ist wahlfrei. Geben Sie eine Zahl von 0 bis 9999 an.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

#### **MOUNTWait**

Gibt die maximale Anzahl Minuten an, die der z/OS Media-Server auf das Laden eines Datenträgers wartet. Wird auf die Ladeanforderung nicht innerhalb der angegebenen Zeit geantwortet, schlägt die Ladeanforderung fehl. Ist eine Einheit erfolgreich zugeordnet und wird die Anforderung zum Öffnen der Einheit nicht innerhalb der angegebenen Zeit ausgeführt, wird die Anforderung zum Öffnen der Einheit beendet und die Ladeanforderung schlägt fehl.

Dieser Parameter ist wahlfrei. Geben Sie eine Zahl von 1 bis 9999 an.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (`LIBTYPE=EXTERNAL`), geben Sie nicht den Parameter `MOUNTWAIT` an.

#### **MOUNTLimit**

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters `MOUNTLIMIT` für eine Einheitenklasse, schlägt die Transaktion fehl.

Sie können einen der folgenden Werte angeben:

#### **DRIVES**

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

#### **Anzahl**

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt. Sie können eine Zahl von 0 bis 4096 angeben.

#### **0 (Null)**

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können.

#### **COMPRESSION**

Gibt an, ob die Dateikomprimierung für diese Einheitenklasse verwendet wird. Dieser Parameter ist wahlfrei.

Sie können einen der folgenden Werte angeben:

#### **Yes**

Gibt an, dass die Daten der Banddatenträger komprimiert werden.

#### **No**

Gibt an, dass die Daten der Banddatenträger nicht komprimiert werden.

#### **EXPIRATION**

Gibt das Verfallsdatum an, das in den Bandkennsätzen für diese Einheitenklasse angegeben wird. Dieser Parameter ist wahlfrei.

Geben Sie das Datum an, an dem der Server das Band nicht mehr benötigt. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Geben Sie das Verfallsdatum im Format `jjjjtt` an (vier Stellen für das Jahr und drei Stellen für den Tag). Beispielsweise wird der 7. Januar 2014 als `2014007` angegeben (der siebte Tag des Jahres 2014).

Wenn Sie den Parameter `EXPIRATION` angeben, können Sie nicht den Parameter `RETENTION` angeben.

#### **RETENTION**

Gibt die Anzahl Tage an, die das Band aufbewahrt werden soll. Dieser Parameter ist wahlfrei.



Geben Sie die Anzahl der Tage (1 - 9999) an, die der Server das Band voraussichtlich verwenden wird. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Wenn Sie den Parameter RETENTION angeben, können Sie nicht den Parameter EXPIRATION angeben.

Tipp: Sie können für diesen Parameter den Wert null angeben. Dieser Wert sollte jedoch nur angegeben werden, wenn auch ein Wert für den Parameter EXPIRATION angegeben werden soll. Sie können keinen Wert für den Parameter EXPIRATION angeben, wenn Sie einen Wert ungleich null für den Parameter RETENTION angeben.

#### PROtection

Gibt an, ob das RACF-Programm (falls installiert) Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Wenn Schutz zur Verfügung gestellt wird, werden RACF-Profile bei der ersten Verwendung der Datenträger erstellt. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass das RACF-Programm keine Datenträger schützt, die dieser Einheitenklasse zugeordnet sind.

Yes

Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Für die Datenträger werden RACF-Profile erstellt, wenn der Server die Datenträger zum ersten Mal verwendet; die Profile werden jedoch nicht gelöscht, wenn Datenträger auf dem Server gelöscht werden. Die Profile müssen manuell gelöscht werden.

Tipp: Sind sensible Daten auf den Datenträgern gespeichert, die dieser Einheitenklasse zugeordnet sind, verwenden Sie PROTECTION=YES und löschen Sie RACF-Profile manuell nur nach dem Entfernen der Banddatenträger.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

#### Automatic

Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. RACF-Profile werden für Datenträger erstellt, wenn der Server zum ersten Mal die Datenträger verwendet. RACF-Profile werden gelöscht, wenn Datenträger auf dem Server gelöscht werden.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

Wichtig: Wird PROTECTION=AUTOMATIC angegeben, wird beim Löschen eines Datenträgers sein RACF-Profil gelöscht. Der Datenträger ist daher nicht mehr durch das RACF-Programm geschützt. Andere Benutzer können auf die Daten auf diesen Datenträgern zugreifen.

Wenn Sie PROTECTION=AUTOMATIC angeben, gibt der z/OS Media-Server RACROUTE-Befehle aus, um Profile zu löschen, wenn ein Datenträger auf dem Server gelöscht wird. Die ausgegebenen Löschbefehle sind von den aktuellen Systemwerten für TAPEVOL und TAPEDSN abhängig. Wenn die Systemeinstellungen geändert werden, löscht der z/OS Media-Server vorhandene Profile möglicherweise nicht.

Ändern Sie nicht die Einstellung in PROTECTION=AUTOMATIC für eine Einheitenklasse, für die PROTECTION=NO definiert wurde. Es können Datenträger ohne Profile vorhanden sein, und es werden Fehlermeldungen generiert, wenn diese Datenträger gelöscht werden. Wenn ein anderer Wert für PROTECTION erforderlich ist, definieren Sie eine neue Einheitenklasse.

Die Erstellung und das Löschen von Profilen erfolgen aufgrund der Schutzeinstellungen, wenn der Datenträger zum ersten Mal verwendet und wenn er gelöscht wird. Der Server erstellt keine Profile für Datenträger, die er bereits verwendet hat. Wenn für den Schutz AUTOMATIC angegeben ist, versucht der Server, Profile zu löschen, wenn Datenträger gelöscht werden.

Die Dokumentation zu dem RACF-Programm enthält ausführliche Informationen zu den Einstellungen für TAPEVOL und TAPEDSN und zu den Profilen, die erstellt werden, wenn diese Einstellungen aktiv sind.

#### UNIT

Gibt einen privaten Einheitennamen für eine Gruppe von Bandeinheiten an, die ECARTRIDGE-Bänder unterstützen. Verwenden Sie den Einheitennamen, der die Untergruppe der Laufwerke im Kassettenarchiv darstellt, die mit dem z/OS-System verbunden sind. Dieser Parameter ist wahlfrei. Der Einheitenname kann bis zu 8 Zeichen umfassen.

## UPDATE DEVCLASS (Einheitenklasse FILE für z/OS Media-Server aktualisieren)

---

Mit diesem Befehl können Sie eine Einheitenklasse aktualisieren, die Sie definiert haben, um mit einem z/OS Media-Server auf Dateien im Magnetplattenspeicher als Datenträger mit sequenziellem Zugriff (wie z. B. Band) zuzugreifen. Die Einheitenklasse, die sich auf Speicher für den z/OS Media-Server bezieht, erfordert eine Kassettenarchivdefinition des Typs ZOSMEDIA.

Ein Datenträger in dieser Einheitenklasse ist eine lineare VSAM-Datei (VSAM - Virtual Storage Access Method), auf die vom z/OS Media-Server zugegriffen wird. Arbeitsdatenträger können mit einer Einheitenklasse verwendet werden und der z/OS Media-Server ordnet dynamisch die lineare VSAM-Datei zu. Es ist nicht erforderlich, Datenträger für den Server zu definieren, um die Einheitenklasse zu verwenden. Wenn Sie Datenträger definieren, definieren Sie das Qualifikationsmerkmal der höheren Ebene so, dass SMS die Zuordnungsanforderung durch den z/OS Media-Server erkennt. Bei Verwendung von definierten Datenträgern wird die Funktion zum Formatieren von Datenträgern für den Server nicht unterstützt, wenn diese Einheitenklasse verwendet wird. Der z/OS Media-Server verwendet beim Füllen von FILE-Datenträgern ein FormatWrite-Feature des DFSMS Media Manager.

Sie können Datenträger für die Einheitenklasse FILE definieren, indem Sie den Befehl DEFINE VOLUME verwenden. Der z/OS Media-Server ordnet jedoch erst dann Speicherbereich für einen definierten Datenträger zu, wenn der Datenträger für seine erste Verwendung geöffnet wird.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
>>-UPDate DEVclass--Einheitenklassenname----->
>--+-----+--+-----+----->
  '-MAXCAPacity----Größe-'  '-PRIMARYalloc----Größe-'
>--+-----+----->
  '-SECONDARYalloc----Größe-'
>--+-----+----->
  '-PREFIX----Dateidatenträgerpräfix-'
>--+-----+-----<
  '-MOUNTLimit----Anzahl-'
```

## Parameter

---

Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

MAXCAPacity

Gibt die maximale Größe der Dateidatenträger an, die für einen Speicherpool in dieser Einheitenklasse definiert sind. Dieser Parameter ist wahlfrei.

Dieser Wert muss als ganze Zahl gefolgt von einem K (KB), M (MB), G (GB) oder T (TB) angegeben werden. Die Mindestgröße ist 1 MB (MAXCAPACITY=1M). Die maximale Größe ist 16384 GB (MAXCAPACITY=16384G).

PRIMARYalloc

Gibt den anfänglichen Speicherbereich an, der dynamisch zugeordnet wird, wenn ein neuer Datenträger geöffnet wird. Es muss genügend Speicherbereich verfügbar sein, um den Wert für die primäre Bereichszuordnung zu erfüllen. Die SMS-Richtlinie (SMS = Storage Management Subsystem) bestimmt, ob mehrere physische Datenträger verwendet werden können, um die Anforderung zur primären Bereichszuordnung zu erfüllen.

Dieser Parameter ist wahlfrei. Dieser Wert muss als ganze Zahl gefolgt von einem K (KB), M (MB), G (GB) oder T (TB) angegeben werden. Die Mindestgröße ist 100 KB (PRIMARYALLOC=100K). Die maximale Größe ist 16384 GB (MAXCAPACITY=16384G). Alle Werte werden auf das nächsthöhere Vielfache von 256 KB gerundet.

Um eine ineffiziente Speichernutzung zu vermeiden, verwendet die Operation für die dynamische Zuordnung den kleineren der in den beiden Parametern PRIMARYALLOC und MAXCAPACITY angegebenen Werte.

SMS-Routinen für die automatische Klassenauswahl können Einfluss darauf haben, ob die Werte für die Parameter PRIMARYALLOC und SECONDARYALLOC verwendet werden.

SECONDARYalloc

Gibt den Speicherbereich an, um den ein Dateidatenträger erweitert wird, wenn der Speicherbereich, der dem Dateidatenträger bereits zugeordnet ist, verbraucht ist. Die Datei für einen Dateidatenträger wird bis zu der Größe erweitert, die mit dem Parameter MAXCAPACITY definiert ist. Danach wird der Datenträger als voll markiert.

Da sich die sekundäre Bereichszuordnung einer linearen Datei nicht über physische Datenträger erstrecken kann, muss bei der Auswahl der Größe für die sekundäre Bereichszuordnung die Größe des physischen Datenträgers berücksichtigt werden. Beispielsweise haben physische Datenträger für ein 3390 Modell 3 eine Größe von ungefähr 2,8 GB. Um sicherzustellen, dass mit jeder Erweiterungsanforderung ungefähr der gesamte physische Datenträger belegt wird (aber nicht mehr), verwenden Sie eine Größe für die sekundäre Bereichszuordnung, die gerade unter 2,8 GB liegt. Mit einer Größe von 2600 MB für die sekundäre Bereichszuordnung wird genügend Speicherbereich für die VSAM-Datenträgerdatei, den Datenträgerkennsatz und das Datenträgerinhaltsverzeichnis zugeordnet.

Dieser Parameter ist wahlfrei. Dieser Wert muss als ganze Zahl gefolgt von einem K (KB), M (MB), G (GB) oder T (TB) angegeben werden. Der Mindestwert ist 0 KB (SECONDARYALLOC=0K). Der Maximalwert ist 16384 GB. Mit Ausnahme von 0 werden alle Werte auf das nächsthöhere Vielfache von 256 KB gerundet.

Geben Sie 0 (SECONDARYALLOC=0) an, kann der Dateidatenträger nicht über den Wert der primären Bereichszuordnung hinaus erweitert werden.

SMS-Routinen für die automatische Klassenauswahl können Einfluss darauf haben, ob die Werte für die Parameter PRIMARYALLOC und SECONDARYALLOC verwendet werden.

Wenn Sie einen Wert für den Parameter SECONDARYALLOCATION angeben, der nicht 0 ist, oder wenn Sie den Standardwert 2600M akzeptieren, muss für die SMS DATACLAS, der die PREFIX-Kennung zugeordnet ist (z. B. Qualifikationsmerkmal der höheren Ebene), das Attribut für die erweiterte Adressierbarkeit (Extended Addressability - EA) angegeben werden. Ohne das EA-Attribut beschränkt die SMS DATACLAS die Zuordnung des linearen VSAM-FILE-Datenträgers auf den primären Bereich. (Siehe die Beschreibung des Parameters PRIMARYALLOCATION). Wenn die Datei auf die primäre Bereichszuordnung beschränkt ist, kann die Datei vom z/OS Media-Server nicht erweitert werden, und der Datenträger wird als FULL markiert, bevor die maximale Kapazität erreicht ist.

Einschränkung: Stellen Sie sicher, dass sich die für die Parameter PRIMARYALLOC und SECONDARYALLOC angegebenen Werte innerhalb praktischer Grenzwerte für die Speichereinheit befinden. Der Server kann nicht überprüfen, ob die Werte praktische Grenzwerte für die Einheit überschreiten, und der Server überprüft nicht, ob die beiden Werte zusammen die aktuelle Einstellung für MAXCAPACITY überschreiten.

Tipp: Um bei der Angabe eines hohen Werts für den Parameter MAXCAPACITY Datenträger zu füllen, geben Sie hohe Werte für die Parameter PRIMARYALLOC und SECONDARYALLOC an. Verwenden Sie höhere MVS-Datenträgergrößen, um die Möglichkeit eines Erweiterungsfehlers zu reduzieren.

#### PREFIX

Gibt die Kennung der oberen Ebene des Dateinamens an, mit der Dateien von Arbeitsdatenträgern zugeordnet werden. Bei allen in dieser Einheitenklasse erstellten Arbeitsdateidatenträgern verwendet der Server dieses Präfix für die Erstellung des Dateinamens. Dieser Parameter ist wahlfrei. Die maximale Länge des Präfix, einschließlich Punkte, beträgt 32 Zeichen.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

`AB.CD2.E`

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@, #, \$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für einen Dateidatenträger unter Verwendung des Standardpräfixes ist `ADSM.B0000021.BFS`.

Wenn Sie eine Namenskonvention für Dateinamen haben, verwenden Sie ein Präfix, das Ihrer Namenskonvention entspricht. Der folgende Wert ist beispielsweise zulässig: `TSM.SERVER2.VSAMFILE`.

Wenn Sie mehrere Serverinstanzen für IBM Spectrum Protect oder Tivoli Storage Manager for z/OS Media ausführen, müssen Sie einen eindeutigen Wert für den Parameter PREFIX für jede Einheitenklasse verwenden, die Sie aktualisieren.

#### MOUNTLimit

Gibt die maximale Anzahl FILE-Datenträger an, die gleichzeitig für diese Einheitenklasse geöffnet sein können. Dieser Parameter ist wahlfrei. Für Einheiten 3995, die Einheiten 3390 emulieren, darf der Wert nicht höher sein als die Anzahl der parallelen Eingabe- und Ausgabedatenströme, die auf den Medien möglich sind, die die Datenträger speichern.

Der in diesem Parameter angegebene Wert ist wichtig, wenn das Umschalten von einem Datenträger zu einem anderen eine große Beeinträchtigung darstellt. Das Umschalten kann beispielsweise erfolgen, wenn Sie Einheiten IBM® 3995 verwenden, um Einheiten 3390 zu emulieren. Der angegebene Wert darf nicht höher als die Anzahl der physischen Laufwerke sein, die auf der Einheit verfügbar sind.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als

der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

## UPDATE DOMAIN (Maßnahmendomäne aktualisieren)

Mit diesem Befehl kann eine Maßnahmendomäne geändert werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für die angegebene Maßnahmendomäne erforderlich.

### Syntax

```
>>-UPDate Domain--Domänenname----->
>+-----+-----+-----+----->
  '-DEscription----Beschreibung-'
>+-----+-----+-----+----->
  '-BACKREtention----Tage-'  '-ARCHREtention----Tage-'
>+-----+-----+-----+-----+><
  |                               .-|-----|. |
  |                               v         | |
  '-ACTIVEDEStination-------Name_des_Pools_für_aktive_Daten----+-'
```

### Parameter

#### Domänenname (Erforderlich)

Gibt den Namen der Maßnahmendomäne an.

#### DEscription

Beschreibt die Maßnahmendomäne unter Verwendung einer Textfolge. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Soll eine zuvor definierte Beschreibung gelöscht werden, ist eine Nullzeichenfolge (") anzugeben.

#### BACKREtention

Gibt die Anzahl Tage an (ab dem Datum, an dem die Sicherungsversionen inaktiv wurden), die die Sicherungsversionen aufbewahrt werden sollen, die sich nicht mehr im Client-Dateisystem befinden. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl im Bereich von 0 bis 9999 angeben. Der Server verwendet den Wert für den Aufbewahrungszeitraum für Sicherung, um inaktive Versionen von Dateien zu verwalten, wenn eine der folgenden Bedingungen zutrifft:

- Eine Datei wird an eine neue Verwaltungsklasse erneut gebunden, aber die neue Verwaltungsklasse und die Standardverwaltungsklasse enthalten keine Sicherungskopiengruppe.
- Die Verwaltungsklasse, an die eine Datei gebunden ist, ist nicht mehr vorhanden. Die Standardverwaltungsklasse enthält keine Sicherungskopiengruppe.
- Die Sicherungskopiengruppe wird aus der Verwaltungsklasse gelöscht, an die eine Datei gebunden ist. Die Standardverwaltungsklasse enthält keine Sicherungskopiengruppe.

#### ARCHREtention

Gibt die Anzahl Tage an (ab dem Datum der Archivierung), die Archivierungskopien aufbewahrt werden sollen. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl im Bereich von 0 bis 30000 angeben. Der Server verwendet den Wert für den Aufbewahrungszeitraum für Archivierung, um Archivierungskopien von Dateien zu verwalten, wenn eine der folgenden Bedingungen zutrifft:

- Die Verwaltungsklasse, an die eine Datei gebunden ist, ist nicht mehr vorhanden. Die Standardverwaltungsklasse enthält keine Archivierungskopiengruppe.
- Die Archivierungskopiengruppe wird aus der Verwaltungsklasse gelöscht, an die eine Datei gebunden ist. Die Standardverwaltungsklasse enthält keine Archivierungskopiengruppe.

#### ACTIVEDEStination

Gibt die Namen der Pools für aktive Daten an, in denen aktive Versionen von Sicherungsdaten für Knoten gespeichert werden, die der Domäne zugeordnet sind. Dieser Parameter ist wahlfrei. Leerzeichen zwischen den Namen der Pools für aktive Daten sind nicht zulässig. Sie können maximal 10 Pools für aktive Daten für eine Domäne angeben.

Bevor der IBM Spectrum Protect-Server Daten in einen Pool für aktive Daten schreibt, überprüft er, ob der Knoten, der Eigner der Daten ist, einer Domäne zugeordnet ist, für die der Pool für aktive Daten in der ACTIVEDESTINATION-Liste aufgelistet ist. Stellt

der Server fest, dass der Knoten diese Kriterien erfüllt, werden die Daten im Pool für aktive Daten gespeichert. Werden die Kriterien vom Knoten nicht erfüllt, werden die Daten nicht im Pool für aktive Daten gespeichert. Werden mit der Funktion für simultanes Schreiben Daten in einen Pool für aktive Daten geschrieben, führt der Server die Prüfung während Sicherungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder durch Anwendungsclients unter Verwendung der IBM Spectrum Protect-API durch. Die Prüfung wird auch durchgeführt, wenn aktive Daten mit dem Befehl COPY ACTIVATEDATA kopiert werden.

## Beispiel: Den Aufbewahrungszeitraum für Sicherung für eine Maßnahmendomäne aktualisieren

Die Maßnahmendomäne ENGPOLDOM so aktualisieren, dass der Aufbewahrungszeitraum für Sicherung auf 90 Tage und der Aufbewahrungszeitraum für Archivierung auf zwei Jahre erweitert wird. Einen Pool für aktive Daten als Ziel für aktive Versionen von Sicherungsdaten angeben, die zu Knoten gehören, die der Domäne zugeordnet sind. Den Namen *engactivedata* für den Pool für aktive Daten verwenden. Geben Sie den folgenden Befehl aus:

```
update domain engpoldom description='Maßnahmendomäne für Entwicklung'
backretention=90 archretention=730 activedestination=engactivedata
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE DOMAIN


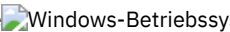


| Befehl           | Beschreibung   |
|------------------|--|
| COPY DOMAIN      | Erstellt eine Kopie einer Maßnahmendomäne.   |
| DEFINE DOMAIN    | Definiert eine Maßnahmendomäne, der Clients zugeordnet werden können.                      |
| DEFINE POLICYSET | Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.                  |
| DELETE DOMAIN    | Löscht eine Maßnahmendomäne und, falls vorhanden, Maßnahmenobjekte in der Maßnahmendomäne. |
| QUERY DOMAIN     | Zeigt Informationen über Maßnahmendomänen an.  |

## UPDATE DRIVE (Laufwerk aktualisieren)

Mit diesem Befehl kann ein Laufwerk aktualisiert werden.

## Berechtigungsklasse

Ausführliche und aktuelle Informationen zur Laufwerkunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

-  [AIX-Betriebssysteme](#)  [Windows-Betriebssysteme](#) Supported devices for AIX and Windows
-  [Linux-Betriebssysteme](#)  [Supported devices for Linux](#)

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-UPDate Drive--Kassettenarchivname--Laufwerkname----->
>+-----+-----+-----+-----+-----+-----+----->
  '-SERial-----+Seriennummer-+-'  '-ONLine-----+Yes+-'
                    '-AUTODetect---'          '-No--'
>+-----+-----+-----+-----+-----+-----+----->
  '-ELEMeNt-----+Adresse-----+'
                    '-AUTODetect-'
>+-----+-----+-----+-----+-----+-----+----->
  |                               (1) |
  '-ACSDRVID-----+Laufwerk-ID-----'
>+-----+-----+-----+-----+-----+-----+-----><
  |                               (2) |
  '-CLEANFREQuency-----+NONE-----+-'
                    |               (3) |
```

+ASNEEDED-----+  
'-Gigabyte-----'

Anmerkungen:

1. Der Parameter ACSDRVID ist nur für Laufwerke in ACSLS-Kassettenarchiven gültig.
2. Der Parameter CLEANFREQUENCY ist nur für Laufwerke in SCSI-Kassettenarchiven gültig.
3. Der Parameterwert CLEANFREQUENCY=ASNEEDED funktioniert nicht bei allen Bandlaufwerken. Weitere Informationen enthält die Parameterbeschreibung.

## Parameter

---

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, dem das Laufwerk zugeordnet ist.

Laufwerkname (Erforderlich)

Gibt den Namen an, der dem Laufwerk zugeordnet ist.

SERial

Gibt die Seriennummer der Laufwerke an, die aktualisiert werden. Dieser Parameter ist nur für Laufwerke in einem SCSI- oder VTL-Archiv (Virtual Tape Library) gültig. Dieser Parameter ist wahlfrei. Gültige Werte sind:

Seriennummer

Gibt die Seriennummer des Laufwerks an, das aktualisiert wird.

Anmerkung: Ist bereits ein Pfad zu diesem Laufwerk definiert, wird die eingegebene Nummer mit der Nummer verglichen, die von IBM Spectrum Protect erkannt wurde. Stimmen die Nummern nicht überein, schlägt der Befehl fehl.

AUTODETECT

Gibt an, dass die Seriennummer automatisch von IBM Spectrum Protect erkannt und verwendet wird, wenn bereits ein Pfad zu diesem Laufwerk definiert ist.

Ist kein Pfad zu diesem Laufwerk definiert, wird die Seriennummer nicht erkannt.

ONLine

Gibt an, ob das Laufwerk für die Verwendung verfügbar ist. Dieser Parameter gibt an, ob Laufwerke abgehängt und für andere Aktivitäten, wie beispielsweise für die Wartung, verwendet werden können. Dieser Parameter ist wahlfrei.

Sie können diesen Befehl ausgeben, wenn das Laufwerk in einem aktiven Prozess oder in einer aktiven Sitzung verwendet wird. Dies wird jedoch nicht empfohlen. Wenn Sie einen Befehl ausgeben, um das Laufwerk abzuhängen, während es im Gebrauch ist, wird eine Fehlermeldung ausgegeben. Der geladene Datenträger beendet den aktuellen Prozess. Wenn dieser Datenträger Teil einer Serie von Datenträgern für eine bestimmte Transaktion war, steht das Laufwerk nicht zur Verfügung, um das Laden der Serie abzuschließen. Sind keine anderen Laufwerke verfügbar, schlägt der Prozess fehl.

Achtung: Ist ein Laufwerk im Gebrauch, geben Sie nicht den Parameter ELEMENT mit dem Parameter ONLINE an. Das Laufwerk wird nicht aktualisiert, und der Befehl schlägt fehl.

Der Laufwerkstatus wird nicht geändert, auch wenn der Server angehalten und erneut gestartet wird. Ist ein Laufwerk offline, wenn der Server erneut gestartet wird, wird in einer Warnung angegeben, dass das Laufwerk manuell in den Online-Status versetzt werden muss. Werden alle Laufwerke in einem Kassettenarchiv in den Offline-Status geändert, können Prozesse, die einen Mountpunkt für ein Kassettenarchiv benötigen, nicht ausgeführt werden (sie reihen sich nicht in die Warteschlange für einen Mountpunkt ein).

YES

Gibt an, dass das Laufwerk für die Verwendung verfügbar (angehängt) ist.

No

Gibt an, dass das Laufwerk nicht für die Verwendung verfügbar ist (das Laufwerk ist abgehängt).

ELEMent

Gibt die Elementadresse des Laufwerks in einem SCSI- oder VTL-Archiv an. Der Server verwendet die Elementadresse, um die physische Adresse des Laufwerks mit der SCSI-Adresse des Laufwerks zu verbinden. Dieser Parameter ist nur für ein Laufwerk in einem SCSI- oder VTL-Archiv gültig, wenn der Befehl von einem IBM Spectrum Protect-Kassettenarchivmanagerserver ausgegeben wird. Gültige Werte sind:

Adresse

Gibt die Elementadresse des Laufwerks an, das aktualisiert wird.

Zum Lokalisieren der Elementadresse für die Archivkonfiguration die Informationen des Herstellers zu Rate ziehen.

Hinweis: Ist bereits ein Pfad zu diesem Laufwerk definiert, wird die eingegebene Nummer mit der Nummer verglichen, die zuvor von IBM Spectrum Protect erkannt wurde. Stimmen die Nummern nicht überein, schlägt dieser Befehl fehl.

## AUTODETECT

Gibt an, dass die Elementnummer automatisch von IBM Spectrum Protect erkannt und verwendet wird, wenn bereits ein Pfad zu diesem Laufwerk definiert ist.

Ist kein Pfad zu diesem Laufwerk definiert, wird die Elementnummer nicht erkannt.

Einschränkung: Wenn das Kassettenarchiv, in dem sich das Laufwerk befindet, den SCSI-Befehl "Read Element Status" nicht unterstützt, und für den Parameter ELEMENT der Wert AUTODETECT angegeben wird, schlägt der Befehl mit einer IBM Spectrum Protect-Fehlernachricht fehl.

## ACSDRVID

Gibt die ID des Laufwerks an, auf das in einem ACSLS-Kassettenarchiv zugegriffen wird. Die Laufwerk-ID ist eine Zahlengruppe, die die physische Adresse eines Laufwerks in einem ACSLS-Kassettenarchiv angibt. Diese Laufwerk-ID muss als *a,l,p,d*, angegeben werden, wobei *a* die ACSID, *l* das LSM (Library Storage Module), *p* die Anzeigennummer und *d* die Laufwerk-ID ist. Der Server benötigt die Laufwerk-ID, um die physische Adresse des Laufwerks mit der SCSI-Adresse des Laufwerks zu verbinden. Die StorageTek-Dokumentation enthält ausführliche Informationen.

## CLEANFREQuency

Gibt an, wie oft der Server die Laufwerkreinigung aktiviert. Dieser Parameter ist wahlfrei. Um die Reinigung für ein automatisiertes Kassettenarchiv nahezu vollständig zu automatisieren, müssen Sie eine Reinigungskassette in den Datenträgerbestand des Kassettenarchivs zurückgestellt haben. Bei Verwendung der speicherarchivbasierten Reinigung wird NONE empfohlen, wenn Ihr Speicherarchivtyp diese Funktion unterstützt. Dieser Parameter ist nur für Laufwerke in SCSI-Kassettenarchiven gültig, und ist für extern verwaltete Kassettenarchive, wie beispielsweise 3494-Kassettenarchive oder StorageTek-Kassettenarchive, die unter ACSLS verwaltet werden, nicht gültig.

Wichtig: Es gibt einige Besonderheiten, die beachtet werden müssen, wenn die vom Server aktivierte Laufwerkreinigung bei einem SCSI-Kassettenarchiv verwendet werden soll, das eine automatische Laufwerkreinigungsunterstützung in seiner Einheitenhardware zur Verfügung stellt.

## NONE

Gibt an, dass der Server die Reinigung dieses Laufwerks nicht verfolgt. Diesen Parameter für Kassettenarchive verwenden, die über ihre eigene automatische Reinigungsunterstützung verfügen.

## ASNEEDED

Gibt an, dass der Server das Laufwerk mit einer zurückgestellten Reinigungskassette nur lädt, wenn ein Laufwerk dem Einheitenreiber mitteilt, dass eine Reinigung erforderlich ist.

Der Parameterwert CLEANFREQUENCY=ASNEEDED funktioniert nicht bei allen Bandlaufwerken. Detaillierte Laufwerkdaten finden Sie auf der Website für unterstützte Einheiten für Ihr Betriebssystem. Wird ASNEEDED nicht unterstützt, können Sie den Gigabyte-Wert für die automatische Reinigung verwenden.

Für IBM 3592- und LTO-Laufwerke wird die speicherarchivbasierte Reinigung empfohlen. Wird die speicherarchivbasierte Reinigung nicht unterstützt, muss ASNEEDED verwendet werden. Gigabyte wird nicht empfohlen.

Einschränkung: IBM Spectrum Protect steuert nicht die Laufwerke, die mit dem NAS-Dateiserver verbunden sind. Ist ein Laufwerk nur mit einem NAS-Dateiserver verbunden (keine Verbindung zu einem Speicheragenten oder Server), geben Sie nicht ASNEEDED für die Häufigkeit der Reinigung an.

## Gigabyte

Gibt in Gigabyte an, wieviel Daten auf dem Laufwerk verarbeitet werden, bevor der Server das Laufwerk mit einer Reinigungskassette lädt. Der Server setzt den Zähler für die verarbeiteten Gigabyte zurück, wenn eine Reinigungskassette in das Laufwerk geladen wird.

Wichtig: Bei CLEANFREQUENCY=Gigabyte kann die Laufwerkreinigung erfolgen, bevor die Einstellung für Gigabyte erreicht ist, wenn das Laufwerk den Einheitenreiber benachrichtigt, dass eine Reinigung erforderlich ist.

Lesen Sie die Empfehlungen des Laufwerkherstellers bezüglich der Reinigung. Werden Empfehlungen für die Reinigungshäufigkeit in Stunden der Verwendung gegeben, führen Sie wie folgt eine Umrechnung in einen Gigabytewert durch:

1. Verwenden Sie den Wert für Byte pro Sekunde des Laufwerks, um einen Wert für Gigabyte pro Stunde zu ermitteln.
2. Multiplizieren Sie den Wert für Gigabyte pro Stunde mit den empfohlenen Stunden der Verwendung zwischen den Reinigungen.
3. Verwenden Sie das Ergebnis als Wert für die Reinigungshäufigkeit.

Tipp: Geben Sie für IBM 3590 einen Wert für die Reinigungshäufigkeit an, um eine adäquate Reinigung der Laufwerke sicherzustellen. Lesen Sie die Empfehlungen des Laufwerkherstellers bezüglich der Reinigung. Bei Verwendung der von IBM empfohlenen Reinigungshäufigkeit wird die Reinigung der Laufwerke nicht zu oft durchgeführt.

## Beispiel: Die Elementadresse für ein Laufwerk aktualisieren

Für das Laufwerk DRIVE3, das sich im Kassettenarchiv AUTO befindet, soll die Elementadresse in 119 geändert werden.





```

| (4) |
+-ACTIVE_DATA_HIGH_PRIORITY-----+
+-DEFAULT-----+
'-NONE-----'

>-----<
| (3) |
'-REPLState-----+ENabled-----+'
+DISabled--+
'-PURGEdata-'

```

Anmerkungen:

1. Sie können keine Dateibereichs-ID angeben, wenn Sie Platzhalterzeichen für den Namen des Clientknotens verwenden.
2. Jede Regel kann nur einmal angegeben werden.
3. Sie müssen entweder den Parameter REPLRULE oder REPLSTATE in diesem Befehl angeben.
4. Die Regeln ACTIVE\_DATA und ACTIVE\_DATA\_HIGH\_PRIORITY sind nur gültig, wenn Sie DATATYPE=BACKUP angeben.

## Parameter

### Knotenname (Erforderlich)

Gibt den Clientknoten an, zu dem der Dateibereich gehört. Dieser Name kann mithilfe von Platzhalterzeichen angegeben werden. Dateibereichs-IDs können jedoch zwischen Clientknoten für denselben Dateibereich unterschiedlich sein. Daher können Sie nicht Platzhalterzeichen für den Namen des Clientknotens und die Dateibereichs-ID als Wert für den Parameter NAMETYPE angeben.

### Dateibereichsname (Erforderlich)

Gibt den Namen des Dateibereichs an, der aktualisiert werden soll. Sie können Platzhalterzeichen oder eine durch Kommas dargestellte Liste verwenden, um Namen anzugeben.

Bei einem Server, der über Clients mit Unicode-fähigen Dateibereichen verfügt, muss möglicherweise der Server die eingegebenen Dateibereichsnamen konvertieren. Beispielsweise muss der Server gegebenenfalls einen Namen aus der Zeichenumsetztabelle des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich in der Beschreibung des Parameters NAMETYPE. Geben Sie nur ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter CODETYPE verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

Bei Dateibereichsnamen muss die Groß-/Kleinschreibung berücksichtigt werden. Um die korrekte Schreibweise für den Dateibereich zu bestimmen, der aktualisiert werden soll, verwenden Sie den Befehl QUERY FILESPACE.

### NAMETYPE

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Sie können diesen Parameter für Unicode-fähige IBM Spectrum Protect-Clients verwenden, die über die Betriebssysteme Windows, Macintosh OS X und NetWare verfügen. Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen eingeben. Der Standardwert lautet SERVER. Sie können einen der folgenden Werte angeben:

#### SERVER

Der Server verwendet die Zeichenumsetztabelle des Servers, um Dateibereichsnamen zu interpretieren.

#### UNICODE

Der Server konvertiert Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Schlägt die Konvertierung fehl, kann der Name Fragezeichen, Leerzeichen oder Auslassungen (...) enthalten.

#### FSID

Der Server interpretiert Dateibereichsnamen als Dateibereichs-IDs.

### CODETYPE

Gibt den Typ der Dateibereiche an, die bei der Knotenreplikationsverarbeitung berücksichtigt werden sollen. Der Standardwert lautet BOTH. Dieser Standardwert bedeutet, dass Dateibereiche unabhängig von der Art der Zeichenumsetztabelle eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben. Sie können einen der folgenden Werte angeben:

#### UNICODE

Gibt nur Dateibereiche an, die in Unicode sind.

#### NONUNICODE

Gibt nur Dateibereiche an, die nicht in Unicode sind.

#### BOTH

Gibt alle Dateibereiche unabhängig von der Art der Zeichenumsetztabelle an.

## DATATYPE (Erforderlich)

Gibt den Datentyp an, für den eine Replikationsregel gilt. Bei der Angabe mehrerer Datentypen müssen die Datentypen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Sie können die folgenden Werte angeben:

### BACKUP

Gibt den Typ 'Sicherungsdaten' an.

### ARCHIVE

Gibt den Typ 'Archivierungsdaten' an.

### SPACEMANAGED

Gibt den Typ 'Speicherverwaltete Daten' an.

## REPLRULE

Gibt die Replikationsregel an, die für einen Datentyp gilt. Sie können keine Platzhalterzeichen verwenden. Werden mehrere Datentypen angegeben, gilt die Replikationsregel für jeden Datentyp. Wenn Sie beispielsweise `DATATYPE=BACKUP, ARCHIVE` angeben, gilt die Replikationsregel für Sicherungsdaten und Archivierungsdaten.

Einschränkung: Der Parameter `REPLRULE` ist optional. Wird er jedoch nicht angegeben, müssen Sie den Parameter `REPLSTATE` angeben.

Sie können Replikationsregeln für normale Priorität oder Replikationsregeln für hohe Priorität angeben. In einem Replikationsprozess, der sowohl Daten mit normaler Priorität als auch Daten mit hoher Priorität einschließt, werden Daten mit hoher Priorität zuerst repliziert. Bevor Sie eine Regel angeben, beachten Sie die Reihenfolge, in der die Daten repliziert werden sollen.

Beispiel: Angenommen, ein Dateibereich enthält aktive Sicherungsdaten und Archivierungsdaten. Die Replikation der aktiven Sicherungsdaten hat eine höhere Priorität als die der Archivierungsdaten. Um die aktiven Sicherungsdaten zu priorisieren, geben Sie `DATATYPE=BACKUP REPLRULE=ACTIVE_DATA_HIGH_PRIORITY` an. Um Archivierungsdaten eine normale Priorität zuzuordnen, geben Sie den Befehl `UPDATE FILESPACE` erneut aus und geben Sie `DATATYPE=ARCHIVE REPLRULE=ALL_DATA` an.

Sie können die folgenden Regeln angeben:

### ALL\_DATA

Repliziert Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten. Die Daten werden mit einer normalen Priorität repliziert.

### ACTIVE\_DATA

Repliziert nur die aktiven Sicherungsdaten in einem Dateibereich. Die Daten werden mit einer normalen Priorität repliziert. Achtung: Wenn Sie `ACTIVE_DATA` angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

- Wenn eine frühere Serverversion als Version 7.1.1 auf dem Quellen- oder Zielreplikationsserver installiert ist.
- Wenn Sie den Befehl `REPLICATE NODE` mit dem Parameter `FORCERECONCILE=YES` verwenden.
- Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Serverversion vor Version 7.1.1 ausführen.

Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

### ALL\_DATA\_HIGH\_PRIORITY

Repliziert Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten. Die Daten werden mit einer hohen Priorität repliziert.

### ACTIVE\_DATA\_HIGH\_PRIORITY

Diese Regel entspricht der Replikationsregel `ACTIVE_DATA`, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden.

### DEFAULT

Daten werden gemäß der Clientknotenregel für den Datentyp repliziert.

Beispiel: Angenommen, Sie möchten die Archivierungsdaten in allen Dateibereichen replizieren, die zu einem Clientknoten gehören. Die Replikation der Archivierungsdaten hat eine hohe Priorität. Eine Methode zur Ausführung dieser Task ist die Angabe von `DATATYPE=ARCHIVE REPLRULE=DEFAULT` für jeden Dateibereich. Stellen Sie sicher, dass die Clientreplikationsregel für Archivierungsdaten auf `ALL_DATA_HIGH_PRIORITY` oder `DEFAULT` gesetzt ist. Lautet die Clientreplikationsregel `DEFAULT`, muss die Serverreplikationsregel für Archivierungsdaten auf `ALL_DATA_HIGH_PRIORITY` gesetzt werden.

### NONE

Daten werden nicht repliziert. Sollen beispielsweise die speicherverwalteten Daten in einem Dateibereich nicht repliziert werden, geben Sie `DATATYPE=SPACEMANAGED REPLRULE=NONE` an.

## REPLState

Gibt den Replikationsstatus für einen Datentyp an. Wenn Sie mehrere Datentypen angegeben haben, gilt der Status für alle Datentypen. Haben Sie beispielsweise `DATATYPE=BACKUP,ARCHIVE` angegeben, gilt der Status für Sicherungs- und Archivierungsdaten.

Der Parameter `REPLSTATE` ist optional. Wird er jedoch nicht angegeben, müssen Sie den Parameter `REPLRULE` angeben. Sie können einen der folgenden Werte für den Parameter `REPLSTATE` angeben:

### ENabled

Gibt an, dass der Datentyp für die Replikation aktiviert ist.

### DISabled

Gibt an, dass die Replikation erst stattfindet, wenn sie aktiviert wurde.

### PURGEdata

Gibt an, dass Daten auf dem Zielreplikationsserver gelöscht werden. Der Typ der Daten, die gelöscht werden, ist der Datentyp, der mit dem Parameter `DATATYPE` angegeben wurde. Geben Sie beispielsweise `DATATYPE=BACKUP,ARCHIVE` und `REPLSTATE=PURGEDATA` an, werden Sicherungs- und Archivierungsdaten aus dem Dateibereich auf dem Zielreplikationsserver gelöscht.

Nach dem Löschen der Daten wird der Parameter `REPLSTATE` auf `DISABLED` gesetzt. Damit wird eine zukünftige Replikation des Datentyps oder der Datentypen verhindert. Die Replikationsregel für den Datentyp wird auf `DEFAULT` gesetzt.

Hinweis: Mit der `PURGEDATA`-Verarbeitung werden keine Dateibereiche gelöscht. Nur Daten werden gelöscht. Der Dateibereich wird in der Ausgabe des Befehls `QUERY OCCUPANCY` als leer angezeigt.

## Beispiel: Replikationsregeln für zwei Datentypen aktualisieren

`NODE1` verfügt über drei Dateibereiche: `/a`, `/b` und `/c`. Die Replikationsregeln für alle Dateibereiche sind auf `ALL_DATA` gesetzt. Sie möchten jedoch die Sicherungs- und Archivierungsdaten im Dateibereich `/a` replizieren, bevor die Daten in den anderen Dateibereichen repliziert werden.

```
update filespace node1 /a datatype=backup,archive replrule=
    all_data_high_priority
```

## Beispiel: Replikationsregeln für zwei Datentypen aktualisieren

`NODE2` verfügt über zwei Dateibereiche: `/a` und `/b`. Sie möchten die Replikation aller Daten im Dateibereich `/b` vorübergehend aussetzen.

```
update filespace node2 /b datatype=backup,archive,spacemanaged
    replstate=disabled
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für `UPDATE FILESPACE`

| Befehl                            | Beschreibung   |
|-----------------------------------|--|
| <code>QUERY FILESPACE</code>      | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.  |
| <code>QUERY NODE</code>           | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.  |
| <code>QUERY REPLICATION</code>    | Zeigt Informationen zu Knotenreplikationsprozessen an.   |
| <code>QUERY STATUS</code>         | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den <code>SET</code> -Befehlen ausgewählten Einstellungen. |
| <code>REPLICATE NODE</code>       | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |
| <code>SET REPLETENTION</code>     | Gibt den Aufbewahrungszeitraum für Replikationsprotokollsätze an.  |
| <code>UPDATE NODE</code>          | Ändert die Attribute, die einem Clientknoten zugeordnet sind.  |
| <code>UPDATE REPLRULE</code>      | Aktiviert oder inaktiviert Replikationsregeln.   |
| <code>VALIDATE REPLICATION</code> | Überprüft die Replikation für Dateibereiche und Datentypen.  |

## UPDATE LIBRARY (Kassettenarchiv aktualisieren)

Verwenden Sie diesen Befehl, um eine Kassettenarchivdefinition zu aktualisieren.

Um den Einheitennamen, die ACS-Nummer oder den Pfadnamen des externen Managers eines Kassettenarchivs zu aktualisieren, müssen Sie den Befehl UPDATE PATH verwenden.

Um den Einheitennamen oder den Pfadnamen des externen Managers eines Kassettenarchivs zu aktualisieren, müssen Sie den Befehl UPDATE PATH verwenden.

Syntax- und Parameterbeschreibungen sind für die folgenden Kassettenarchivtypen verfügbar.

- UPDATE LIBRARY (349X-Kassettenarchiv aktualisieren)
- UPDATE LIBRARY (ACSLs-Kassettenarchiv aktualisieren)
- UPDATE LIBRARY (Externes Kassettenarchiv aktualisieren)
- UPDATE LIBRARY (Kassettenarchiv FILE aktualisieren)
- UPDATE LIBRARY (Manuelles Kassettenarchiv aktualisieren)
- UPDATE LIBRARY (SCSI-Kassettenarchiv aktualisieren)
- UPDATE LIBRARY (Gemeinsam genutztes Kassettenarchiv aktualisieren)
- UPDATE LIBRARY (VTL-Speicherarchiv aktualisieren)

Ausführliche und aktuelle Informationen zur Kassettenarchivunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

- Supported devices for AIX and Windows
- Supported devices for Linux

Um Banddatenträger in SCSI-Speicherarchiven automatisch zu kennzeichnen, verwenden Sie den Parameter AUTOLABEL in den Befehlen DEFINE LIBRARY und UPDATE LIBRARY. Wird dieser Parameter verwendet, ist es nicht erforderlich, eine Gruppe von Bändern vorab zu kennzeichnen. Außerdem ist die Verwendung dieses Parameters effizienter als die Verwendung des Befehls LABEL LIBVOLUME, der es erfordert, dass Datenträger separat bereitgestellt werden. Wenn Sie den Parameter AUTOLABEL verwenden, müssen Sie Bänder zurückstellen, indem Sie CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME angeben.

Ein Kennsatz darf keine eingebetteten Leerzeichen oder Punkte enthalten und muss gültig sein, wenn er als Dateiname auf den Datenträgern verwendet wird.

Sie müssen CD-ROM-, Zip- oder Jaz-Datenträger mit den Dienstprogrammen des Einheitenherstellers oder den Windows-Dienstprogrammen kennzeichnen, da IBM Spectrum Protect keine Dienstprogramme zum Formatieren oder Kennzeichnen dieser Datenträgertypen bereitstellt. Die Dienstprogramme des Betriebssystems schließen das Plattenverwaltungsprogramm (Disk Administrator) (eine grafische Benutzerschnittstelle) und den Befehl zum Zuordnen von Kennsätzen ein.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE LIBRARY

| Befehl             | Beschreibung  |
|--------------------|---|
| AUDIT LIBRARY      | Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet. |
| CHECKIN LIBVOLUME  | Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.                            |
| CHECKOUT LIBVOLUME | Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.                          |
| DEFINE DRIVE       | Ordnet ein Laufwerk einem Kassettenarchiv zu.   |
| DEFINE LIBRARY     | Definiert ein automatisiertes oder manuelles Kassettenarchiv.                                       |
| DEFINE PATH        | Definiert einen Pfad von einer Quelle zu einem Ziel.  |
| DELETE DRIVE       | Löscht ein Laufwerk aus einem Kassettenarchiv.  |
| DELETE LIBRARY     | Löscht ein Kassettenarchiv.   |
| DELETE PATH        | Löscht einen Pfad von einer Quelle zu einem Ziel.   |
| LABEL LIBVOLUME    | Kennzeichnet Datenträger in manuellen oder automatisierten Kassettenarchiven.                       |
| QUERY DRIVE        | Zeigt Informationen zu Laufwerken an.   |

| Befehl           | Beschreibung  |
|------------------|---|
| QUERY LIBRARY    | Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an. |
| QUERY PATH       | Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.     |
| UPDATE DRIVE     | Ändert die Attribute eines Laufwerks.                               |
| UPDATE LIBVOLUME | Ändert den Status eines Speicherdatenträgers.                       |
| UPDATE PATH      | Ändert die zu einem Pfad gehörigen Attribute.                       |

## UPDATE LIBRARY (349X-Kassettenarchiv aktualisieren)

Verwenden Sie diese Syntax, um ein 349X-Kassettenarchiv zu aktualisieren.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-UPDate LIBRARY--Speicherarchivname--+-+-----+----->
                                     '-SHARED-----Yes---'

>--+-+-----+----->
   '-RESETDrives-----+Yes-+-'
                                     '-No--'

>--+-+-----+----->
   '-AUTOLabel-----+No-----+-'
                                     +-Yes-----+
                                     '-OVERWRITE-'

>--+-+-----+-----><
   '-WORMSCatchcategory-----Anzahl-'
```

### Parameter

**Speicherarchivname (Erforderlich)**

Gibt den Namen des Kassettenarchivs an, das aktualisiert werden soll.

**SHARED**

Gibt an, dass dieses Speicherarchiv mit anderen Servern in einem Speicherbereichsnetz (SAN) gemeinsam genutzt wird. Dieser Befehl muss von dem Server ausgegeben werden, der als primärer Speicherarchivmanager für das gemeinsam genutzte Speicherarchiv definiert ist. Dieser Parameter ist für Speicherarchive erforderlich, die für einen Speicherarchivmanager definiert sind, und ist für Speicherarchive erforderlich, die für NDMP-Operationen verwendet werden. Geben Sie SHARED=YES an, um ein Speicherarchiv zu aktualisieren, das gegenwärtig nicht gemeinsam genutzt wird.

Wichtig: Hat ein Speicherarchiv einen Pfad von einer Einheit zum Versetzen von Daten (beispielsweise einem NAS-Dateiserver), aber keine Verbindung zu dem Server, kann das Speicherarchiv nicht mit einem anderen Server gemeinsam genutzt werden.

**AUTOLabel**

Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

**No**

Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

**Yes**

Gibt an, daß der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

**OVERWRITE**

Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.


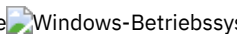
**WORMSCatchcategory**


Gibt die Kategoriennummer an, die für WORM-Arbeitsdatenträger in dem Kassettenarchiv verwendet werden soll. Dieser Parameter ist erforderlich, wenn WORM-Datenträger verwendet werden. Es kann eine Zahl von 1 bis 65279 angegeben werden. Diese Zahl muss eindeutig sein. Sie kann nicht mit anderen Anwendungen oder definierten Kassettenarchiven gemeinsam genutzt werden, und sie muss sich von den anderen Kategoriennummern in diesem Kassettenarchiv unterscheiden. Dieser Parameter ist nur bei Verwendung von WORM-Datenträgern 3592 gültig.

Einschränkung: Dieser Parameter kann nur aktualisiert werden, wenn der Parameter WORM für die Einheitenklasse auf YES gesetzt ist und für WORMSCRATCHCATEGORY gegenwärtig kein Wert definiert ist.

#### RESETDrives

Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird.

  Wird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

 Wird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

In der folgenden Tabelle sind die drei möglichen Konfigurationen für Laufwerke beschrieben, die an NAS-Einheiten angeschlossen werden können.

Tabelle 1. Konfigurationen für Laufwerke, die an NAS-Einheiten angeschlossen sind

| Konfiguration der Speicherarchivereinheit   | Verhalten für persistente Reserve  |
|---|--|
| Die Speicherarchivereinheit wird an den IBM Spectrum Protect-Server angeschlossen, und die Bandlaufwerke werden vom Server und der NAS-Einheit gemeinsam genutzt. | Die Zurückstellung der Laufwerkreservierung wird unterstützt, wenn die NAS-Einheit die persistente Reserve unterstützt und diese aktiviert ist. Weitere Informationen zum Definieren der persistenten Reserve finden Sie in der Dokumentation für Ihre NAS-Einheit.  |
| Die Speicherarchivereinheit wird an den IBM Spectrum Protect-Server angeschlossen, und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen.            | Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben. |

Yes

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird.

No

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.



Yes



Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird.

No

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

## Beispiel: Neue Einheiten einem gemeinsam genutzten Kassettenarchiv hinzufügen

Das gemeinsam benutzte 3494-Kassettenarchiv 3494LIB2 mit neuen Einheitennamen aktualisieren.  

```
update library 3494lib2 device=/dev/lmcp1,/dev/lmcp2,/dev/lmcp3
```




```
update library 3494lib device=lb3.0.0.0,lb4.0.0.0,lb5.0.0.0
```

# UPDATE LIBRARY (ACSLs-Kassettenarchiv aktualisieren)

Verwenden Sie diese Syntax, um ein ACSLS-Kassettenarchiv zu aktualisieren.

## Berechtigungsklasse

 Windows-Betriebssysteme Um ACSLS-Funktionen verwenden zu können, ist die Installation von StorageTek Library Attach-Software erforderlich.

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-UPDate LIBRARY--Speicherarchivname--+-+-----+-----+----->
                                     '-SHARED-----Yes--'
>+-+-----+-----+----->
  '-RESETDrives-----+Yes-+-'
                               '-No--'
>+-+-----+-----+-----+-----+-----><
  '-AUTOLabel-----+No-----+-'   '-ACSID-----Nummer-'
                               +-Yes-----+
                               '-OVERWRITE-'
```

## Parameter

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das aktualisiert werden soll.



SHARED


Gibt an, dass dieses Speicherarchiv mit anderen Servern in einem Speicherbereichsnetz (SAN) gemeinsam genutzt wird. Dieser Befehl muss von dem Server ausgegeben werden, der als primärer Speicherarchivmanager für das gemeinsam genutzte Speicherarchiv definiert ist. Dieser Parameter ist für Speicherarchive erforderlich, die für einen Speicherarchivmanager definiert sind, und ist für Speicherarchive erforderlich, die für NDMP-Operationen verwendet werden. Geben Sie SHARED=YES an, um ein Speicherarchiv zu aktualisieren, das gegenwärtig nicht gemeinsam genutzt wird.

Wichtig: Hat ein Speicherarchiv einen Pfad von einer Einheit zum Versetzen von Daten (beispielsweise einem NAS-Dateiserver), aber keine Verbindung zu dem Server, kann das Speicherarchiv nicht mit einem anderen Server gemeinsam genutzt werden.

RESETDrives

Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird.

 AIX-Betriebssysteme  Windows-Betriebssysteme Wird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

 Linux-Betriebssysteme Wird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

In der folgenden Tabelle sind die drei möglichen Konfigurationen für Laufwerke beschrieben, die an NAS-Einheiten angeschlossen werden können.

Tabelle 1. Konfigurationen für Laufwerke, die an NAS-Einheiten angeschlossen sind

| Konfiguration der Speicherarchiveinheit | Verhalten für persistente Reserve |
|---|-----------------------------------|
|---|-----------------------------------|

| Konfiguration der Speicherarchivereinheit   | Verhalten für persistente Reserve  |
|---|--|
| Die Speicherarchivereinheit wird an den IBM Spectrum Protect-Server angeschlossen, und die Bandlaufwerke werden vom Server und der NAS-Einheit gemeinsam genutzt. | Die Zurückstellung der Laufwerkreservierung wird unterstützt, wenn die NAS-Einheit die persistente Reserve unterstützt und diese aktiviert ist. Weitere Informationen zum Definieren der persistenten Reserve finden Sie in der Dokumentation für Ihre NAS-Einheit.  |
| Die Speicherarchivereinheit wird an den IBM Spectrum Protect-Server angeschlossen, und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen.            | Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben. |

Yes

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird.

No

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.



Yes

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird.

No

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

AUTOLabel

Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

No

Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes

Gibt an, daß der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE

Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

ACSID (Erforderlich)

Gibt die Nummer dieses StorageTek-Kassettenarchivs an, das von ACSSA (Automatic Cartridge System System Administrator) zugeordnet wird. Hierbei kann es sich um eine Zahl von 0 bis 126 handeln. Geben Sie den Befehl QUERY ACS auf dem System aus, um die Nummer für die Kassettenarchiv-ID abzufragen. Dieser Parameter ist erforderlich.

Die StorageTek-Dokumentation enthält weitere Informationen.

## Beispiel: Eine ID-Nummer für ein ACSLS-Kassettenarchiv aktualisieren

Das ACSLS-Kassettenarchiv ACSLSLIB mit einer neuen ID-Nummer aktualisieren.

```
update library acslslib acsid=1
```

## UPDATE LIBRARY (Externes Kassettenarchiv aktualisieren)

Verwenden Sie diese Syntax, um ein externes Kassettenarchiv zu aktualisieren.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax



```
>>-UPDate LIBRary--Speicherarchivname----->
>--+-----+-----><
  '-AUTOLabel--==+-No-----+-'
      +-Yes-----+
  '-OVERWRITE-'
```

## Parameter

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das aktualisiert werden soll.

AUTOLabel

Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

No

Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.



Yes

Gibt an, daß der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE

Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

## Beispiel: Den Pfadnamen eines externen Kassettenarchivs aktualisieren

Das externe Kassettenarchiv EXTLIB mit einem neuen Pfadnamen für den Datenträgermanager aktualisieren.  AIX-Betriebssysteme  
 Linux-Betriebssysteme

```
update library extlib externalmanager=/v/server/mediamanager
```

 Windows-Betriebssysteme

```
update library extlib externalmanager=c:\server\mediamanager
```

## UPDATE LIBRARY (Kassettenarchiv FILE aktualisieren)

Verwenden Sie diese Syntax, um ein Kassettenarchiv FILE zu aktualisieren.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-UPDate LIBRary--Speicherarchivname--+-+-----+-----><
      '-SHAREd-----Yes---'
```

## Parameter

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das aktualisiert werden soll.

SHAREd

Gibt an, dass dieses Speicherarchiv mit anderen Servern in einem Speicherbereichsnetz (SAN) gemeinsam genutzt wird. Dieser Befehl muss von dem Server ausgegeben werden, der als primärer Speicherarchivmanager für das gemeinsam genutzte Speicherarchiv definiert ist. Dieser Parameter ist für Speicherarchive erforderlich, die für einen Speicherarchivmanager definiert sind, und ist für Speicherarchive erforderlich, die für NDMP-Operationen verwendet werden. Geben Sie SHARED=YES an, um ein Speicherarchiv zu aktualisieren, das gegenwärtig nicht gemeinsam genutzt wird.

Wichtig: Hat ein Speicherarchiv einen Pfad von einer Einheit zum Versetzen von Daten (beispielsweise einem NAS-Dateiserver), aber keine Verbindung zu dem Server, kann das Speicherarchiv nicht mit einem anderen Server gemeinsam genutzt werden.

## Beispiel: Ein Kassettenarchiv FILE aktualisieren, das gemeinsam genutzt werden soll

---

Ein Kassettenarchiv FILE mit dem Namen FILE2 aktualisieren, damit es gemeinsam genutzt wird.

```
update library file2 shared=yes
```

## UPDATE LIBRARY (Manuelles Kassettenarchiv aktualisieren)

---

Verwenden Sie diese Syntax, um ein manuelles Kassettenarchiv zu aktualisieren.

### Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

---

```
>>-UPDate LIBRARY--Speicherarchivname----->
>+-----+-----+-----+-----+-----+
'-RESETDrives-----+-Yes-+-'
      '-No--'
>+-----+-----+-----+-----+-----+<
'-AUTOLabel--==--+-No-----+-'
      +-Yes-----+
      '-OVERWRITE-'
```

### Parameter

---

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das aktualisiert werden soll.

RESETDrives

Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird.

Wird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

Wird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

Yes

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird.

No

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.

Yes

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird.

No

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

#### AUTOLabel

Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

#### No

Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

#### Yes

Gibt an, dass der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

#### OVERWRITE

Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

## UPDATE LIBRARY (SCSI-Kassettenarchiv aktualisieren)

---

Verwenden Sie diese Syntax, um ein SCSI-Kassettenarchiv zu aktualisieren.

### Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

---

```
>>-UPDate LIBRary--Speicherarchivname----->
>---LIBType---+---+SCSI+---+-----+----->
           '-VTL--'      '-SHAREd-----Yes--'
>---+-----+-----+----->
           '-RESETDrives-----+Yes-+-'
           '-No--'
>---+-----+-----+----->
           '-AUTOLabel-----+No-----+-'
           '+-Yes-----+
           '-OVERWRITE-'
>---+-----+-----+----->
           '-RELABELSCRatch-----+No---+-'
           '-Yes-'
>---+-----+-----+-----><
           '-SERial---+---+Seriennummer+---'
           '-AUTODetect---
```

### Parameter

---

#### Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das aktualisiert werden soll.

#### LIBType (Erforderlich)

Gibt den Kassettenarchivtyp an, der aktualisiert werden soll. Gültige Werte:

#### VTL

Gibt an, dass das Speicherarchiv über einen SCSI-gesteuerten Datenträgerwechsler verfügt, der durch ein virtuelles Bandarchiv (Virtual Tape Library - VTL) dargestellt wird. Zum Bereitstellen von Datenträgern in Laufwerken bei diesem Typ von Speicherarchiv verwendet IBM Spectrum Protect die Datenträgerwechslereinheit. Dieser Wert ist wirksam, wenn er für Speicherarchive mit dem aktuellen Speicherarchivtyp SCSI angegeben wird.

Anmerkung: Die Auswahl des Kassettenarchivtyps VTL setzt voraus, dass die folgenden Bedingungen zutreffen:

- Ihre Umgebung enthält keine gemischten Datenträger.
- Pfade sind zwischen allen Laufwerken in dem Kassettenarchiv und allen definierten Servern, einschließlich Speicheragenten, die das Kassettenarchiv verwenden, definiert

Wenn beide Bedingungen nicht zutreffen, kann die Leistung in demselben Maße wie beim Speicherarchivtyp SCSI abnehmen. Dies ist besonders in Zeiten hoher Belastung der Fall, wenn die meisten Laufwerke gleichzeitig verwendet werden.

#### SCSI

Gibt an, dass das Speicherarchiv über einen SCSI-gesteuerten Datenträgerwechsler verfügt. Zum Bereitstellen von Datenträgern in Laufwerken bei diesem Typ von Speicherarchiv verwendet IBM Spectrum Protect die Datenträgerwechslereinheit. Dieser Wert ist wirksam, wenn er für Speicherarchive mit dem aktuellen Speicherarchivtyp VTL angegeben wird.


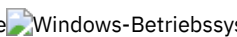
#### SHAREd


Gibt an, dass dieses Speicherarchiv mit anderen Servern in einem Speicherbereichsnetz (SAN) gemeinsam genutzt wird. Dieser Befehl muss von dem Server ausgegeben werden, der als primärer Speicherarchivmanager für das gemeinsam genutzte Speicherarchiv definiert ist. Dieser Parameter ist für Speicherarchive erforderlich, die für einen Speicherarchivmanager definiert sind, und ist für Speicherarchive erforderlich, die für NDMP-Operationen verwendet werden. Geben Sie SHARED=YES an, um ein Speicherarchiv zu aktualisieren, das gegenwärtig nicht gemeinsam genutzt wird.

Wichtig: Hat ein Speicherarchiv einen Pfad von einer Einheit zum Versetzen von Daten (beispielsweise einem NAS-Dateiserver), aber keine Verbindung zu dem Server, kann das Speicherarchiv nicht mit einem anderen Server gemeinsam genutzt werden.

#### RESETDrives

Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird.

  Wird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

 Wird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

In der folgenden Tabelle sind die drei möglichen Konfigurationen für Laufwerke beschrieben, die an NAS-Einheiten angeschlossen werden können.

Tabelle 1. Konfigurationen für Laufwerke, die an NAS-Einheiten angeschlossen sind

| Konfiguration der Speicherarchivereinheit   | Verhalten für persistente Reserve  |
|---|--|
| Die Speicherarchivereinheit wird an den IBM Spectrum Protect-Server angeschlossen, und die Bandlaufwerke werden vom Server und der NAS-Einheit gemeinsam genutzt.   | Die Zurückstellung der Laufwerkreservierung wird unterstützt, wenn die NAS-Einheit die persistente Reserve unterstützt und diese aktiviert ist. Weitere Informationen zum Definieren der persistenten Reserve finden Sie in der Dokumentation für Ihre NAS-Einheit.  |
| Die Speicherarchivereinheit wird an den IBM Spectrum Protect-Server angeschlossen, und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen.  | Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben. |
| Die Speicherarchivereinheit wird an die NAS-Einheit angeschlossen und der Zugriff erfolgt indirekt durch NDMP (Network Data Management Protocol), und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen. | Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben. |

#### Yes

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird.

#### No

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.



Yes

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird.

No

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

AUTOLabel

Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

No

Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes

Gibt an, daß der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE

Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

SERIAL

Gibt die Seriennummer des Speicherarchivs an, das aktualisiert wird. Dieser Parameter ist wahlfrei. Gültige Werte sind:

Seriennummer

Gibt die Seriennummer des Speicherarchivs an, das aktualisiert wird.

Wurde bereits ein Pfad zu diesem Speicherarchiv definiert, wird die eingegebene Nummer mit der Nummer verglichen, die von IBM Spectrum Protect erkannt wurde. Stimmen die Nummern nicht überein, schlägt der Befehl fehl. Wurde kein Pfad definiert, wird diese Seriennummer beim Definieren eines Pfads geprüft.

AUTODetect

Gibt an, dass die Seriennummer automatisch von IBM Spectrum Protect erkannt und verwendet wird, wenn bereits ein Pfad zu diesem Speicherarchiv definiert wurde.

Wurde kein Pfad zu diesem Kassettenarchiv definiert, wird die Seriennummer nicht erkannt.

RELABELSCRatch

Gibt an, ob der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht wurden und wieder als Arbeitsdatenträger verwendet werden. Wird dieser Parameter auf YES gesetzt, wird eine Operation LABEL LIBVOLUME gestartet und der vorhandene Datenträgerkennsatz wird überschrieben. Dieser Parameter ist optional und für die Verwendung mit einem VTL-Speicherarchiv (VTL = Virtual Tape Library) bestimmt.

Anmerkung: Haben Sie sowohl virtuelle als auch reale Datenträger in Ihrem VTL, werden beide Typen mit einem neuen Kennsatz versehen, wenn dieser Parameter aktiviert ist. Enthält das VTL reale Datenträger, kann die Angabe dieser Option Auswirkungen auf die Leistung haben.

No

Gibt an, dass der Server Datenträger nicht mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden.

Yes

Gibt an, dass der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden.

## UPDATE LIBRARY (Gemeinsam genutztes Kassettenarchiv aktualisieren)

---

Verwenden Sie diese Syntax, um ein gemeinsam genutztes Kassettenarchiv zu aktualisieren.

### Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

---

```
>>-UPDate LIBRARY--Speicherarchivname----->
```

```
>--PRIMarylibmanager-----Servername-----><
```

## Parameter

---

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

PRIMarylibmanager

Gibt den Namen des Servers an, der für die Steuerung des Zugriffs auf Kassettenarchivressourcen zuständig ist. Sie müssen diesen Server mit dem Befehl DEFINE SERVER definieren, bevor Sie ihn als Kassettenarchivmanager verwenden können.

## Beispiel: Den Kassettenarchivmanagerserver für ein Kassettenarchiv ändern

---

Für einen Kassettenarchivclientserver den Namen des Kassettenarchivmanagerservers in CASTOR ändern.

```
update library ltolib primarylibmanager=castor
```

## UPDATE LIBRARY (VTL-Speicherarchiv aktualisieren)

---

Verwenden Sie diese Syntax, um ein Speicherarchiv zu aktualisieren, das als VTL definiert ist.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

---

```
>>-UPDate LIBRary--Speicherarchivname----->
>---LIBType---+VTL--+-----+-----+----->
          '-SCSI-'      '-SHARed-----Yes---'
>--+-----+-----+----->
          '-RESETDrives-----+Yes-+-'
          '-No--'
>--+-----+-----+----->
          '-AUTOLabel-----+No-----+-'
          '+-Yes-----+
          '-OVERWRITE-'
>--+-----+-----+----->
          '-RELABELSCRatch-----+No--+-'
          '-Yes-'
>--+-----+-----+-----><
          '-SERial-----+Seriennummer-+-'
          '-AUTODetect---
```

## Parameter

---

Speicherarchivname (Erforderlich)

Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType (Erforderlich)

Gibt den Typ des Speicherarchivs an, das definiert wird. Gültige Werte:

SCSI

Gibt an, dass das Speicherarchiv über einen SCSI-gesteuerten Datenträgerwechsler verfügt. Zum Bereitstellen von Datenträgern in Laufwerken bei diesem Typ von Speicherarchiv verwendet IBM Spectrum Protect die Datenträgerwechslereinheit. Dieser Wert ist wirksam, wenn er für Speicherarchive mit dem aktuellen Speicherarchivtyp VTL angegeben wird.

VTL

Gibt an, dass das Speicherarchiv über einen SCSI-gesteuerten Datenträgerwechsler verfügt, der durch ein virtuelles Bandarchiv (Virtual Tape Library - VTL) dargestellt wird. Zum Bereitstellen von Datenträgern in Laufwerken bei diesem Typ von Speicherarchiv verwendet IBM Spectrum Protect die Datenträgerwechslereinheit. Dieser Wert ist wirksam, wenn er für Speicherarchive mit dem aktuellen Speicherarchivtyp SCSI angegeben wird.

Anmerkung: Wählen Sie den Speicherarchivtyp VTL nur aus, wenn die folgenden Bedingungen zutreffen:

- Ihre Umgebung enthält keine gemischten Datenträger.
- Pfade sind zwischen allen Laufwerken in dem Speicherarchiv und allen definierten Servern, einschließlich Speicheragenten, die das Speicherarchiv verwenden, definiert.

Wenn beide Bedingungen nicht zutreffen, kann die Leistung in demselben Maße wie beim Speicherarchivtyp SCSI abnehmen. Dies ist besonders in Zeiten hoher Belastung der Fall, wenn die meisten Laufwerke gleichzeitig verwendet werden.



#### SHAREd


Gibt an, dass dieses Speicherarchiv mit anderen Servern in einem Speicherbereichsnetz (SAN) gemeinsam genutzt wird. Dieser Befehl muss von dem Server ausgegeben werden, der als primärer Speicherarchivmanager für das gemeinsam genutzte Speicherarchiv definiert ist. Dieser Parameter ist für Speicherarchive erforderlich, die für einen Speicherarchivmanager definiert sind, und ist für Speicherarchive erforderlich, die für NDMP-Operationen verwendet werden. Geben Sie SHARED=YES an, um ein Speicherarchiv zu aktualisieren, das gegenwärtig nicht gemeinsam genutzt wird.

Wichtig: Hat ein Speicherarchiv einen Pfad von einer Einheit zum Versetzen von Daten (beispielsweise einem NAS-Dateiserver), aber keine Verbindung zu dem Server, kann das Speicherarchiv nicht mit einem anderen Server gemeinsam genutzt werden.

#### RESETDrives

Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird.

  Wird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

 Wird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

Yes

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird.

No

Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.



Yes

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird.

No

Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

#### AUTOlabel

Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

No

Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes

Gibt an, daß der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

#### OVERWRITE

Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

## RELABELSCRatch

Gibt an, ob der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht wurden und wieder als Arbeitsdatenträger verwendet werden. Wird dieser Parameter auf YES gesetzt, wird eine Operation LABEL LIBVOLUME gestartet und der vorhandene Datenträgerkennsatz wird überschrieben.

Anmerkung: Haben Sie sowohl virtuelle als auch reale Datenträger in Ihrem VTL, werden beide Typen mit einem neuen Kennsatz versehen, wenn dieser Parameter aktiviert ist. Enthält das VTL reale Datenträger, kann die Angabe dieser Option Auswirkungen auf die Leistung haben.

### Yes

Gibt an, dass der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden.

### No

Gibt an, dass der Server Datenträger nicht mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden.

## SERial

Gibt die Seriennummer des Speicherarchivs an, das aktualisiert wird. Dieser Parameter ist wahlfrei. Gültige Werte sind:

### Seriennummer

Gibt die Seriennummer des Speicherarchivs an, das aktualisiert wird.

Wurde bereits ein Pfad zu diesem Speicherarchiv definiert, wird die eingegebene Nummer mit der Nummer verglichen, die von IBM Spectrum Protect erkannt wurde. Stimmen die Nummern nicht überein, schlägt der Befehl fehl. Wurde kein Pfad definiert, wird diese Seriennummer beim Definieren eines Pfads geprüft.

### AUTODetect

Gibt an, dass die Seriennummer automatisch von IBM Spectrum Protect erkannt und verwendet wird, wenn bereits ein Pfad zu diesem Speicherarchiv definiert wurde.

Wurde kein Pfad zu diesem Speicherarchiv definiert, wird die Seriennummer nicht erkannt.

## UPDATE LIBVOLUME (Status eines Speicherdatenträgers ändern)

---

Mit diesem Befehl kann der Status eines Speicherdatenträgers mit sequenziellem Zugriff in einem Speicherarchiv geändert werden.

### Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

---

```
>>-UPDate LIBVolume--Speicherarchivname--Datenträgername--STATus-----+PRIVate-+++>
                                     '-SCRatch-'
>--+-----+-----><
   '-OWNer-----Servername-'
```

### Parameter

---

#### Speicherarchivname (Erforderlich)

Gibt den Namen des Speicherarchivs an.

#### Datenträgername (Erforderlich)

Gibt den Namen des Speicherdatenträgers an.

#### STATus (Erforderlich)

Gibt eine Änderung im Status eines Speicherdatenträgers an. Gültige Werte sind:

#### PRIVate

Gibt an, dass der Server den Speicherdatenträger in einen privaten Datenträger ändert.

#### SCRatch

Gibt an, dass der Server den Speicherdatenträger in einen Arbeitsdatenträger ändert.

Einschränkung: Sie können nicht den Status eines Datenträgers von 'privat' in 'Arbeitsdatenträger' ändern, wenn der Datenträger zu einem Speicherpool gehört oder in der Protokolldatei für Datenträger definiert ist. Sie können den Status ändern, wenn beim Zurückstellen von Datenträgern in das Speicherarchiv ein Fehler unterlaufen ist und den Datenträgern der falsche Status zugeordnet wurde.



Gibt an, welcher Server der Eigner eines privaten Datenträgers in einem Kassettenarchiv ist, das in einem SAN gemeinsam benutzt wird. Der Eigner eines privaten Datenträgers in einem gemeinsam benutzten Kassettenarchiv (SAN) kann geändert werden, wenn der Befehl von dem Kassettenarchivmanager-Server ausgegeben wird. Wird dieser Parameter nicht angegeben, ist der Kassettenarchivmanager-Server der Eigner des privaten Datenträgers.

Wichtig: Verwenden Sie nicht OWNER als Wert für Arbeitsdatenträger. Sie können OWNER jedoch verwenden, wenn Sie einen Arbeitsdatenträger in einen privaten Datenträger ändern.

## Beispiel: Den Status eines Datenträgers aktualisieren

Für den Datenträger WPDV00 im Speicherarchiv AUTO soll der Status PRIVATE vergeben werden.

```
update libvolume auto wpdv00 status=private
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE LIBVOLUME

| Befehl             | Beschreibung   |
|--------------------|--|
| AUDIT LIBRARY      | Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet.            |
| CHECKIN LIBVOLUME  | Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.                                       |
| CHECKOUT LIBVOLUME | Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.                                     |
| DEFINE VOLUME      | Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll. |
| LABEL LIBVOLUME    | Kennzeichnet Datenträger in manuellen oder automatisierten Kassettenarchiven.                                  |
| QUERY LIBRARY      | Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.  |
| QUERY LIBVOLUME    | Zeigt Informationen zu einem Datenträger im Kassettenarchiv an.  |

## UPDATE MACHINE (Maschineninformationen aktualisieren)

Mit diesem Befehl können Maschinendaten aktualisiert werden. Diese Informationen werden in der Wiederherstellungsplandatei berücksichtigt, um den Benutzer bei der Wiederherstellung der Client-Maschinen zu unterstützen.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-UPDate MACHine--Maschinenname----->
>-+-----+-----+-----+----->
  '-DEScRiption----Beschreibung-' '-BUildung----Gebäude-'
>-+-----+-----+-----+----->
  '-FLoor----Stockwerk-' '-ROom----Raum-'
>-+-----+-----+-----+----->
  '-PRIOriTy----Zahl-' '-ADSMServer----+Yes+-'
                                     '-No--'
```

## Parameter

Maschinenname (Erforderlich)

Gibt den Namen der Maschine an, die aktualisiert werden soll.

**DEScRiption**

Gibt eine Beschreibung der Maschine an. Dieser Parameter ist wahlfrei. Der Text kann bis zu 255 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält. Soll vorhandener Text entfernt werden, geben Sie eine Nullzeichenfolge ("" ) an.

**BUilding**

Gibt den Namen oder die Nummer des Gebäudes an, in dem sich diese Maschine befindet. Dieser Parameter ist wahlfrei. Der Text kann bis zu 16 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält. Soll vorhandener Text entfernt werden, geben Sie eine Nullzeichenfolge ("" ) an.

**FLoor**

Gibt den Namen oder die Nummer des Stockwerks an, auf dem sich diese Maschine befindet. Dieser Parameter ist wahlfrei. Der Text kann bis zu 16 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält. Soll vorhandener Text entfernt werden, geben Sie eine Nullzeichenfolge ("" ) an.

**ROom**

Gibt den Namen oder die Nummer des Raums an, in dem sich diese Maschine befindet. Dieser Parameter ist wahlfrei. Der Text kann bis zu 16 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält. Soll vorhandener Text entfernt werden, geben Sie eine Nullzeichenfolge ("" ) an.

**PRIOrity**

Gibt die Zurückschreibungspriorität für die Maschine als ganze Zahl von 1 bis 99 an. Die höchste Priorität ist 1. Dieser Parameter ist wahlfrei. Verwenden Sie diesen Wert für die Vergabe von Prioritäten bei der Wiederherstellung von Clientmaschinen.

**ADSMSeRver**

Gibt an, ob die Maschine einen IBM Spectrum Protect-Server enthält. Dieser Parameter ist wahlfrei. Gültige Werte:

No

Diese Maschine enthält keinen IBM Spectrum Protect-Server.

Yes

Diese Maschine enthält einen IBM Spectrum Protect-Server. Es kann nur eine Maschine definiert werden, die einen IBM Spectrum Protect-Server enthält.

## Beispiel: Informationen zu einer bestimmten Maschine aktualisieren

In die Maschineninformationen von DISTRICT5 soll ein Eintrag aufgenommen werden, der besagt, dass die Maschine den Server enthält.

```
update machine district5 adsmserver=yes
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE MACHINE

| Befehl         | Beschreibung  |
|----------------|---|
| DEFINE MACHINE | Definiert eine Maschine für DRM.  |
| DELETE MACHINE | Löscht eine Maschine.   |
| INSERT MACHINE | Fügt Maschinenkenndaten oder Wiederherstellungsanweisungen in die IBM Spectrum Protect-Datenbank ein. |
| QUERY MACHINE  | Zeigt Informationen über Maschinen an.  |

## UPDATE MGMTCLASS (Verwaltungsklasse aktualisieren)

Mit diesem Befehl kann eine Verwaltungsklasse geändert werden. Um Clients die Verwendung der aktualisierten Verwaltungsklasse zu ermöglichen, muß die Maßnahmengruppe aktiviert werden, die die Verwaltungsklasse enthält.

Wichtig: Der Befehl UPDATE MGMTCLASS schlägt fehl, wenn ein Kopierspeicherpool als Zielort für Dateien angegeben wird, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Maßnahmengruppe gehört.

## Syntax

```
>>-UPDate MGMTclass----->
```



Beschreibung der Verwaltungsklasse. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Soll eine zuvor definierte Beschreibung gelöscht werden, ist eine Nullzeichenfolge ("" ) anzugeben.

## Beispiel: Die Maßnahmendomäne und den Speicherpool einer bestimmten Verwaltungsklasse aktualisieren

Für die Verwaltungsklasse ACTIVEFILES in Maßnahmengruppe VACATION in der Maßnahmendomäne EMPLOYEE\_RECORDS den Speicherpool ändern, in dem umgelagerte Dateien gespeichert werden.

```
update mgmtclass employee_records vacation
activefiles migdestination=diskpool2
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE MGMTCLASS

| Befehl              | Beschreibung  |
|---------------------|---|
| ASSIGN DEFMGMTCLASS | Ordnet eine Verwaltungsklasse als Standardklasse für eine angegebene Maßnahmengruppe zu.                                      |
| COPY MGMTCLASS      | Erstellt eine Kopie einer Verwaltungsklasse.  |
| DEFINE COPYGROUP    | Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse. |
| DEFINE MGMTCLASS    | Definiert eine Verwaltungsklasse.   |
| DEFINE POLICYSET    | Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.   |
| DELETE MGMTCLASS    | Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe.                     |
| QUERY COPYGROUP     | Zeigt die Attribute einer Kopiengruppe an.  |
| QUERY MGMTCLASS     | Zeigt Informationen zu Verwaltungsklassen an.   |
| QUERY POLICYSET     | Zeigt Informationen über Maßnahmengruppen an.   |
| UPDATE COPYGROUP    | Ändert ein oder mehrere Attribute einer Kopiengruppe.   |

## UPDATE NODE (Attribute eines Knotens aktualisieren)

Verwenden Sie diesen Befehl, um die Attribute eines registrierten Knotens zu ändern.

Sie müssen den Befehl RENAME NODE verwenden, um den Namen eines registrierten Knotens zu ändern.

Wenn Sie die Knotenauthentifizierungsmethode oder die Einstellung für SSLREQUIRED des Knotens aktualisieren und ein Administrator mit demselben Namen vorhanden ist, ändern sich diese Einstellungen für die Administrator-ID.

Sie müssen über die Berechtigung auf Systemebene verfügen, um die Knotenauthentifizierungsmethode oder die Einstellung für SSLREQUIRED des Knotens und eine Administrator-ID mit demselben Namen zu aktualisieren. Wenn die Administrator-ID mit demselben Namen die Clienteignerberechtigung über den Knoten hat, der aktualisiert wird, ist die Berechtigung auf Systemebene nicht erforderlich. Sie müssen über uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne verfügen, zu der der Clientknoten gehört.

Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol):

- Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.
- Wenn Sie den Authentifizierungsmodus in LDAP ändern und der Knotenname mit einer Benutzer-ID mit Administratorberechtigung übereinstimmt, stellen Sie möglicherweise ein nicht erwartetes Verhalten fest, wenn eine automatische Kennwortänderung stattfindet, weil das Kennwort unter Umständen zweimal aktualisiert wird. Dies hat zur Folge, dass das Kennwort für die Benutzer-ID mit Administratorberechtigung unbekannt ist. Es kann aber auch vorkommen, dass die Kennwortaktualisierungsoperation fehlschlägt.

Wenn Sie einen Knoten registrieren oder aktualisieren, können Sie angeben, ob beschädigte Dateien auf dem Knoten von einem Zielreplikationsserver wiederhergestellt werden können. Dateien können nur wiederhergestellt werden, wenn alle folgenden Bedingungen erfüllt sind:

- Version 7.1.1 oder höher ist auf dem Quellen- und Zielreplikationsserver installiert.
- Der Systemparameter REPLRECOVERDAMAGED ist auf ON gesetzt. Der Systemparameter kann mit dem Befehl SET REPLRECOVERDAMAGED definiert werden.
- Der Quellenserver schließt mindestens eine Datei ein, die auf dem Knoten, der repliziert wird, als beschädigt markiert ist.
- Die Knotendaten wurden repliziert, bevor die Beschädigung aufgetreten ist.

In der folgenden Tabelle wird beschrieben, wie sich Parametereinstellungen auf die Wiederherstellung beschädigter, replizierter Dateien auswirken.

Tabelle 1. Einstellungen, die sich auf die Wiederherstellung beschädigter Dateien auswirken

| Einstellung für den Systemparameter REPLRECOVERDAMAGED | Wert des Parameters RECOVERDAMAGED im Befehl REPLICATE NODE | Wert des Parameters RECOVERDAMAGED in den Befehlen REGISTER NODE und UPDATE NODE | Ergebnis  |
|--|---|--|---|
| OFF  | YES, NO oder nicht angegeben                                | YES oder NO  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.    |
| OFF  | ONLY  | YES oder NO  | Eine Fehlernachricht wird angezeigt, weil Dateien nicht wiederhergestellt werden können, wenn der Systemparameter REPLRECOVERDAMAGED auf OFF gesetzt ist. |
| ON   | YES   | YES oder NO  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.          |
| ON   | NO  | YES oder NO  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.    |
| ON   | ONLY  | YES oder NO  | Beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt, aber es findet keine Standardknotenreplikation statt.                            |
| ON   | Nicht angegeben   | YES  | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.          |
| ON   | Nicht angegeben   | NO   | Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.    |

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der der Clientknoten gehört.

## Syntax

```

(1)
>>-UPDate Node-----Knotenname----->
>-----+-----+----->
| (2) |
+-----Kennwort-----+-----+-----+
|          '-FORCEPwreset-----+No--+-' |
|          '-Yes-' |
| '-FORCEPwreset-----Yes-----' |
>-----+-----+----->
'-PASSExp----Tage-' '-CLOptset----Optionsgruppenname-'

```

```

>----->
'-CONTACT---Text-' '-DOMAIN---Domänenname-'

>----->
'-COMpression---Client+' '-ARCHDElete---Yes+'
  +-Yes---+                '-No--'
  '-No-----'

>----->
'-BACKDElete---No--+'
  '-Yes-'

>----->
'-WHEREDomain---Domänenname-'

>----->
'-WHEREPlatform---Name_der_Clientplattform-'

>----->
'-MAXNUMMP---Anzahl-' '-KEEPMP---No--+'
  '-Yes-'

>----->
'-URL---URL-Adresse-'

>----->
'-UTILITYUrl---Dienstprogramm-URL-'

(3)
>----->
'-AUTOFSRename---Yes---+'
  +-No-----+
  '-Client-'

>----->
'-VALIDateprotocol---No-----+'
  +-Dataonly-+
  '-All-----'

>----->
'-TXNGroupmax---0-----+'
  '-Anzahl-'

.-DATAWritepath---ANY-----
>----->
'-DATAWritepath---ANY---+'
  +-LAN-----+
  '-LANFree-'

.-DATAReadpath---ANY-----
>----->
'-DATAReadpath---ANY---+'
  +-LAN-----+
  '-LANFree-'

>----->
'-TARGETLevel---V.R.M.F-'

.-SESSIONINITiation---Clientorserver-----
>----->
'-SESSIONINITiation---Clientorserver-----'
  |
  '-SERVEROnly--HLAddress---IP-Adresse--LLAddress---TCP-Anschluss-----' (4) |

>----->
'-HLAddress---IP-Adresse-'

>----->
| (4) |
'-LLAddress---TCP-Anschluss-----'

>----->
'-EMAILAddress---Benutzer-ID@Knoten-'

>----->
'-DEDUPlication---SERVEROnly---+'
  '-Clientorserver-'

```



6. Wenn Sie den Parameter REPLSTATE angeben und den Parameter REPLMODE nicht angeben, wird der Replikationsmodus des Knotens auf SEND gesetzt.
7. Wenn Sie den Parameter REPLMODE angeben, müssen Sie auch den Parameter REPLSTATE angeben.
8. Der Parameter SYNCLDAPDELETE gilt nur, wenn ein Knoten, der sich mit einem Lightweight Directory Access Protocol-Server (LDAP-Server) authentifiziert, zur lokalen Authentifizierung zurückkehrt.
9. Der Parameter SSLREQUIRED ist veraltet.

## Parameter

---

### Knotenname (Erforderlich)

Gibt den Namen des Clientknotens an, der aktualisiert werden soll. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden.

Einschränkung: Wenn ein Kennwort mit dem Befehl UPDATE NODE aktualisiert wird, können Sie kein Platzhalterzeichen beim Parameter `Knotenname` verwenden.

### Kennwort

Gibt das neue Kennwort für den Clientknoten an. Dieser Parameter ist in den meisten Fällen optional. Wenn die Authentifizierungsmethode des Knotens von LDAP in LOCAL geändert wird, ist ein Kennwort erforderlich. Wenn LDAP als Knotenauthentifizierungsmethode verwendet wird, geben Sie bei Verwendung des Befehls UPDATE NODE kein Kennwort an. Das Kennwort darf maximal 64 Zeichen lang sein. Die Gültigkeitsdauer von Kennwörtern richtet sich nach der Kennwortablaufdauer.

### FORCEPwreset

Gibt an, ob ein Client zum Ändern oder Zurücksetzen des Kennworts gezwungen werden soll. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

#### No

Gibt an, dass die Kennwortablaufdauer über den Befehl SET PASSEXP definiert wird. Einen Client nicht zwingen, das Kennwort zu ändern oder zurückzusetzen, während er versucht, sich beim Server anzumelden.

#### Yes

Gibt an, dass das Kennwort des Clientknotens oder des Administrators bei der nächsten Anmeldung abläuft. Der Client muss das Kennwort bei der nächsten Anmeldung ändern oder zurücksetzen.

Einschränkungen:

- Für Knoten, die mit einem LDAP-Server authentifiziert werden, wird der Kennwortablauf mithilfe von LDAP-Serverdienstprogrammen definiert. Geben Sie daher nicht FORCEPWRESET=YES an, wenn AUTHENTICATION=LDAP angegeben werden soll.
- Soll ein Knoten für die Authentifizierung mit einem LDAP-Server aktualisiert werden, und haben Sie FORCEPWRESET=YES angegeben, müssen Sie das Kennwort ändern, bevor Sie FORCEPWRESET=NO und AUTHENTICATION=LDAP angeben können.

### PASSExp

Gibt die Anzahl der Tage an, die das Kennwort gültig ist. Für die Kennwortablaufdauer kann ein Wert von 0 bis 9999 Tage definiert werden. Der Wert 0 bedeutet, dass das Kennwort niemals abläuft. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, wird die Kennwortablaufdauer nicht geändert.

Sie können die Kennwortablaufdauer mit dem Befehl UPDATE NODE oder SET PASSEXP ändern. Um eine allgemeine Ablaufdauer für alle Administratoren und Clientknoten zu definieren, geben Sie den Befehl SET PASSEXP aus. Sie können den Befehl SET PASSEXP auch verwenden, um die Kennwortablaufdauer selektiv festzulegen. Wenn Sie eine Kennwortablaufdauer selektiv mit dem Befehl REGISTER NODE, UPDATE NODE oder SET PASSEXP festlegen, wird die Ablaufdauer von der jeweiligen allgemeinen Kennwortablaufdauer ausgeschlossen, die mit dem Befehl SET PASSEXP erstellt wurde.

Sie können den Befehl RESET PASSEXP verwenden, um die Kennwortablaufdauer auf die allgemeine Kennwortablaufdauer zurückzusetzen. Dieser Parameter gilt nicht für Kennwörter, die sich mit einem LDAP-Verzeichnisserver authentifizieren.

### CLOptset

Gibt den Namen der Optionsgruppe an, die der Client verwenden soll. Dieser Parameter ist wahlfrei. Um eine Clientoptionsgruppe zu entfernen, geben Sie den Parameter CLOPTSET mit einer Nullzeichenfolge ("" ) an.

### CONTACT

Gibt eine Informationszeichenfolge an, die den Clientknoten identifiziert. Dieser Parameter ist wahlfrei. Die maximale Länge der Zeichenfolge beträgt 255 Zeichen. Die Kontaktinformationen in Anführungszeichen einschließen, wenn sie Leerzeichen enthalten. Sollen zuvor definierte Kontaktinformationen entfernt werden, geben Sie eine Nullzeichenfolge ("" ) an.

### DOMAIN

Gibt den Namen der Maßnahmendomäne an, für die der Clientknoten registriert werden soll. Dieser Parameter ist wahlfrei.

Einschränkung: Für Server mit aktiviertem Aufbewahrungsschutz für Daten kann ein archivierter registrierter Knoten nicht erneut einer anderen Maßnahmendomäne zugeordnet werden.

### COMPRESSION



Gibt an, ob der Clientknoten seine Dateien komprimiert, bevor sie zum Sichern und Archivieren an den Server gesendet werden. Dieser Parameter ist wahlfrei.

Einschränkung: Dieser Parameter kann nicht für einen NAS-Knoten angegeben werden.

Sie können einen der folgenden Werte angeben:

Client

Gibt an, dass der Client festlegt, ob Dateien komprimiert werden sollen.

Yes

Gibt an, dass der Clientknoten seine Dateien komprimiert, bevor sie zum Sichern und Archivieren an den Server gesendet werden.

No

Gibt an, dass der Clientknoten seine Dateien nicht komprimiert, bevor sie zum Sichern und Archivieren an den Server gesendet werden.

ARCHDElete

Gibt an, ob der Clientknoten seine eigenen Archivierungsdateien aus dem Server löschen darf. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

Yes

Gibt an, dass der Clientknoten seine eigenen Archivierungsdateien aus dem Server löschen darf.

No

Gibt an, dass der Clientknoten seine eigenen Archivierungsdateien nicht aus dem Server löschen darf.

BACKDElete

Gibt an, ob der Clientknoten seine eigenen Sicherungsdateien aus dem Server löschen darf. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass der Clientknoten seine eigenen Sicherungsdateien nicht aus dem Server löschen darf.

Yes

Gibt an, dass der Clientknoten seine eigenen Sicherungsdateien aus dem Server löschen darf.

WHEREDomain

Gibt den Namen der Maßnahmendomäne an, die in Kombination mit dem Knotennamen als Filter verwendet werden soll, um zu aktualisierende Knoten auszuwählen. Dieser Parameter ist wahlfrei.

WHEREPlatform

Gibt den Namen der Clientplattform an, die in Kombination mit dem Knotennamen als Filter verwendet werden soll, um zu aktualisierende Knoten auszuwählen. Dieser Parameter ist wahlfrei.

MAXNUMMP

Gibt die maximale Anzahl der Mountpunkte an, die ein Knoten nur für Operationen, wie beispielsweise Sicherung, Archivierung und IBM Spectrum Protect for Space Management-Umlagerung, auf dem Server oder dem Speicheragenten verwenden kann. Der Parameter ist optional und gilt nicht für Knoten mit dem Typ NAS oder SERVER. Der Standardwert ist 1. Sie können eine ganze Zahl im Bereich von 0 bis 999 angeben. Der Wert 0 gibt an, dass ein Knoten keinen Mountpunkt für eine Operation zum Speichern von Clientdaten anfordern kann. Der Wert für MAXNUMMP wird während der Operationen zum Lesen von Clientdaten, wie beispielsweise Zurückschreiben, Abrufen und Zurückrufen durch IBM Spectrum Protect for Space Management, nicht ausgewertet oder umgesetzt. Mountpunkte, die für Operationen zum Lesen von Daten verwendet werden, werden jedoch in Bezug auf versuchte gleichzeitig ablaufende Datenspeicherungsoperationen für denselben Clientknoten ausgewertet und können verhindern, dass die Datenspeicherungsoperationen Mountpunkte anfordern können.

Für Datenträger in einem Speicherpool, dem der Einheitentyp FILE oder CENTERA zugeordnet ist, kann der Server über mehrere Sitzungen verfügen, um gleichzeitig denselben Datenträger zu lesen, und über eine Sitzung verfügen, um auf diesen Datenträger zu schreiben. Um den gemeinsamen Zugriff zu erweitern und einen effizienten Zugriff für Knoten mit Daten in Speicherpools des Typs FILE oder CENTERA zur Verfügung zu stellen, erhöhen Sie den Wert des Parameters MAXNUMMP.

Für Knoten, die mit aktivierter Funktion für simultanes Schreiben Daten in primären Speicherpools speichern, müssen Sie den Wert des Parameters MAXNUMMP anpassen, um die korrekte Anzahl der Mountpunkte für jede Clientsitzung anzugeben. Eine Clientsitzung erfordert einen Mountpunkt für den primären Speicherpool und einen Mountpunkt für jeden Kopierspeicherpool und jeden Pool für aktive Daten.

URL

Gibt die URL des IBM Spectrum Protect-Web-Clients an, die auf dem Clientsystem konfiguriert ist. Sie können die URL in einem Web-Browser und im Operations Center verwenden, um den Clientknoten über Fernzugriff zu verwalten.

Dieser Parameter ist wahlfrei. Die URL muss den DNS-Namen oder die IP-Adresse des Clientsystems und die Anschlussnummer enthalten, die auf dem Clientsystem für den IBM Spectrum Protect-Web-Client definiert ist. Beispiel:

`http://client.mycorp.com:1581`

Soll der Wert für diesen Parameter entfernt werden, geben Sie leere einfache Anführungszeichen oder leere Anführungszeichen ohne Leerzeichen an (' für einfache Anführungszeichen oder "" für Anführungszeichen).

#### UTILITYUrl

Gibt die Adresse der IBM Spectrum Protect-Clientverwaltungsservices an, die auf dem Clientsystem konfiguriert sind. Diese URL wird vom Operations Center verwendet, um auf Clientprotokolldateien zuzugreifen, sodass Sie im Operations Center Clientprobleme über Fernzugriff diagnostizieren können.

Dieser Parameter ist wahlfrei. Sie können eine URL mit maximal 200 Zeichen angeben. Die URL muss mit `https` beginnen. Sie enthält den DNS-Namen oder die IP-Adresse des Clientsystems und die Anschlussnummer, die auf dem Clientsystem für die IBM Spectrum Protect-Clientverwaltungsservices definiert ist. Beispiel: `https://client.mycorp.com:9028`

Wird keine Anschlussnummer angegeben, verwendet das Operations Center die Anschlussnummer 9028. Dies ist die Standardanschlussnummer, wenn Sie die Clientverwaltungsservices auf dem Clientsystem installieren.

#### KEEPMP

Gibt an, ob der Clientknoten den Mountpunkt für die gesamte Sitzung beibehält. Der Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass der Clientknoten den Mountpunkt während der Sitzung freigibt. Haben Maßnahmendefinitionen zur Folge, dass Daten in einem Plattenspeicherpool gespeichert werden, nachdem Daten in einem Speicherpool mit sequenziellem Zugriff gespeichert wurden, werden alle von der Sitzung belegten Mountpunkte freigegeben.

Yes

Gibt an, dass der Clientknoten den Mountpunkt während der gesamten Sitzung beibehalten muss. Haben Maßnahmendefinitionen zur Folge, dass Daten in einem Plattenspeicherpool gespeichert werden, nachdem Daten in einem Speicherpool mit sequenziellem Zugriff gespeichert wurden, werden alle von der Sitzung belegten Mountpunkte nicht freigegeben.

#### AUTOFSRename

Gibt an, ob der Client zum Umbenennen von Dateibereichen aufgefordert wird, wenn für das Clientsystem ein Upgrade auf einen Client erfolgt, der Unicode unterstützt. Das Auffordern und Umbenennen (falls zulässig) findet nur statt, wenn der Client eine der folgenden Operationen ausführt: Archivieren, selektive Sicherung, vollständige Teilsicherung oder partielle Teilsicherung. Beim Umbenennen werden die Namen von bestehenden gesicherten Dateibereichen, die nicht in Unicode sind, im Serverspeicher geändert. Anschließend werden die Dateibereiche in Unicode gesichert. Sie können diesen Parameter für Unicode-fähige IBM Spectrum Protect-Clients mit den Betriebssystemen Windows, Macintosh OS X und NetWare verwenden.

Wichtig: Nachdem der Client mit Unterstützung für Unicode installiert wurde, werden alle neuen Dateibereiche, die der Client sichert, im Serverspeicher mit der Zeichenumsetztabelle UTF-8 gespeichert. UTF-8 ist eine byte-orientierte Verschlüsselungsform, die durch den Unicode Standard angegeben wird.

Sie können einen der folgenden Werte angeben:

Yes

Vorhandene Dateibereiche werden vom Server automatisch umbenannt, wenn für das Clientsystem ein Upgrade auf einen Client erfolgt, der Unicode unterstützt, und der Client eine der folgenden Operationen ausführt: Archivieren, selektive Sicherung, vollständige Teilsicherung oder partielle Teilsicherung. Das Umbenennen findet statt, wenn der Client die grafische Benutzerschnittstelle, die Befehlszeile oder den Client-Scheduler verwendet. Beispielsweise wird ein Laufwerk vom Server wie folgt umbenannt:

- Ursprünglicher Name: D\_DRIVE
- Neuer Name: D\_DRIVE\_OLD

Der neue Name gibt an, dass der Dateibereich auf dem Server in einem Format gespeichert wird, das kein Unicode ist.

No

Dateibereiche werden vom Server nicht automatisch umbenannt, wenn für das Clientsystem ein Upgrade auf einen Client erfolgt, der Unicode unterstützt, und der Client eine der folgenden Operationen ausführt: Archivieren, selektive Sicherung, vollständige Teilsicherung oder partielle Teilsicherung.

Client

Die Option AUTOFSRENAME in der Clientoptionsdatei bestimmt, ob Dateibereiche umbenannt werden.

Standardmäßig ist die Clientoption auf PROMPT gesetzt. Wenn für das Clientsystem ein Upgrade auf einen Client erfolgt, der Unicode unterstützt, und der Client eine IBM Spectrum Protect-Operation mit der grafischen Benutzerschnittstelle oder der Befehlszeile ausführt, zeigt das Programm dem Benutzer einmalig eine Bedienungshilfe an und fordert den Benutzer zur Angabe auf, ob Dateibereiche umbenannt werden sollen.

Wenn der Client-Scheduler eine Operation ausführt, fordert das Programm nicht zur Angabe einer Auswahl für das Umbenennen auf, und es werden keine Dateibereiche umbenannt. Sicherungen von vorhandenen Dateibereichen werden wie zuvor gesendet (nicht in Unicode).

#### VALIDateprotocol (veraltet)

Gibt an, ob IBM Spectrum Protect eine zyklische Blockprüfung ausführt, um die Daten zu validieren, die zwischen dem Client und dem Server gesendet werden. Der Parameter ist wahlfrei.

Wichtig: Ab IBM Spectrum Protect Version 8.1.2 und Tivoli Storage Manager Version 7.1.8 wird dieser Parameter nicht mehr verwendet. Die durch diesen Parameter aktivierte Validierung wird durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter SESSIONSECURITY durchgesetzt wird. Der Parameter VALIDATEPROTOCOL wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

#### TXNGroupmax

Gibt die Anzahl Dateien an, die als Gruppe zwischen einem Client und einem Server zwischen Transaktions-COMMIT-Punkten übertragen werden. Die Clientleistung kann verbessert werden, indem ein höherer Wert für diese Option verwendet wird.

Der Wert 0 gibt an, dass der Knoten den globalen Serverwert verwendet, der in der Serveroptionsdatei definiert ist. Soll ein anderer Wert als der globale Serverwert verwendet werden, geben Sie einen Wert von 4 bis 65.000 für diesen Parameter an. Der Knotenwert hat Vorrang vor dem Serverwert.

Tipp: Die Vergrößerung des Werts für TXNGROUPMAX führt zu einer Erhöhung der Auslastung des Wiederherstellungsprotokolls. Eine höhere Auslastung des Wiederherstellungsprotokolls kann das Risiko erhöhen, dass der Protokollspeicherbereich nicht mehr ausreicht. Werten Sie die Leistung jedes Knotens aus, bevor Sie den Parameter ändern.

#### DATAWritepath

Gibt den Übertragungspfad an, der verwendet wird, wenn der Client während Speicheroperationen (Sicherung oder Archivierung) Daten an den Server und/oder den Speicheragenten sendet. Der Parameter ist wahlfrei.

Hinweis: Ist kein Pfad verfügbar, kann der Knoten keine Daten senden. Wenn Sie z. B. die LAN-unabhängige Option auswählen, aber kein LAN-unabhängiger Pfad definiert ist, schlägt die Operation fehl.

Sie können einen der folgenden Werte angeben:

##### ANY

Gibt an, dass Daten über einen beliebigen verfügbaren Pfad an den Server und/oder Speicheragenten gesendet werden. Ein LAN-unabhängiger Pfad wird verwendet, wenn einer verfügbar ist. Ist kein LAN-unabhängiger Pfad verfügbar, werden die Daten über das LAN übertragen.

##### LAN

Gibt an, dass Daten über das LAN gesendet werden.

##### LANFree

Gibt an, dass Daten über einen LAN-unabhängigen Pfad gesendet werden.

#### DATAReadpath

Gibt den Übertragungspfad an, der verwendet wird, wenn der Server und/oder Speicheragent während Operationen wie Zurückschreiben oder Abrufen Daten für einen Client lesen. Der Parameter ist wahlfrei.

Hinweis: Ist kein Pfad verfügbar, können keine Daten gelesen werden. Wenn Sie z. B. die LAN-unabhängige Option auswählen, aber kein LAN-unabhängiger Pfad definiert ist, schlägt die Operation fehl. Der Wert für den Übertragungspfad gilt auch für Übernahmeverbindungen. Wird der Wert auf LANFree gesetzt, kann für den Knoten auf dem sekundären Server keine Übernahme erfolgen.

Sie können einen der folgenden Werte angeben:

##### ANY

Gibt an, dass der Server und/oder Speicheragent einen beliebigen verfügbaren Pfad verwenden, um Daten zu lesen. Ein LAN-unabhängiger Pfad wird verwendet, wenn einer verfügbar ist. Ist kein LAN-unabhängiger Pfad verfügbar, werden die Daten über das LAN gelesen.

##### LAN

Gibt an, dass Daten über das LAN gelesen werden.

##### LANFree

Gibt an, dass Daten über einen LAN-unabhängigen Pfad gelesen werden.

#### SESSIONINITiation

Steuert, ob der Server oder der Client Sitzungen einleitet. Der Parameter ist wahlfrei.

#### Clientorserver

Gibt an, dass der Client Sitzungen mit dem Server einleiten kann, indem über den TCP/IP-Anschluss kommuniziert wird, der mit der Serveroption TCPPOINT definiert wird. Die Zeitplanung über Serversystemanfrage kann ebenfalls verwendet werden, um den Client aufzufordern, eine Verbindung zum Server herzustellen.

#### SERVEROnly

Gibt an, dass der Server keine Clientanforderungen für Sitzungen akzeptiert. Alle Sitzungen müssen durch die Zeitplanung über Serversystemanfrage an dem Anschluss eingeleitet werden, der mit dem Befehl REGISTER oder

UPDATE NODE für den Client definiert wird. Sie können den Clientakzeptor (dsmcad) nicht verwenden, um den Scheduler zu starten, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist.

#### HLAddress

Gibt die Client-IP-Adresse an, die der Server anspricht, um geplante Ereignisse einzuleiten. Dieser Parameter muss verwendet werden, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist, unabhängig von den Adressen, die zuvor vom Client verwendet wurden, um den Server anzusprechen.

Die Adresse kann entweder im numerischen Format oder im Hostnamenformat angegeben werden. Wird eine numerische Adresse verwendet, wird sie ohne Prüfung durch einen Domänennamensserver gesichert. Ist die Adresse nicht korrekt, kann dies zu Fehlern führen, wenn der Server versucht, den Client anzusprechen. Adressen im Hostnamenformat werden mit einem Domänennamensserver geprüft. Geprüfte Namen werden mit Domänennamensservices (Domain Name Services) gesichert und aufgelöst, wenn der Server den Client kontaktiert.

#### LLAddress

Gibt die Clientanschlussnummer an, an der der Client für Sitzungen von dem Server empfangsbereit ist. Dieser Parameter muss verwendet werden, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist, unabhängig von den Adressen, die zuvor vom Client verwendet wurden, um den Server anzusprechen.

Der Wert für diesen Parameter muss mit dem Wert der Clientoption TCPCLIENTPORT übereinstimmen. Der Standardwert ist 1501.

#### HLAddress

Gibt die Client-IP-Adresse an, die der Server anspricht, um geplante Ereignisse einzuleiten. Dieser optionale Parameter wird nur verwendet, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist, unabhängig von den Adressen, die zuvor vom Client verwendet wurden, um den Server zu kontaktieren. Wird SESSIONINITIATION=SERVERONLY nicht verwendet, hat diese Option keine Auswirkung.

Die Adresse kann entweder im numerischen Format oder im Hostnamenformat angegeben werden. Wird eine numerische Adresse verwendet, wird sie ohne Prüfung durch einen Domänennamensserver gesichert. Ist die Adresse nicht korrekt, kann dies zu Fehlern führen, wenn der Server versucht, den Client anzusprechen. Adressen im Hostnamenformat werden mit einem Domänennamensserver geprüft. Geprüfte Namen werden mit Domänennamensservices (Domain Name Services) gesichert und aufgelöst, wenn der Server den Client kontaktiert.

#### LLAddress

Gibt die Clientanschlussnummer an, an der der Client für Sitzungen von dem Server empfangsbereit ist. Dieser optionale Parameter wird nur verwendet, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist, unabhängig von den Adressen, die zuvor vom Client verwendet wurden, um den Server zu kontaktieren. Wird SESSIONINITIATION=SERVERONLY nicht verwendet, hat diese Option keine Auswirkung.

Der Wert für diesen Parameter muss mit dem Wert der Clientoption TCPCLIENTPORT übereinstimmen. Der Standardwert ist 1501.

#### EMAILAddress

Dieser Parameter wird für weitere Kontaktinformationen verwendet. Die mit diesem Parameter angegebenen Informationen werden von IBM Spectrum Protect nicht verwendet.

#### DEDUPLICATION

Gibt an, wo die Datendeduplizierung für diesen Knoten stattfinden kann. Sie können einen der folgenden Werte angeben:

##### SERVEROnly

Gibt an, dass von diesem Knoten gespeicherte Daten nur auf dem Server dedupliziert werden können.

##### Clientorserver

Gibt an, dass von diesem Knoten gespeicherte Daten entweder auf dem Client oder auf dem Server dedupliziert werden können. Um die Datendeduplizierung auf dem Client auszuführen, müssen Sie auch den Wert YES für die Clientoption DEDUPLICATION angeben. Sie können diese Option in der Clientoptionsdatei oder in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server angeben.

#### TARGETLevel

Gibt das Clientimplementierungspaket für diesen Knoten an. Für V.R.M.F (Version.Release.Modifikation.Fix-Level) kann ein gültiges Releasepaket angegeben werden. Beispiel: TARGETLevel=6.2.0.0.

Sie müssen jedes Segment mit einer Zahl angeben, die für ein Implementierungspaket zutreffend ist. Sie können keinen Stern in einem Feld als Ersetzung für eine gültige Zahl verwenden. Soll ein vorhandener Wert entfernt werden, eine

Nullzeichenfolge (" ") angeben. Der Parameter ist wahlfrei.

Einschränkung: Der Parameter TARGETLEVEL gilt nicht für Knoten mit dem Typ NAS oder SERVER.

#### BACKUPINITiation

Gibt an, ob die ID eines Benutzers ohne Rootberechtigung auf dem Clientknoten Dateien auf dem Server sichern kann. Der Parameter ist wahlfrei. Der Standardwert ALL gibt an, dass IDs der Benutzer ohne Rootberechtigung Daten auf dem Server sichern können. Sie können einen der folgenden Werte auswählen:

##### All

Gibt an, dass die IDs der Benutzer ohne Rootberechtigung Dateien auf dem Server sichern können. ALL ist der Standardwert, wenn BACKUPINITIATION nicht angegeben wird.

##### ROOT

Gibt an, dass nur die Rootbenutzer-ID Dateien auf dem Server sichern kann.

Einschränkung: Das Attribut wird vom Server ignoriert, wenn der Client für Sichern/Archivieren eine Verbindung von einem anderen Betriebssystem als AIX, Linux, Solaris oder Mac OS herstellt.

#### BKREPLRuledefault, ARREPLRuledefault und SPREPLRuledefault

Gibt die Replikationsregel an, die für einen Datentyp gilt, wenn die Dateibereichsregeln für den Datentyp auf DEFAULT gesetzt sind:

##### BKREPLRuledefault

Gibt die Replikationsregel für Sicherungsdaten an.

##### ARREPLRuledefault

Gibt die Replikationsregel für Archivierungsdaten an.

##### SPREPLRuledefault

Gibt die Replikationsregel für speicherverwaltete Daten an.

Sie können Replikationsregeln für normale Priorität oder Replikationsregeln für hohe Priorität angeben. In einem Replikationsprozess, der sowohl Daten mit normaler Priorität als auch Daten mit hoher Priorität einschließt, werden Daten mit hoher Priorität zuerst repliziert. Bevor Sie eine Regel angeben, beachten Sie die Reihenfolge, in der die Daten repliziert werden sollen.

Beispiel: Angenommen, ein Clientknoten enthält aktive Sicherungsdaten und Archivierungsdaten. Die Replikation der aktiven Sicherungsdaten hat eine höhere Priorität als die der Archivierungsdaten. Um beide Datentypen zu priorisieren, geben Sie `BKREPLRULEDEFAULT=ACTIVE_DATA_HIGH_PRIORITY ARREPLRULEDEFAULT=ALL_DATA` an.

Sie können die folgenden Regeln angeben:

##### ALL\_DATA

Repliziert aktive und inaktive Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten. Die Daten werden mit einer normalen Priorität repliziert.

##### ACTIVE\_DATA

Repliziert nur aktive Sicherungsdaten. Die Daten werden mit einer normalen Priorität repliziert. Diese Regel ist nur für BKREPLRULEDEFAULT gültig.

Achtung:

Wenn Sie ACTIVE\_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

- Wenn eine Releaseversion vor Version 7.1.1 entweder auf dem Quellenreplikationsserver oder auf dem Zielreplikationsserver installiert ist.
- Wenn Sie den Befehl REPLICATE NODE mit dem Parameter `FORCERECONCILE=YES` verwenden.
- Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Releaseversion vor Version 7.1.1 ausführen.

Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

##### ALL\_DATA\_HIGH\_PRIORITY

Repliziert aktive und inaktive Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten. Daten werden mit einer hohen Priorität repliziert.

##### ACTIVE\_DATA\_HIGH\_PRIORITY

Diese Regel entspricht der Replikationsregel ACTIVE\_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden. Diese Regel ist nur für BKREPLRULEDEFAULT gültig.

##### DEFAULT

Repliziert Daten gemäß der Serverreplikationsregel für Sicherungsdaten.

Beispiel: Angenommen, Sie möchten die Archivierungsdaten in allen Dateibereichen replizieren, die zu einem Clientknoten gehören. Die Replikation der Archivierungsdaten hat eine hohe Priorität. Eine Methode zur Ausführung dieser Task ist die Angabe von `ARREPLRULEDEFAULT=DEFAULT`. Stellen Sie sicher, dass die Dateibereichsregeln für Archivierungsdaten ebenfalls auf `DEFAULT` gesetzt sind und die Serverregel für Archivierungsdaten auf `ALL_DATA_HIGH_PRIORITY` gesetzt ist.

Einschränkung: Wenn ein Knoten für die Replikation konfiguriert ist, werden die Dateibereichsregeln auf `DEFAULT` gesetzt, nachdem der Knoten Daten auf dem Quellenreplikationsserver gespeichert hat.

#### NONE

Daten des angegebenen Typs werden nicht repliziert.

Sollen beispielsweise speicher verwaltete Daten, die zu einem Clientknoten gehören, nicht repliziert werden, geben Sie `SPREPLRULEDEFAULT=NONE` an.

#### REPLState

Gibt an, ob Daten, die zu dem Clientknoten gehören, für die Replikation bereit sind. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

##### ENabled

Gibt an, dass der Clientknoten für die Replikation bereit ist.

##### DISabled

Gibt an, dass die Replikation erst stattfindet, wenn sie aktiviert wurde.

Die Systemantwort auf diese Einstellungen hängt davon ab,

ob die Clientknotendefinition nur auf dem Quellenreplikationsserver vorhanden ist und Sie den Clientknoten zum ersten Mal für die Replikation konfigurieren

Wenn Sie den Replikationsstatus auf `ENABLED` oder `DISABLED` setzen, wird der Replikationsmodus des Knotens auf dem Quellenreplikationsserver automatisch auf `SEND` gesetzt, nachdem der Befehl `UPDATE NODE` ausgegeben wurde. Wenn die Replikation zum ersten Mal erfolgt, wird eine Clientknotendefinition automatisch auf dem Zielsystem erstellt. Der Replikationsstatus des Clientknotens auf dem Zielsystem wird automatisch auf `ENABLED` gesetzt. Der Replikationsmodus wird auf `RECEIVE` gesetzt.

ob die Clientknotendefinition auf dem Quellen- und dem Zielreplikationsserver vorhanden ist und die Knotendaten zuvor repliziert wurden

Damit die Replikation ausgeführt werden kann, muss der Replikationsstatus des Clientknotens sowohl auf dem Quellen- als auch auf dem Zielsystem auf `ENABLED` gesetzt werden. Lautet beispielsweise der Replikationsstatus eines Clientknotens auf dem Quellensystem `ENABLED` und der Replikationsstatus auf dem Zielsystem `DISABLED`, findet keine Replikation statt.

ob die Clientknotendefinition auf dem Quellen- und dem Zielreplikationsserver vorhanden ist und die Knotendaten zuvor vom Quellenreplikationsserver exportiert und auf den Zielreplikationsserver importiert wurden

In diesem Fall konfigurieren Sie die Clientknoten, um die Daten zwischen den beiden Servern zu synchronisieren. Wenn die Replikation zum ersten Mal erfolgt, wird der Replikationsstatus des Clientknotens auf dem Zielsystem automatisch auf `ENABLED` gesetzt. Daten auf dem Quellen- und Zielsystem werden synchronisiert.

Einschränkung: Um Daten zu synchronisieren, müssen Sie zusätzlich zum Parameter `REPLSTATE` den Parameter `REPLMODE` angeben.

Sie können den Parameter `REPLMODE` nur angeben, wenn der Clientknoten noch nie repliziert wurde:

- Wenn die Clientknotendefinition nur auf dem Quellenreplikationsserver vorhanden ist, wird der Replikationsmodus des Knotens auf dem Quellenreplikationsserver automatisch auf `SEND` gesetzt, wenn der Befehl `UPDATE NODE` ausgegeben wird. Der Replikationsmodus des Knotens auf dem Zielreplikationsserver wird automatisch auf `RECEIVE` gesetzt.
- Wenn Daten, die zu dem Knoten gehören, zuvor repliziert wurden, lautet der Replikationsmodus des Knotens auf dem Quellenreplikationsserver `SEND`. Der Replikationsmodus des Knotens auf dem Zielreplikationsserver lautet `RECEIVE`.

#### REPLMode

Gibt an, ob die Daten synchronisiert werden sollen, die zu diesem Clientknoten gehören. Geben Sie diesen Parameter nur an, wenn Daten, die zu dem Clientknoten gehören, vom Quellenreplikationsserver exportiert und auf den Zielreplikationsserver importiert wurden. Die Synchronisation erfolgt während der Replikation.

Um Daten zu synchronisieren, müssen Sie den Befehl `UPDATE NODE` sowohl auf dem Quellen- als auch auf dem Zielreplikationsserver ausgeben und die Parameter `REPLMODE` und `REPLSTATE` angeben. Der Wert, den Sie für den Parameter `REPLMODE` angeben, hängt davon ab, ob der Server eine Quelle oder ein Ziel für replizierte Daten ist.

Sie können einen der folgenden Werte angeben:

##### SYNCSEnd

Gibt an, dass Daten, die zu diesem Clientknoten gehören, während der Replikation mit Daten auf dem Zielsystem synchronisiert werden. Geben Sie diesen Wert nur auf dem Server an, der die Daten exportiert hat. Nach Beendigung der Synchronisation wird der Replikationsmodus für den Clientknoten auf dem Quellensystem automatisch auf `SEND` gesetzt. Der Replikationsmodus lautet so lange `SEND`, bis Sie den Knoten mit dem Befehl `REMOVE REPLNODE` entfernen.

## SYNCRECeive

Gibt an, dass Daten, die zu diesem Clientknoten gehören, während der Replikation mit Daten auf einem Quellenserver synchronisiert werden. Geben Sie diesen Wert nur auf dem Server an, der die Daten importiert hat. Nach Beendigung der Synchronisation wird der Replikationsmodus für den Clientknoten auf dem Zielsystem automatisch auf RECEIVE gesetzt. Der Replikationsmodus lautet so lange RECEIVE, bis Sie den Knoten mit dem Befehl REMOVE REPLNODE entfernen.

### Einschränkungen:

- Sie können den Parameter REPLMODE nur definieren, wenn der anfängliche Replikationsstatus NONE lautet. Um Daten zu synchronisieren, ändern Sie den Replikationsstatus in ENABLED oder DISABLED und geben Sie einen Wert für den Parameter REPLMODE an.
- Daten können nur synchronisiert werden, wenn Sie DATES=ABSOLUTE im Befehl IMPORT NODE angegeben haben. Wenn Sie DATES=RELATIVE angegeben haben, um Daten zu importieren, müssen Sie den Knoten vor der Replikation umbenennen oder seine Daten löschen. Wenn Sie nicht einen dieser Schritte ausführen, können Daten verloren gehen.
- Wurde der Parameter REPLMODE nicht korrekt definiert, müssen Sie den Befehl REMOVE REPLNODE ausgeben, bevor die Clientknotendefinition aktualisiert wird. Beispiel: Angenommen, Sie haben die Definition eines Clientknotens aktualisiert, dessen Daten repliziert werden sollten. Die Daten, die zu dem Knoten gehören, wurden zuvor auf den Zielreplikationsserver exportiert. Sie haben ENABLED als Einstellung des Parameters REPLSTATE angegeben. Sie haben jedoch nicht SYNCSEND auf dem Quellenreplikationsserver angegeben. Daher wurde der Parameter REPLMODE automatisch auf SEND gesetzt, und Daten, die zu dem Knoten gehören, konnten nicht synchronisiert oder repliziert werden.

Mit dem Befehl REMOVE REPLNODE werden der Replikationsstatus und der Replikationsmodus auf NONE gesetzt. Geben Sie nach der Ausführung des Befehls REMOVE REPLNODE den Befehl UPDATE NODE mit den korrekten Parametern und Werten erneut aus.

## RECOVERDamaged

Gibt an, ob beschädigte Dateien für diesen Knoten von einem Zielreplikationsserver wiederhergestellt werden können. Der Parameter ist wahlfrei. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

### Yes

Gibt an, dass die Wiederherstellung beschädigter Dateien durch einen Zielreplikationsserver für diesen Knoten aktiviert ist.

### No

Gibt an, dass die Wiederherstellung beschädigter Dateien durch einen Zielreplikationsserver für diesen Knoten nicht aktiviert ist.

Tipp: Der Wert des Parameters RECOVERDAMAGED ist nur eine von mehreren Einstellungen, die bestimmen, ob beschädigte Dateien wiederhergestellt werden. Informationen zur Angabe der Einstellungen finden Sie in Einstellungen, die sich auf die Wiederherstellung beschädigter Dateien auswirken.

## ROLEOVERRIDE

Gibt an, ob die zurückgemeldete Rolle des Clients für die Zurückmeldung der PVU-Schätzung (PVU - Prozessor-Value-Unit) überschrieben werden soll. Der Standardwert ist USERREPORTED.

Die vom Client zurückgemeldete Rolle ist entweder 'Clienteinheit' (z. B. eine Workstation) oder 'Servereinheit' (z. B. Datei-/Druckserver, Anwendungsserver, Datenbank). Standardmäßig meldet der Client seine Rolle auf der Basis des Clienttyps und des Betriebssystems zurück. Alle Clients melden anfänglich ihre Rolle als 'Servereinheit' zurück, mit Ausnahme von IBM Spectrum Protect-Clients für Sichern/Archivieren, auf denen Microsoft Windows-Workstationverteilungen (Windows Vista) und Macintosh OS X ausgeführt werden.

Geben Sie einen der folgenden Werte an:

### Client

Gibt eine Clienteinheit an.

### Server

Gibt eine Servereinheit an.

### Other

Gibt an, dass dieser Knoten nicht für die Zurückmeldung der PVU-Schätzung verwendet werden soll. Der Wert 'Other' kann nützlich sein, wenn mehrere Knoten für ein physisches System implementiert sind (z. B. virtuelle Umgebungen, Testknoten, Knoten im Ruhezustand und Knoten, die nicht in der Produktion oder im Clustering sind).

### Userreported

Die zurückgemeldete Rolle verwenden, die vom Client bereitgestellt wird.

## AUTHentication

Dieser Parameter bestimmt die von Ihnen verwendete Kennwortauthentifizierungsmethode (LDAP oder LOCAL).

### Local

Gibt an, dass der Knoten die lokale IBM Spectrum Protect-Serverdatenbank zum Speichern von Kennwörtern verwendet.

### LDap

Gibt an, dass der Knoten einen LDAP-Verzeichnisserver für die Authentifizierung von Kennwörtern verwendet. Kennwörter werden nicht in der IBM Spectrum Protect-Datenbank gespeichert.

#### SYNCLdapdelete

Dieser Parameter gilt nur, wenn ein Knoten, der sich mit einem Lightweight Directory Access Protocol-Server (LDAP-Server) authentifiziert, zur Authentifizierung mit dem IBM Spectrum Protect-Server wechseln soll. Der Parameter gibt an, ob der Knoten auf dem LDAP-Server entfernt werden soll.

##### Yes

Gibt an, dass der Knoten entfernt wird.

Einschränkung: Sie dürfen nicht den Wert YES angeben. (Der Wert YES ist nur für die Benutzer der vorherigen LDAP-Authentifizierungsmethode gültig, die in Kennwörter und Anmeldeverfahren verwalten beschrieben wird.)

##### No

Gibt an, dass der Knoten nicht entfernt wird. Dies ist der Standardwert.

#### SSLrequired (veraltet)

Gibt an, ob der Knoten das Protokoll Secure Sockets Layer (SSL) für die Kommunikation mit dem IBM Spectrum Protect-Server verwenden muss. Der Parameter ist wahlfrei. Wenn Sie Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren, müssen Sie die Sitzungen mit SSL oder einer anderen Netzsicherheitsmethode schützen.

Wichtig: Ab IBM Spectrum Protect Version 8.1.2 und Tivoli Storage Manager Version 7.1.8 wird dieser Parameter nicht mehr verwendet. Die durch diesen Parameter aktivierte Validierung wird durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter SESSIONSECURITY durchgesetzt wird. Der Parameter SSLREQUIRED wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

#### SESSIONSECURITY

Gibt an, ob der Knoten die sichersten Einstellungen verwenden muss, um mit einem IBM Spectrum Protect-Server zu kommunizieren. Dieser Parameter ist wahlfrei.

Sie können einen der folgenden Werte angeben:

##### STRICT

Gibt an, dass die striktesten Sicherheitseinstellungen für den Knoten durchgesetzt werden. Der Wert STRICT verwendet das sicherste Kommunikationsprotokoll, das verfügbar ist. Dies ist derzeit TLS 1.2. Das TLS 1.2-Protokoll wird für SSL-Sitzungen zwischen dem Server und dem Knoten verwendet. Um anzugeben, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, lesen Sie die Informationen zur Clientoption SSL.

Für die Verwendung des Werts STRICT müssen die folgenden Anforderungen erfüllt werden, um sicherzustellen, dass sich der Knoten mit dem Server authentifizieren kann:

- Der Knoten und der Server müssen IBM Spectrum Protect-Software verwenden, die den Parameter SESSIONSECURITY unterstützt.
- Der Knoten muss für die Verwendung des TLS 1.2-Protokolls für SSL-Sitzungen zwischen dem Server und dem Knoten konfiguriert werden.

Knoten, für die der Wert STRICT definiert ist und die diese Anforderungen nicht erfüllen, können sich nicht mit dem Server authentifizieren.

##### TRANSITIONAL

Gibt an, dass die vorhandenen Sicherheitseinstellungen für den Knoten durchgesetzt werden. Dies ist der Standardwert. Dieser Wert ist für die temporäre Verwendung bestimmt, während Sie Ihre Sicherheitseinstellungen aktualisieren, um die Anforderungen für den Wert STRICT zu erfüllen.

Ist SESSIONSECURITY=TRANSITIONAL definiert und hat der Knoten nie die Anforderungen für den Wert STRICT erfüllt, authentifiziert sich der Knoten weiterhin mithilfe des Werts TRANSITIONAL. Wenn ein Knoten jedoch die Anforderungen für den Wert STRICT erfüllt, wird der Wert des Parameters SESSIONSECURITY automatisch von TRANSITIONAL in STRICT aktualisiert. Der Knoten kann sich dann nicht mehr mit einer Version des Clients oder mit einem SSL/TLS-Protokoll authentifizieren, die bzw. das die Anforderungen für STRICT nicht erfüllt. Nachdem sich ein Knoten erfolgreich mit einem Kommunikationsprotokoll authentifiziert hat, das mehr Sicherheit bietet, kann sich der Knoten nicht mehr mit einem weniger sicheren Protokoll authentifizieren. Beispiel: Wenn ein Knoten, der nicht SSL verwendet, aktualisiert wird und sich mithilfe von TLS 1.2 erfolgreich authentifiziert, kann sich der Knoten nicht mehr ohne SSL-Protokoll oder mithilfe von TLS 1.1 authentifizieren. Diese Einschränkung gilt auch bei Verwendung von Funktionen wie z. B. virtuelle Datenträger, wenn sich der Knoten beim IBM Spectrum Protect-Server als Knoten von einem anderen Server authentifiziert.

#### SPLITLARGEObjects

Gibt an, ob große Objekte, die von diesem Knoten gespeichert werden, automatisch vom Server in kleinere Teile aufgeteilt werden, um die Serververarbeitung zu optimieren. Die Angabe von 'Yes' hat zur Folge, dass der Server große Objekte (über 10 GB) in kleinere Teile aufteilt, wenn sie von einem Clientknoten gespeichert werden. Bei Angabe von 'No' wird dieser Prozess übergangen. Geben Sie 'No' nur an, wenn Ihr primäres Ziel die Maximierung des Durchsatzes von Sicherungen direkt auf Band ist. Der Standardwert ist 'Yes'.



## Beispiel: Der Knoten SIMON soll sich mit einem LDAP-Verzeichnisserver authentifizieren und die Verbindung über SSL herstellen

---

```
update node simon authentication=ldap sslrequired=yes
```

Wenn Sie den Parameter SSLREQUIRED angeben, wird der Server nicht automatisch für SSL konfiguriert. Sie müssen die Anweisungen zum Herstellen der Verbindung mit SSL befolgen, damit das Beispiel funktioniert.

## Beispiel: Alle Knoten für die Kommunikation mit einem Server unter Verwendung der Sitzungssicherheit 'strict' aktualisieren

---

Alle Knoten für die Verwendung der striktesten Sicherheitseinstellungen aktualisieren, um sich mit dem Server zu authentifizieren.

```
update node * sessionsecurity=strict
```

## Beispiel: Einen Knoten mit Informationen zu einem Software-Release für eine zukünftige Implementierung aktualisieren

---

Das Feature für die Clientimplementierung unterstützt Sie bei der Aktualisierung eines Clients für Sichern/Archivieren auf ein neues Release. Die Informationen, die von dem Befehl UPDATE NODE generiert werden, können Ihnen bei der Planung einer Implementierung helfen. Die Informationen werden für eine zukünftige Implementierung gespeichert und können mit dem Befehl QUERY NODE angezeigt werden. Nach einer Implementierung können Sie den Befehl QUERY NODE ausgeben, um die aktuelle Version und die Zielversion anzuzeigen. In diesem Beispiel soll der Knoten LARRY in Version 6.3.0.0 des Clients für Sichern/Archivieren aktualisiert werden.

```
update node LARRY targetlevel=6.3.0.0
```

## Beispiel: Die Sicherung eines Knotens aktualisieren, um Daten zu komprimieren und zu verhindern, dass der Client archivierte Dateien löscht

---

Den Knoten LARRY so aktualisieren, dass die Daten auf dem Knoten LARRY komprimiert werden, wenn sie von IBM Spectrum Protect gesichert bzw. archiviert werden; außerdem soll dem Client nicht gestattet sein, archivierte Dateien zu löschen.

```
update node larry compression=yes archdelete=no
```

## Beispiel: Die Anzahl der Dateien eines Knotens aktualisieren, die als Gruppe übertragen werden können

---

Den Knoten LARRY aktualisieren und den Wert für TXNGroupmax auf 1.000 erhöhen.

```
update node larry txngroupmax=1000
```

## Beispiel: Einen Knoten aktualisieren und die Deduplizierung auf dem Client zulassen

---

Den Knoten BOB aktualisieren, damit er Daten auf dem Client deduplizieren kann.

```
update node bob deduplication=clientorserver
```

## Beispiel: Die Rolle des Knotens BOB in eine Servereinheit für die Zurückmeldung der PVU-Schätzung aktualisieren

---

Sollen PVU-Werte akkumuliert werden, werden nur Servereinheitenrollen aufgezeichnet. Sie können einen Knoten von 'Clienteinheit' in 'Servereinheit' aktualisieren, indem Sie den Befehl UPDATE NODE ausgeben. In diesem Beispiel wird der Knoten BOB in eine Servereinheit aktualisiert.

```
update node bob role=server
```

## Beispiel: Eine Knotendefinition auf einem Quellenreplikationsserver aktualisieren

---

NODE1 ist für einen Quellenreplikationsserver definiert. Die Daten, die zu NODE1 gehören, wurden zuvor auf einen Zielreplikationsserver exportiert. Die Replikationsregel für Sicherungsdaten, die zu NODE1 gehören, aktualisieren, sodass aktive Sicherungsdaten mit einer hohen Priorität repliziert werden. Die Replikation für den Knoten aktivieren. Die Datensynchronisation mit dem Zielreplikationsserver definieren.

```
update node node1 bkreplruledefault=active_data_high_priority  
replstate=enabled replmode=syncsend
```

## Beispiel: Eine Knotendefinition aktualisieren, um die Wiederherstellung beschädigter Dateien zu aktivieren

Den Knoten PAYROLL aktualisieren, um die Wiederherstellung beschädigter Dateien durch einen Zielreplikationsserver zu aktivieren.

```
update node payroll recoverdamaged=yes
```

### Zugehörige Befehle

Tabelle 2. Zugehörige Befehle für UPDATE NODE

| Befehl                     | Beschreibung   |
|----------------------------|--|
| QUERY FILESPACE            | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.  |
| QUERY NODE                 | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.  |
| QUERY PVUESTIMATE          | Zeigt eine Schätzung der Clienteinheiten und Servereinheiten an, die verwaltet werden.   |
| QUERY REPLNODE             | Zeigt Informationen zum Replikationsstatus eines Clientknotens an.   |
| REGISTER ADMIN             | Definiert einen neuen Administrator, ohne Administratorberechtigung zu erteilen.   |
| REGISTER NODE              | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.  |
| REMOVE NODE                | Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.                               |
| REMOVE REPLNODE            | Entfernt einen Knoten aus der Replikation.   |
| RENAME NODE                | Ändert den Namen eines Clientknotens.  |
| REPLICATE NODE             | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |
| RESET PASSEXP              | Setzt die Kennwortablaufdauer für Knoten oder Administratoren zurück.  |
| SET DEDUPVERIFICATIONLEVEL | Gibt den Prozentsatz der Bereiche an, die vom Server während der clientseitigen Deduplizierung geprüft werden sollen.          |
| SET PASSEXP                | Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.   |
| SET REPLRECOVERDAMAGED     | Gibt an, ob die Knotenreplikation aktiviert ist, um beschädigte Dateien durch einen Zielreplikationsserver wiederherzustellen. |
| UPDATE ADMIN               | Ändert das Kennwort eines Administrators bzw. die zu einem Administrator gehörigen Kontaktinformationen.                       |
| UPDATE FILESPACE           | Ändert Knotenreplikationsregeln für Dateibereiche.   |

#### Zugehörige Verweise:

[Ssl \(Clientoption\)](#)

## UPDATE NODEGROUP (Knotengruppe aktualisieren)

Verwenden Sie diesen Befehl, um die Beschreibung einer Knotengruppe zu ändern.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

### Syntax

```
>>-UPDate NODEGroup--Gruppenname----->
```

>--DESCRiption--==--Beschreibung-----><

## Parameter

### Gruppenname

Gibt den Namen der Knotengruppe an, deren Beschreibung aktualisiert werden soll.

### DESCRiption (Erforderlich)

Gibt eine Beschreibung der Knotengruppe an. Dieser Parameter ist erforderlich. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Enthält die Beschreibung Leerzeichen, schließen Sie die gesamte Beschreibung in Anführungszeichen ein.

## Beispiel: Die Beschreibung einer Knotengruppe aktualisieren

Die Knotengruppe `group1` mit einer neuen Beschreibung aktualisieren.

```
update nodegroup group1 description="Personalabteilung"
```

## Zugehörige Befehle



Tabelle 1. Zugehörige Befehle für UPDATE NODEGROUP

| Befehl                 | Beschreibung  |
|------------------------|---|
| DEFINE BACKUPSET       | Definiert eine zuvor generierte Sicherungsgruppe für einen Server.          |
| DEFINE NODEGROUP       | Definiert eine Gruppe von Knoten.   |
| DEFINE NODEGROUPMEMBER | Fügt einer Knotengruppe einen Clientknoten hinzu.                           |
| DELETE BACKUPSET       | Löscht eine Sicherungsgruppe.   |
| DELETE NODEGROUP       | Löscht eine Knotengruppe.   |
| DELETE NODEGROUPMEMBER | Löscht einen Clientknoten aus einer Knotengruppe.                           |
| GENERATE BACKUPSET     | Generiert eine Sicherungsgruppe mit den Daten eines Clients.                |
| QUERY BACKUPSET        | Zeigt Sicherungsgruppen an.   |
| QUERY NODEGROUP        | Zeigt Informationen zu Knotengruppen an.                                    |
| UPDATE BACKUPSET       | Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum. |




## UPDATE PATH (Pfad ändern)

Verwenden Sie diesen Befehl, um eine Pfaddefinition zu aktualisieren.

Syntax- und Parameterbeschreibungen sind für die folgenden Pfadtypen verfügbar.

- UPDATE PATH (Pfad ändern, wenn das Ziel ein Laufwerk ist)
- UPDATE PATH (Pfad ändern, wenn das Ziel ein Kassettenarchiv ist)
-  AIX-Betriebssysteme  Linux-Betriebssysteme UPDATE PATH (Pfad aktualisieren, wenn das Ziel ein ZOSMEDIA-Kassettenarchiv ist)

Ausführliche und aktuelle Informationen zur Einheitenunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

-  AIX-Betriebssysteme  Windows-Betriebssysteme Supported devices for AIX and Windows
-  Linux-Betriebssysteme Supported devices for Linux

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE PATH

| Befehl           | Beschreibung  |
|------------------|---|
| DEFINE DATAMOVER | Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server. |
| DEFINE DRIVE     | Ordnet ein Laufwerk einem Kassettenarchiv zu.                                       |

| Befehl           | Beschreibung  |
|------------------|---|
| DEFINE LIBRARY   | Definiert ein automatisiertes oder manuelles Kassettenarchiv.   |
| DEFINE PATH      | Definiert einen Pfad von einer Quelle zu einem Ziel.            |
| DELETE PATH      | Löscht einen Pfad von einer Quelle zu einem Ziel.               |
| QUERY PATH       | Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an. |
| UPDATE DATAMOVER | Ändert die Definition einer Einheit zum Versetzen von Daten.    |

## UPDATE PATH (Pfad ändern, wenn das Ziel ein Laufwerk ist)

Verwenden Sie diese Syntax, wenn Sie die Definition eines Pfads zu einem Laufwerk aktualisieren.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-UPDate PATH--Quellename--Zielname----->
>--SRCType-----+--DATAMover+--+-----+----->
      '-SERVer----'   '-AUTODetect-----+No--+-'
                          '-Yes-'
>--DESTType-----DRive--LIBRARY-----Kassettenarchivname----->
>+-----+-----+-----+----->
      '-DEVIce-----Einheitename-'   '-ONLine-----+Yes+--'
                          '-No--'
>+-----+-----+-----+-----><
      |               .,-----., |
      |               v             | |
      '-DIRectory-----Verzeichnisname+--'
```

### Parameter

Quellename (Erforderlich)

Gibt den Namen der Quelle des Pfads an. Dieser Parameter ist erforderlich.

Zielname (Erforderlich)

Gibt den Namen des Ziels an. Dieser Parameter ist erforderlich.

SRCType (Erforderlich)

Gibt den Typ der Quelle an. Dieser Parameter ist erforderlich. Gültige Werte:

DATAMover

Gibt an, dass eine Einheit zum Versetzen von Daten die Quelle ist.

SERVer

Gibt an, dass ein Server oder ein Speicheragent die Quelle ist.

AUTODetect

Gibt an, ob die Seriennummer für ein Laufwerk oder Kassettenarchiv automatisch in IBM Spectrum Protect erkannt, gemeldet und aktualisiert wird. Dieser Parameter ist wahlfrei. Dieser Parameter ist nur für Pfade gültig, die von dem lokalen Server zu einem Laufwerk oder Kassettenarchiv definiert sind. Gültige Werte:

No

Gibt an, dass die Seriennummer nicht automatisch aktualisiert wird.

Yes

Gibt an, dass die Seriennummer automatisch aktualisiert wird, um dieselbe Seriennummer widerzuspiegeln, die das Laufwerk an IBM Spectrum Protect meldet.

Wichtig:

1. Wurde zuvor keine Seriennummer eingegeben, erhält AUTODETECT den Standardwert YES. Wurde zuvor eine Seriennummer eingegeben, erhält AUTODETECT den Standardwert NO.

2. AUTODETECT=YES in diesem Befehl überschreibt die Seriennummer, die in dem Befehl DEFINE DRIVE definiert wurde.
3. Wenn Sie DESTTYPE=DRIVE und AUTODETECT=YES definieren, wird die Elementnummer des Laufwerks in der IBM Spectrum Protect-Datenbank automatisch geändert, um dieselbe Elementnummer widerzuspiegeln, die der Seriennummer dieses Laufwerks entspricht. Dies gilt für Laufwerke in einem SCSI-Kassettenarchiv. Weitere Informationen zu der Elementnummer befinden sich in der Beschreibung des Befehls DEFINE DRIVE.
4. Je nach Leistungsspektrum der Einheit wird der Parameter AUTODETECT möglicherweise nicht unterstützt.

#### DESTType=Drive (Erforderlich)

Gibt an, dass ein Laufwerk das Ziel ist. Ist das Ziel ein Laufwerk, müssen Sie einen Kassettenarchivnamen angeben. Dieser Parameter ist erforderlich.

#### LIBRARY

Gibt den Namen des Kassettenarchivs an, dem das Laufwerk zugeordnet ist. Das Kassettenarchiv und seine Laufwerke müssen bereits für den Server definiert sein. Verläuft der Pfad von einer NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv, muss das Kassettenarchiv den Typ (LIBTYPE) SCSI, 349x oder ACSLS haben.

#### DEVICE

Gibt den Namen der Einheit an, die der Quelle bekannt ist, oder FILE an, wenn die Einheit ein logisches Laufwerk in einem Kassettenarchiv FILE ist.



 Die Quelle verwendet den Einheitenamen für den Zugriff auf das Laufwerk. Für Beispiele siehe Tabelle 1.

Tabelle 1. Beispiele für Einheitenamen

| Quelle zum Ziel   | Beispiel   |
|---|--|
| Server zu einem Laufwerk (kein FILE-Laufwerk)   |  AIX-Betriebssysteme/dev/rmt3 |
| Speicheragent zu einem Laufwerk (kein FILE-Laufwerk)  | mt3  |
| Speicheragent zu einem Laufwerk, wenn das Laufwerk ein logisches Laufwerk in einem FILE-Kassettenarchiv ist | FILE   |
| NAS-Einheit zum Versetzen von Daten zu einem Laufwerk   | NetApp NAS-Dateiserver: rst01<br>EMC Celerra NAS-Dateiserver: c436t011<br>IBM® System Storage N Series: rst01    |


 Die Quelle verwendet den Einheitenamen für den Zugriff auf das Laufwerk. Für Beispiele siehe Tabelle 2.

Tabelle 2. Beispiele für Einheitenamen

| Quelle zum Ziel   | Beispiel   |
|---|--|
| Server zu einem Laufwerk (kein FILE-Laufwerk)   | /dev/tmscsi/mt3  |
| Speicheragent zu einem Laufwerk (kein FILE-Laufwerk)  | /dev/tmscsi/mt3  |
| Speicheragent zu einem Laufwerk, wenn das Laufwerk ein logisches Laufwerk in einem FILE-Kassettenarchiv ist | FILE   |
| NAS-Einheit zum Versetzen von Daten zu einem Laufwerk   | NetApp NAS-Dateiserver: rst01<br>EMC Celerra NAS-Dateiserver: c436t011<br>IBM System Storage N Series: rst01 |



 Die Quelle verwendet den Einheitenamen für den Zugriff auf das Laufwerk. Für Beispiele siehe Tabelle 3.

Tabelle 3. Beispiele für Einheitenamen

| Quelle zum Ziel   | Beispiel  |
|---|---|
| Server zu einem Laufwerk (kein FILE-Laufwerk)   |  Windows-Betriebssysteme\mt3 |
| Server zu einem Laufwerk (REMOVABLEFILE-Laufwerk)   | e:  |
| Speicheragent zu einem Laufwerk (kein FILE-Laufwerk)  | mt3   |
| Speicheragent zu einem Laufwerk, wenn das Laufwerk ein logisches Laufwerk in einem FILE-Kassettenarchiv ist | FILE  |
| NAS-Einheit zum Versetzen von Daten zu einem Laufwerk   | NetApp NAS-Dateiserver: rst01<br>EMC Celerra NAS-Dateiserver: c436t011<br>IBM System Storage N Series: rst01      |

Wichtig:

- Für 349X-Kassettenarchive ist der Aliasname ein symbolischer Name, der in der Datei `/etc/ibmatl.conf` angegeben ist. Weitere Informationen enthält das Handbuch *IBM Tape Device Drivers Installation and User's Guide*, das von der Site der IBM Systemunterstützung unter <http://www.ibm.com/support/docview.wss?uid=ssg1S7002972> heruntergeladen werden kann.
- Informationen über Namen für Einheiten, die mit einem NAS-Dateiserver verbunden sind, enthält die Produktinformation für den Dateiserver. Beispiel: Stellen Sie für einen NetApp-Dateiserver unter Verwendung von Telnet eine Verbindung zu dem Dateiserver her und geben Sie den Befehl `SYSCONFIG` aus. Verwenden Sie diesen Befehl, um Einheitennamen für Laufwerke zu bestimmen:

```
sysconfig -t
```

#### ONLine

Gibt an, ob der Pfad für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei. Gültige Werte:

Yes

Gibt an, dass der Pfad für die Verwendung verfügbar ist.

No

Gibt an, dass der Pfad nicht für die Verwendung verfügbar ist.

Die Quelle und das Ziel müssen verfügbar sein, um den Pfad verwenden zu können.

Ist beispielsweise der Pfad von einer Einheit zum Versetzen von Daten zu einem Laufwerk online, aber ist entweder die Einheit zum Versetzen von Daten oder das Laufwerk offline, kann der Pfad nicht verwendet werden.

#### DIRectory


Gibt die Verzeichnisposition(en) für einen Speicheragenten für den Zugriff auf die Dateien in einem FILE-Kassettenarchiv an. Der Parameter `DIRECTORY` wird auch für Einheiten des Typs `REMOVABLEFILE` verwendet. Für Einheiten des Typs `REMOVABLEFILE` stellt der Parameter `DIRECTORY` in Verbindung mit dem Parameter `DRIVE` dem Server (kein Speicheragent) Informationen zur Verfügung, die den Zugriff auf die Einheit beschreiben. Dieser Parameter ist wahlfrei.

Auf Speicheragenten ist dieser Parameter nur gültig, wenn *alle* folgenden Bedingungen zutreffen:

- Der Quellentyp ist `SERVER` (d. h., ein Speicheragent, der für diesen Server als Server definiert wurde).
- Der Quellename ist der Name eines Speicheragenten, *nicht* der Servername.
- Das Ziel ist ein logisches Laufwerk, das Teil eines FILE-Kassettenarchivs ist.
- Wurden mehrere Verzeichnisse für die Einheitenklasse angegeben, die dem FILE-Kassettenarchiv zugeordnet ist, muss dieselbe Anzahl Verzeichnisse mit dem Parameter `DIRectory` des Befehls `DEFINE PATH` für jedes Laufwerk in dem FILE-Kassettenarchiv angegeben werden. Verzeichnisse des Speicheragenten werden auf dem Server nicht geprüft. Werden falsche Verzeichnisse angegeben, kann dies einen Laufzeitfehler verursachen.

Der Verzeichnisname/die Verzeichnisnamen identifiziert/identifizieren die Position(en), an der/denen der Speicheragent die Dateien liest und schreibt, die Speicherdatenträger für die Einheitenklasse `FILE` darstellen, die dem FILE-Kassettenarchiv zugeordnet ist. Der Standardwert für `DIRECTORY` ist das Verzeichnis des Servers zum Zeitpunkt der Befehlsausgabe.

Verwenden Sie eine Namenskonvention, mit der Sie das Verzeichnis einem bestimmten physischen Laufwerk zuordnen können. Damit kann sichergestellt werden, dass Ihre Konfiguration für die gemeinsame Benutzung des FILE-Kassettenarchivs zwischen dem Server und dem Speicheragenten gültig ist. Befindet sich der Speicheragent auf einem Windows-System, verwenden Sie eine allgemeine Namenskonvention. Verfügt der Speicheragent nicht über die Berechtigung für den Zugriff auf fernen Speicher, treten Mountfehler im Speicheragenten auf.

 **Windows-Betriebssysteme** Das dem Speicheragentendienst zugeordnete Konto muss ein Konto in der Gruppe der lokalen Administratoren oder ein Konto in der Gruppe der Domänenadministratoren sein. Befindet sich das Konto in der Gruppe der lokalen Administratoren, müssen Benutzer-ID und Kennwort den Angaben eines Kontos entsprechen, das über Berechtigungen für den Zugriff auf Speicher verfügt, der von der Maschine bereitgestellt wird, die den fernen Sharepunkt verwaltet. Wenn beispielsweise ein SAMBA-Server Zugriff auf fernen Speicher bereitstellt, müssen Benutzer-ID und Kennwort in der SAMBA-Konfiguration der Benutzer-ID und dem Kennwort des lokalen Administrators entsprechen, der dem Speicheragentendienst zugeordnet ist.

```
define devclass file devtype=file shared=yes mountlimit=1
directory=d:\filedir\dir1
define path stal file1 srctype=server desttype=drive
library=file1 device=file directory=\\192.168.1.10\filedir\dir1
```


In dem vorherigen Beispiel baut der Befehl `DEFINE DEVCLASS` das gemeinsam genutzte Dateisystem in dem Verzeichnis auf, auf das der Server als `D:\FILEDIR\DIR1` zugreift. Der Speicheragent verwendet jedoch den UNC-Namen `\\192.168.1.10\FILEDIR\DIR1`. Das bedeutet, dass die Maschine mit TCP/IP-Adresse `192.168.1.10` dasselbe Verzeichnis gemeinsam nutzt, wobei `FILEDIR` als gemeinsam genutzter Name verwendet wird. Außerdem verfügt der Speicheragentendienst über ein Konto, das auf diesen Speicher zugreifen kann. Der Zugriff ist möglich, weil das Konto einem lokalen Konto mit derselben Benutzer-ID und demselben Kennwort wie `192.168.1.10` zugeordnet ist oder weil es einem Domänenkonto zugeordnet ist, das

sowohl auf dem Speicheragenten als auch auf 192.168.1.10 verfügbar ist. Sie können gegebenenfalls 192.168.1.10 durch einen symbolischen Namen wie folgt ersetzen:

Beispiel.IhreFirma.com

Wichtig:


- IBM Spectrum Protect erstellt keine Shares oder Berechtigungen und lädt nicht das Zielsystem. Sie müssen diese Aktionen ausführen, bevor der Speicheragent gestartet wird.
- Sie können eine Verzeichnisliste nur ändern, indem Sie die gesamte Liste ersetzen.
- Sie müssen sicherstellen, dass Speicheragenten auf neu erstellte FILE-Datenträger zugreifen können. Für den Zugriff auf FILE-Datenträger ersetzen Speicheragenten Namen aus der Verzeichnisliste in der Einheitenklassendefinition durch die Namen in der Verzeichnisliste für die zugeordnete Pfaddefinition. Der folgende Abschnitt verdeutlicht die Bedeutung übereinstimmender Einheitenklassen und Pfade, um sicherzustellen, dass Speicheragenten auf neu erstellte FILE-Datenträger zugreifen können.

Beispiel: Sie möchten folgende drei Verzeichnisse für ein FILE-Kassettenarchiv verwenden:  Windows-Betriebssysteme

- o c:\server
- o d:\server
- o e:\server

 AIX-Betriebssysteme  Linux-Betriebssysteme


- o /opt/tivoli1
- o /opt/tivoli2
- o /opt/tivoli3

1. Sie verwenden den folgenden Befehl, um ein FILE-Kassettenarchiv mit dem Namen CLASSA mit einem Laufwerk mit dem Namen CLASSA1 auf SERVER1 zu definieren:  Windows-Betriebssysteme


```
define devclass classa devtype=file
directory="c:\server,d:\server,e:\server"
shared=yes mountlimit=1
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

```
define devclass classa devtype=file
directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
shared=yes mountlimit=1
```



2. Sie wollen, dass der Speicheragent STA1 das FILE-Kassettenarchiv verwenden kann. Daher definieren Sie folgenden Pfad für Speicheragent STA1:  Windows-Betriebssysteme


```
define path server1 stal srctype=server desttype=drive device=file
directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
\\192.168.1.10\e\server" library=classa
```

 Windows-Betriebssysteme In diesem Szenario ersetzt der Speicheragent STA1 den Verzeichnisnamen c:\server durch den Verzeichnisnamen \\192.168.1.10\c\server, um auf FILE-Datenträger zuzugreifen, die sich in dem Verzeichnis c:\server auf dem Server befinden.

 AIX-Betriebssysteme  Linux-Betriebssysteme



```
define path server1 stal srctype=server desttype=drive device=file
directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
```

 AIX-Betriebssysteme  Linux-Betriebssysteme In diesem Szenario ersetzt der Speicheragent STA1 den Verzeichnisnamen /opt/tivoli1 durch den Verzeichnisnamen /opt/ibm1/, um auf FILE-Datenträger zuzugreifen, die sich in dem Verzeichnis /opt/tivoli1 auf dem Server befinden.

3.  Windows-Betriebssysteme FILE-Datenträger c:\server\file1.dsm wird durch SERVER1 erstellt. Wenn Sie das erste Verzeichnis für die Einheitenklassen später mit folgendem Befehl ändern:

```
update devclass classa directory="c:\otherdir,d:\server,e:\server"
```

kann SERVER1 weiterhin auf FILE-Datenträger c:\server\file1.dsm zugreifen, der Speicheragent STA1 jedoch nicht, weil in der PATH-Verzeichnisliste kein übereinstimmender Verzeichnisname mehr vorhanden ist. Ist kein Verzeichnisname in der Verzeichnisliste verfügbar, die der Einheitenklasse zugeordnet ist, kann der Speicheragent den Zugriff auf einen FILE-Datenträger in diesem Verzeichnis verlieren. Obwohl der Server zum Lesen noch auf den Datenträger zugreifen kann, kann der fehlgeschlagene Zugriff des Speicheragenten auf den FILE-Datenträger dazu führen, dass Operationen nur auf einem LAN-Pfad wiederholt werden können oder dass sie fehlschlagen.

4.  AIX-Betriebssysteme  Linux-Betriebssysteme Wird der FILE-Datenträger /opt/tivoli1/file1.dsm auf SERVER1 erstellt und wird der Befehl

```
update devclass classa directory="/opt/otherdir,/opt/tivoli2,
/opt/tivoli3"
```

ausgegeben, kann *SERVER1* weiterhin auf FILE-Datenträger */opt/tivoli1/file1.dsm* zugreifen, der Speicheragent *STA1* jedoch nicht, weil in der PATH-Verzeichnisliste kein übereinstimmender Verzeichnisname mehr vorhanden ist. Ist kein Verzeichnisname in der Verzeichnisliste verfügbar, die der Einheitenklasse zugeordnet ist, kann der Speicheragent den Zugriff auf einen FILE-Datenträger in diesem Verzeichnis verlieren. Obwohl der Server zum Lesen noch auf den Datenträger zugreifen kann, kann der fehlgeschlagene Zugriff des Speicheragenten auf den FILE-Datenträger dazu führen, dass Operationen nur auf einem LAN-Pfad wiederholt werden können oder dass sie fehlschlagen.

## Beispiel: Einen Pfad von einer Einheit zum Versetzen von Daten, die ein NAS-Dateiserver ist, zu einem Bandlaufwerk aktualisieren

---

Einen Pfad von einer Einheit zum Versetzen von Daten, die ein NAS-Dateiserver ist, zu dem Laufwerk *TAPEDRV2* aktualisieren, das von der Einheit zum Versetzen von Daten für Sicherungs- und Zurückschreibungsoperationen verwendet wird. In diesem Beispiel hat die NAS-Einheit zum Versetzen von Daten den Namen *NAS1*, das Kassettenarchiv ist *NASLIB* und der Einheitenname für das Laufwerk lautet *rst0l*.

```
update path nas1 tapedrv2 srctype=datamover desttype=drive library=naslib
device=rst0l
```

## UPDATE PATH (Pfad ändern, wenn das Ziel ein Kassettenarchiv ist)

---

Verwenden Sie diese Syntax, wenn Sie die Definition eines Pfads zu einem Kassettenarchiv aktualisieren.

### Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

### Syntax

---

```
>>-UPDate PATH--Quellename--Zielname----->
>--SRCType-----+DATAMover-+-----+----->
      '-SERVer----'  '-AUTODetect-----+No--+-'
                          '-Yes-'
>--DESTType-----LIBRARY-+-----+----->
      +-DEVIce-----Einheitenname-----+
      '-EXTERNALManager-----Pfadname-'
>+-----+-----><
  '-ONLine-----+Yes--+-'
      '-No--'
```

### Parameter

---

#### Quellename (Erforderlich)

Gibt den Namen der Quelle des Pfads an. Dieser Parameter ist erforderlich.

#### Zielname (Erforderlich)

Gibt den Namen des Ziels an. Dieser Parameter ist erforderlich.

Wichtig: Um einen Pfad von einer NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv zu definieren, muss das Kassettenarchiv den Typ (LIBTYPE) SCSI, 349X oder Automated Cartridge System Library Software (ACSL) haben.

#### SRCType (Erforderlich)

Gibt den Typ der Quelle an. Dieser Parameter ist erforderlich. Gültige Werte:

##### DATAMover

Gibt an, dass eine Einheit zum Versetzen von Daten die Quelle ist.

##### SERVer

Gibt an, dass ein Server oder ein Speicheragent die Quelle ist.

#### AUTODetect

Gibt an, ob die Seriennummer für ein Laufwerk oder Kassettenarchiv automatisch in IBM Spectrum Protect erkannt, gemeldet und aktualisiert wird. Dieser Parameter ist wahlfrei. Dieser Parameter ist nur für Pfade gültig, die von dem lokalen Server zu einem



Kassettenarchiv definiert sind. Gültige Werte:

No

Gibt an, dass die Seriennummer nicht automatisch aktualisiert wird.

Yes

Gibt an, dass die Seriennummer automatisch aktualisiert wird, um dieselbe Seriennummer widerzuspiegeln, die das Laufwerk an IBM Spectrum Protect meldet.

Wichtig:

1. Wurde zuvor keine Seriennummer eingegeben, erhält AUTODETECT den Standardwert YES. Wurde zuvor eine Seriennummer eingegeben, erhält AUTODETECT den Standardwert NO.
2. AUTODETECT=YES in diesem Befehl überschreibt die Seriennummer, die in dem Befehl DEFINE DRIVE definiert wurde.
3. Je nach Leistungsspektrum der Einheit wird der Parameter AUTODETECT möglicherweise nicht unterstützt.

DESTType=LIBRARY (Erforderlich)

Gibt an, dass ein Kassettenarchiv das Ziel ist. Dieser Parameter ist erforderlich.

DEVICE

Gibt den Namen der Einheit an, die der Quelle bekannt ist, oder FILE an, wenn die Einheit ein logisches Laufwerk in einem Kassettenarchiv FILE ist.




 Die Quelle verwendet den Einheitennamen für den Zugriff auf das Laufwerk oder das Kassettenarchiv. Für Beispiele siehe Tabelle 1.

Tabelle 1. Beispiele für Einheitennamen

| Quelle zum Ziel  | Beispiel  |
|--|---|
| Server zu einem Kassettenarchiv                              |  /dev/lb4<br> /dev/tmscsi/lb4 |
| NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv | mc0   |


 Die Quelle verwendet den Einheitennamen für den Zugriff auf das Laufwerk oder das Kassettenarchiv. Für Beispiele siehe Tabelle 2.

Tabelle 2. Beispiele für Einheitennamen

| Quelle zum Ziel  | Beispiel        |
|--|-----------------|
| Server zu einem Kassettenarchiv                              | /dev/tmscsi/lb4 |
| NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv | mc0             |



 Die Quelle verwendet den Einheitennamen für den Zugriff auf das Laufwerk oder das Kassettenarchiv. Für Beispiele siehe Tabelle 3.

Tabelle 3. Beispiele für Einheitennamen


| Quelle zum Ziel  | Beispiel  |
|--|---|
| Server zu einem Kassettenarchiv                              |  lb4.1 |
| NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv | mc0   |

Wichtig:

- Für 349X-Kassettenarchive ist der Aliasname ein symbolischer Name, der in der Datei /etc/ibmatl.conf angegeben ist. Weitere Informationen enthält das Handbuch *IBM Tape Device Drivers Installation and User's Guide*, das von der Site der IBM® Systemunterstützung unter <http://www.ibm.com/support/docview.wss?uid=ssg1S7002972> heruntergeladen werden kann.
- Informationen über Namen für Einheiten, die mit einem NAS-Dateiserver verbunden sind, enthält die Produktinformation für den Dateiserver. Beispiel: Stellen Sie für einen NetApp-Dateiserver unter Verwendung von Telnet eine Verbindung zu dem Dateiserver her und geben Sie den Befehl SYSCONFIG aus. Verwenden Sie diesen Befehl, um den Einheitennamen für ein Kassettenarchiv zu bestimmen:

```
sysconfig -m
```

EXTERNALManager

Gibt den Standort des externen Kassettenarchivmanagers an, an den IBM Spectrum Protect Zugriffsanforderungen für Datenträger senden kann. Der Wert dieses Parameters muss zwischen einfachen Anführungszeichen stehen. Geben Sie beispielsweise Folgendes ein: 

```
/usr/lpp/GEsedt-acsls/bin/elmdt
```



```
/opt/GEsedt-acsls/bin/elmdt
```



# UPDATE POLICYSET (Beschreibung einer Maßnahmengruppe aktualisieren)

Mit diesem Befehl kann die Beschreibung einer Maßnahmengruppe geändert werden. Die Beschreibung der aktiven (ACTIVE) Maßnahmengruppe kann nicht geändert werden.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Maßnahmengruppe gehört.

## Syntax

```
>>-UPDate Policyset--Domänenname--Name_der_Maßnahmengruppe----->
>>-DESCRiption--==--Beschreibung----->><
```

## Parameter

Domänenname (Erforderlich)

Gibt die Maßnahmendomäne an, zu der die Maßnahmengruppe gehört.

Name\_der\_Maßnahmengruppe (Erforderlich)

Gibt die Maßnahmengruppe an, die aktualisiert werden soll. Die aktive Maßnahmengruppe (ACTIVE) kann nicht geändert werden.

DESCRIPTION (Erforderlich)

Gibt den Text an, der die Maßnahmengruppe beschreibt. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Soll eine zuvor definierte Beschreibung gelöscht werden, ist eine Nullzeichenfolge ("" ) anzugeben.

## Beispiel: Eine Maßnahmengruppe aktualisieren

Für die Maßnahmengruppe VACATION (Maßnahmendomäne EMPLOYEE\_RECORDS) soll die Beschreibung "Schedule Planning Information" vergeben werden.

```
update policyset employee_records vacation
description="schedule planning information"
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE POLICYSET

| Befehl             | Beschreibung  |
|--------------------|---|
| ACTIVATE POLICYSET | Wertet eine Maßnahmengruppe aus und aktiviert sie.  |
| COPY MGMTCLASS     | Erstellt eine Kopie einer Verwaltungsklasse.  |
| DEFINE DOMAIN      | Definiert eine Maßnahmendomäne, der Clients zugeordnet werden können.   |
| DEFINE MGMTCLASS   | Definiert eine Verwaltungsklasse.   |
| DEFINE POLICYSET   | Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.   |
| DELETE POLICYSET   | Löscht eine Maßnahmengruppe einschließlich ihrer Verwaltungsklassen und Kopiengruppen aus einer Maßnahmendomäne.        |
| QUERY POLICYSET    | Zeigt Informationen über Maßnahmengruppen an.   |
| VALIDATE POLICYSET | Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert. |

## UPDATE PROFILE (Profilbeschreibung aktualisieren)

Mit diesem Befehl kann auf einem Konfigurationsmanager eine Profilbeschreibung aktualisiert werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-UPDate PROFIle--Profilname--DESCription-----Beschreibung----><
```

## Parameter

Profilname (Erforderlich)

Gibt das Profil an, das aktualisiert werden soll.

DESCription (Erforderlich)

Gibt eine Beschreibung für das Profil an. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Soll eine Beschreibung entfernt werden, eine Nullzeichenfolge ("" ) angeben.

## Beispiel: Die Beschreibung eines Profils aktualisieren

Die Beschreibung für Profil DELTA aktualisieren.

```
update profile delta description="PAYROLL domain"
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE PROFILE

| Befehl                 | Beschreibung  |
|------------------------|---|
| COPY PROFILE           | Erstellt eine Kopie eines Profils.  |
| DEFINE PROFASSOCIATION | Ordnet Objekte einem Profil zu.   |
| DEFINE PROFILE         | Definiert ein Profil für die Verteilung von Informationen an verwaltete Server. |
| DELETE PROFASSOCIATION | Löscht die Zuordnung zwischen einem Objekt und einem Profil.                    |
| DELETE PROFILE         | Löscht ein Profil aus einem Konfigurationsmanager.                              |
| LOCK PROFILE           | Verhindert die Verteilung eines Konfigurationsprofils.                          |
| QUERY PROFILE          | Zeigt Informationen über Konfigurationsprofile an.                              |
| SET CONFIGMANAGER      | Gibt an, ob ein Server ein Konfigurationsmanager ist.                           |
| UNLOCK PROFILE         | Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server.        |

## UPDATE RECOVERYMEDIA (Wiederherstellungsdatenträger aktualisieren)

Mit diesem Befehl können Informationen über Wiederherstellungsdatenträger aktualisiert werden.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-UPDate RECOVERYMedia--Datenträgername----->
>+-----+
|           .-,------. |
|           v             | |
| '-VOLumentnames-----Datenträgername-+-'
>+-----+>
```



## UPDATE REPLRULE (Replikationsregeln aktualisieren)

Verwenden Sie diesen Befehl, um eine Replikationsregel zu aktivieren oder zu inaktivieren.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-UPDate REPLRule--RegelName----State-----+ENabled--+-----<<  
                                     '-DISabled-'
```

### Parameter

Regelname (Erforderlich)

Gibt den Namen der Replikationsregel an, die aktualisiert werden soll. Sie können Platzhalterzeichen verwenden, um eine oder mehrere Regeln anzugeben. Sie können eine der folgenden Regeln angeben:

- ALL\_DATA
- ACTIVE\_DATA
- ALL\_DATA\_HIGH\_PRIORITY
- ACTIVE\_DATA\_HIGH\_PRIORITY

SState (Erforderlich)

Gibt an, ob die Replikation für die Regel zulässig ist. Sie können einen der folgenden Werte angeben:

ENabled

Gibt an, dass die Daten, für die die Regel gilt, für die Replikation bereit sind.

DISabled

Gibt an, dass die Replikation erst stattfindet, wenn sie aktiviert wurde.

### Beispiel: Die Replikation für Sicherungsdaten inaktivieren

Die Replikation von aktiven Sicherungsdaten mit normaler Priorität für alle Dateibereiche in allen Clientknoten inaktivieren, die für die Replikation konfiguriert sind.

```
update replrule active_data state=disabled
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE REPLRULE

| Befehl                | Beschreibung  |
|-----------------------|---|
| QUERY FILESPACE       | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.   |
| QUERY NODE            | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an. |
| QUERY REPLICATION     | Zeigt Informationen zu Knotenreplikationsprozessen an.                            |
| QUERY REPLRULE        | Zeigt Informationen zu Knotenreplikationsregeln an.                               |
| SET ARREPLRULEDEFAULT | Gibt die Serverknotenreplikationsregel für Archivierungsdaten an.                 |
| SET BKREPLRULEDEFAULT | Gibt die Serverknotenreplikationsregel für Sicherungsdaten an.                    |
| SET SPREPLRULEDEFAULT | Gibt die Serverknotenreplikationsregel für speicher verwaltete Daten an.          |
| UPDATE FILESPACE      | Ändert Knotenreplikationsregeln für Dateibereiche.                                |
| UPDATE NODE           | Ändert die Attribute, die einem Clientknoten zugeordnet sind.                     |

| Befehl               | Beschreibung  |
|----------------------|---|
| VALIDATE REPLICATION | Überprüft die Replikation für Dateibereiche und Datentypen. |

## UPDATE SCHEDULE (Zeitplan aktualisieren)

Mit diesem Befehl kann ein Zeitplan für einen Client oder Verwaltungsbefehl aktualisiert werden.

Der Befehl UPDATE SCHEDULE kann zwei Formen haben, je nachdem, ob der Zeitplan Client-Operationen oder Verwaltungsbefehle betrifft. Innerhalb dieser beiden Formen können Sie entweder Zeitpläne mit klassischer Darstellung oder Zeitpläne mit erweiterter Darstellung auswählen. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für UPDATE SCHEDULE

| Befehl                | Beschreibung  |
|-----------------------|---|
| COPY SCHEDULE         | Erstellt eine Kopie eines Zeitplans.  |
| DEFINE SCHEDULE       | Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl.   |
| DELETE SCHEDULE       | Löscht einen Zeitplan aus der Datenbank.  |
| QUERY EVENT           | Zeigt Informationen über geplante und abgeschlossene Ereignisse für ausgewählte Clients an.                             |
| QUERY SCHEDULE        | Zeigt Informationen über Zeitpläne an.  |
| SET MAXCMDRETRIES     | Gibt die maximale Anzahl Wiederholungen nach der fehlgeschlagenen Ausführung eines geplanten Befehls an.                |
| SET MAXSCHEDESESSIONS | Gibt die maximale Anzahl Client-/Serversitzungen an, die bei der Arbeit mit einem Verarbeitungszeitplan verfügbar sind. |
| SET RETRYPERIOD       | Gibt die Zeitspanne zwischen Wiederholungsversuchen des Client-Schedulers an.   |

- UPDATE SCHEDULE (Clientzeitplan aktualisieren)  
Mit dem Befehl UPDATE SCHEDULE können ausgewählte Parameter für einen Clientzeitplan aktualisiert werden.
- UPDATE SCHEDULE (Verwaltungszeitplan aktualisieren)  
Mit diesem Befehl können ausgewählte Parameter für einen Verwaltungszeitplan aktualisiert werden.

## UPDATE SCHEDULE (Clientzeitplan aktualisieren)

Mit dem Befehl UPDATE SCHEDULE können ausgewählte Parameter für einen Clientzeitplan aktualisiert werden.

Dieser Befehl ändert nicht die Clientzuordnungen, die für diesen Zeitplan vorgenommen wurden. Alle dem Originalzeitplan zugeordneten Clients verarbeiten den geänderten Zeitplan.

Nicht alle Clients können alle geplanten Operationen ausführen, auch wenn Sie den Zeitplan auf dem Server definieren und ihn dem Client zuordnen können. Ein Macintosh-Client kann beispielsweise keinen Zeitplan ausführen, wenn es sich bei der Aktion um das Zurückschreiben oder Abrufen von Dateien oder um das Ausführen einer ausführbaren Prozedur handelt. Eine ausführbare Prozedur wird auch als Befehlsdatei, Stapeldatei oder Prozedur auf anderen Client-Betriebssystemen bezeichnet.

### Berechtigungsklasse

Zum Aktualisieren eines Clientzeitplans ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der der Zeitplan gehört.

### Syntax für einen klassischen Clientzeitplan

```

(1)
>>-UPDate SChedule-----Domänenname--Zeitplanname----->
>-+-----+-----+-----+-----+----->
  '-Type----Client-'  '-DESCription----Beschreibung-'
>-+-----+-----+-----+-----+----->
  '-ACTion----+Incremental-----+----->

```

```

+-Selective-----+
+-Archive-----+
|               | .-"-----| |
|               | '-SUBAction--'+-----+ |
|               |         '-FASTBack-' |
+-Backup-----+
|               | .-"-----| |
|               | '-SUBAction--'+-----+ |
|               |         +-FASTBack----+ |
|               |         +-SYSTEMState-+ |
|               |         '-VM-----' |
+-REStore-----+
+-REtrieve-----+
+-IMAGEBACKup-----+
+-IMAGERESTore-----+
+-Command-----+
+-Macro-----+
'-Deploy-----'

>----->
'-OPTions--Optionszeichenfolge-'

>----->
'-OBJects--Objektzeichenfolge-' '-PRIority--Zahl-'

>----->
'-STARTDate--Datum-' '-STARTTime--Zeit-'

>----->
'-DURation--Zahl-' '-DURUnits--Minutes-'
|               |         +-Hours-----+
|               |         +-Days-----+
|               |         '-INDefinite-'

>----->
'-MAXRUNtime--Anzahl-' '-SCHEDStyle--Classic-'

>----->
'-PERiod--Zahl-' '-PERUnits--Hours-'
|               |         +-Days-----+
|               |         +-Weeks----+
|               |         +-Months---+
|               |         +-Years---+
|               |         '-Onetime-'

>----->
'-DAYofweek--ANY-'
|               |         +-WEEKDay---+
|               |         +-WEEKEnd---+
|               |         +-Sunday----+
|               |         +-Monday----+
|               |         +-Tuesday---+
|               |         +-Wednesday-+
|               |         +-Thursday--+
|               |         +-Friday---+
|               |         '-SATurday--'

>-----<
'-EXPIration--Never-+'
|               |         '-Datum-'

```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.

## Syntax für einen erweiterten Clientzeitplan

```

(1)
>>-UPDate SCHEDULE-----Domänenname--Zeitplanname----->
>----->
'-Type--Client-' '-DESCription--Beschreibung-'

>----->
'-ACTion--Incremental-----+-'

```



```

+-Selective-----+
+-Archive-----+
|           '-SUBACTion--==+'-'-----+' |
|                                     '-FASTBack-' |
+-Backup-----+
|           '-SUBACTion--==+'-'-----+' |
|                                     +-FASTBack----+ |
|                                     +-SYSTEMState-+ |
|                                     +-VApp-----+ |
|                                     '-VM-----' |
+-REStore-----+
+-RETRieve-----+
+-IMAGEBACKup-----+
+-IMAGERESStore-----+
+-Command-----+
'-Macro-----'

>----->
'-OPTions---Optionszeichenfolge-'

>----->
'-OBJects---Objektzeichenfolge-' '-PRIority---Zahl-'

>----->
'-STARTDate---Datum-' '-STARTTime---Zeit-'

>----->
'-DURation---Zahl-' '-DURUnits---Minutes-+-'
|                                     +-Hours---+
|                                     '-Days---'

>----->
'-MAXRUNtime---Anzahl-' '-SCHEDStyle---Enhanced-'

>----->
'-MONth---ANY-----+' '-DAYOFMonth---ANY-+-'
|   +-JANuary---+ |           '-Day-'
|   +-February---+
|   +-MARch-----+
|   +-APril-----+
|   +-May-----+
|   +-JUNe-----+
|   +-JULy-----+
|   +-AUGust-----+
|   +-September-+
|   +-October---+
|   +-November---+
|   '-December--'

>----->
'-WEEKofmonth---ANY-----+'
|   +-First---+
|   +-Second---+
|   +-Third---+
|   +-FOurth---+
|   '-Last---'

>----->
'-DAYofweek---ANY-----+'
|   +-WEEKDay---+
|   +-WEEKEnd---+
|   +-SUnday----+
|   +-Monday----+
|   +-TUESday---+
|   +-Wednesday-+
|   +-THursday--+
|   +-Friday---+
|   '-SATurday--'

>-----<
'-EXPIration---Never-+-'
|   '-Datum-'

```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.

## Parameter

---

### Domänenname (Erforderlich)

Gibt den Namen der Maßnahmendomäne an, zu der dieser Zeitplan gehört.

### Zeitplanname (Erforderlich)

Gibt den Namen des Zeitplans an, der aktualisiert werden soll.

### Type=Client

Gibt an, daß ein Client-Zeitplan aktualisiert wird. Dieser Parameter ist wahlfrei. Der Standardwert ist CLIENT.

### DESCRiption

Gibt eine Beschreibung des Zeitplans an. Dieser Parameter ist wahlfrei. Für die Beschreibung können bis zu 255 Zeichen angegeben werden. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Soll eine zuvor definierte Beschreibung gelöscht werden, ist eine leere Zeichenfolge ("" ) anzugeben.

### ACTiOn

Gibt die Aktion an, die bei der Verarbeitung dieses Zeitplans ausgeführt wird. Gültige Werte:

#### Incremental

Gibt an, daß der Zeitplan alle Dateien sichert, die neu sind oder sich seit der letzten Teilsicherung geändert haben. Mit "Incremental" werden auch alle Dateien gesichert, für die alle vorhandenen Sicherungen möglicherweise verfallen sind.

#### Selective

Gibt an, daß der Zeitplan nur Dateien sichert, die mit dem Parameter OBJECTS angegeben werden.

#### Archive

Gibt an, daß der Zeitplan Dateien archiviert, die mit dem Parameter OBJECTS angegeben werden.

#### Backup

Gibt an, dass der Zeitplan Dateien sichert, die mit dem Parameter OBJECTS angegeben werden.

#### REStore

Gibt an, daß der Zeitplan Dateien zurückschreibt, die mit dem Parameter OBJECTS angegeben werden.

Wenn Sie ACTION=RESTORE für eine geplante Operation angeben, und ist die Option REPLACE auf PROMPT gesetzt, erfolgt keine Aufforderung. Wird die Option auf PROMPT gesetzt, werden die Dateien übersprungen.

Wenn Sie eine zweite Dateispezifikation angeben, agiert diese zweite Dateispezifikation als Zielort für die Zurückschreibung. Müssen mehrere Gruppen von Dateien zurückgeschrieben werden, planen Sie eine für jede Dateispezifikation, die zurückgeschrieben werden muss.

#### RETRieve

Gibt an, dass der Zeitplan Dateien abrufen, die mit dem Parameter OBJECTS angegeben werden.

Hinweis: Eine zweite Datei, die angegeben wird, dient als Abrufzielort. Müssen mehrere Gruppen von Dateien abgerufen werden, erstellen Sie einen separaten Zeitplan für jede Dateigruppe.

#### IMAGEBACKup

Gibt an, daß der Zeitplan logische Datenträger sichert, die mit dem Parameter OBJECTS angegeben werden.

#### IMAGERESStore

Gibt an, daß der Zeitplan logische Datenträger zurückschreibt, die mit dem Parameter OBJECTS angegeben werden.

#### Command

Gibt an, dass der Zeitplan einen Client-Betriebssystembefehl oder ein Script verarbeitet, der bzw. das mit dem Parameter OBJECTS angegeben wird.

#### Macro

Gibt an, daß ein Client ein Makro verarbeitet, dessen Dateiname im Parameter OBJECTS angegeben ist.

#### SUBACTiOn

Sie können einen der folgenden Werte angeben:

""

Wenn eine Nullzeichenfolge (zwei Anführungszeichen) mit ACTION=BACKUP angegeben wird, ist die Sicherung eine Teilsicherung.

#### FASTBACk

Gibt an, dass eine FastBack-Clientoperation, die durch den Parameter ACTION angegeben wird, für die Verarbeitung geplant werden soll. Der Wert des Parameters ACTION muss ARCHIVE oder BACKUP sein.

#### SYSTEMState

Gibt an, dass eine Clientsystemstatussicherung geplant ist.

#### VApp

Gibt an, dass eine vApp-Clientsicherung geplant ist. Eine vApp ist eine Sammlung von vorimplementierten virtuellen Maschinen.

#### VM

Gibt an, dass eine VMware-Clientsicherungsoperation geplant ist.

#### Deploy

Gibt an, ob Client-Workstations mit Implementierungspaketen aktualisiert werden sollen, die mit dem Parameter OBJECTS angegeben werden. Der Parameter OBJECTS muss zwei Spezifikationen enthalten: die Paketdateien, die abgerufen werden sollen, und die Position, an der sie abgerufen werden sollen. Stellen Sie sicher, dass die Objekte die Reihenfolge *Dateien Position* haben. Beispiel:

```
define schedule standard deploy_1 action=DEPLOY objects=  
"\\IBM_ANR_WIN\c$\tasm\maintenance\client\v6r2\Windows\X32\v620\v6200\*  
..\IBM_ANR_WIN\"
```

Die Werte für die folgenden Optionen sind eingeschränkt, wenn Sie ACTION=DEPLOY angeben:

#### PERUNITS

Geben Sie PERUNITS=ONETIME an. Wenn Sie PERUNITS=PERIOD angeben, wird der Parameter ignoriert.

#### DURUNITS

Geben Sie MINUTES, HOURS oder DAYS für den Parameter DURUNITS an. Geben Sie nicht INDEFINITE an.

#### SCHEDSTYLE

Geben Sie die Standarddarstellung CLASSIC an.


Der Befehl SCHEDULE schlägt fehl, wenn die Parameter nicht den erforderlichen Parameterwerten wie V.R.M.F entsprechen.

### OPTions

Gibt die Clientoptionen an, die für den geplanten Befehl angegeben werden, wenn der Zeitplan verarbeitet wird. Dieser Parameter ist wahlfrei.

Für diesen Parameter können nur die Optionen angegeben werden, die für den geplanten Befehl gültig sind. Informationen zu den Optionen, die in der Befehlszeile gültig sind, befinden sich im entsprechenden Clienthandbuch. Alle Optionen, für die im Clienthandbuch angegeben ist, dass sie nur in der Anfangsbefehlszeile gültig sind, führen zu einem Fehler oder werden ignoriert, wenn der Zeitplan vom Server ausgeführt wird. Geben Sie beispielsweise die folgenden Optionen nicht an, da sie keinen Einfluss darauf haben, wann der Client den geplanten Befehl verarbeitet:

- MAXCMDRETRIES
- OPTFILE
- QUERYSCHEDPERIOD
- RETRYPERIOD
- SCHEDLOGNAME
- SCHEDMODE
- SERVERNAME
- TCPCLIENTADDRESS
- TCPCLIENTPORT

 Windows-Betriebssysteme Wenn Sie einen Scheduler-Service definieren, indem Sie den Befehl DSMCUTIL oder den Assistenten für die GUI des Clients für Sichern/Archivieren verwenden, geben Sie eine Optionsdatei an. Sie können die Optionen in dieser Optionsdatei nicht überschreiben, indem Sie den geplanten Befehl ausgeben. Sie müssen die Optionen in Ihrem Schedulerservice ändern.

Enthält die Optionszeichenfolge mehrere Optionen oder Optionen mit eingebetteten Leerzeichen, schließen Sie die gesamte Optionszeichenfolge in Hochkommas ein. Schließen Sie einzelne Optionen, die Leerzeichen enthalten, in Anführungszeichen ein. Vor der Option muss ein führendes Minuszeichen stehen. Fehler können auftreten, wenn die Optionszeichenfolge Leerzeichen enthält, die nicht korrekt in Anführungszeichen eingeschlossen sind.

Die folgenden Beispiele zeigen, wie einige Clientoptionen angegeben werden:

- Geben Sie Folgendes ein, um `subdir=yes` und `domain all-local -systemobject` anzugeben:
  - `options='-subdir=yes -domain="all-local -c: -systemobject"'`
- Geben Sie Folgendes ein, um `domain all-local -c: -d:` anzugeben:
  - `options='-domain="all-local -c: -d:"'`

 Windows-Betriebssysteme Tipp:

Für Windows-Clients, die im Stapelbetrieb ausgeführt werden: Ist die Verwendung von Anführungszeichen erforderlich, verwenden Sie den Dialogmodus oder Escapezeichen des Betriebssystems. Weitere Informationen liefern die folgenden Abschnitte:

- Eine Serie von Befehlen des Verwaltungsclients verarbeiten
- Einzelne Befehle mit dem Verwaltungsclient verarbeiten

### OBJects

Gibt die Objekte an, für die die angegebene Aktion ausgeführt wird. Verwenden Sie ein einzelnes Leerzeichen zwischen jedem Objekt. Außer bei ACTION=INCREMENTAL ist dieser Parameter erforderlich. Ist die Aktion eine Sicherungs-, Archivierungs-,

Abruf- oder Zurückschreibungsoperation, sind die Objekte Dateibereiche, Verzeichnisse oder logische Datenträger. Dient die Aktion zur Ausführung eines Befehls oder Makros, ist das Objekt der Name des auszuführenden Befehls oder Makros.

Wenn ACTION=INCREMENTAL ohne Angabe eines Werts für diesen Parameter angegeben wird, wird der geplante Befehl ohne angegebene Objekte aufgerufen, und der Befehl versucht, die Objekte wie in der Clientoptionsdatei definiert zu verarbeiten. Um alle Dateibereiche oder Verzeichnisse für eine Aktion auszuwählen, müssen sie explizit in der Objektzeichenfolge aufgeführt werden. Wird nur ein Stern in die Objektzeichenfolge eingegeben, erfolgt die Sicherung nur für das Verzeichnis, bei dem der Scheduler gestartet wurde.

Wichtig:

- Wenn Sie eine zweite Dateispezifikation angeben, und handelt es sich nicht um einen gültigen Zielort, empfangen Sie diesen Fehler:


```
ANS1082E Ungültige
Zieldateispezifikation <Dateispezifikation> eingegeben.
```

- Geben Sie mehr als zwei Dateispezifikationen an, empfangen Sie diesen Fehler:


```
ANS1102E Zu viele Befehlszeilenparameter an das Programm übergeben!
```

Wird für diesen Parameter ACTION=ARCHIVE, INCREMENTAL oder SELECTIVE angegeben, können Sie maximal 20 Dateispezifikationen auflisten.

Schließen Sie die Objektzeichenfolge in Anführungszeichen ein, wenn sie Leerzeichen enthält, und schließen Sie dann die Anführungszeichen in Hochkommas ein. Enthält die Objektzeichenfolge mehrere Dateinamen, schließen Sie jeden Dateinamen in Anführungszeichen ein und schließen Sie dann die gesamte Zeichenfolge in Hochkommas ein. Fehler können auftreten, wenn Dateinamen ein Leerzeichen enthalten, das nicht korrekt in Anführungszeichen eingeschlossen ist.

 Windows-Betriebssysteme Wenn Sie Zeichen verwenden, die für Windows-Benutzer eine besondere Bedeutung haben, wie z. B. Kommas, schließen Sie das gesamte Argument in doppelte Anführungszeichen ein und schließen Sie dann die gesamte Zeichenfolge in Hochkommas ein. Die folgenden Beispiele zeigen, wie einige Dateinamen angegeben werden:

- Geben Sie Folgendes ein, um C:\FILE 2, D:\GIF FILES und E:\MY TEST FILE anzugeben:
  - OBJECTS="\"C:\FILE 2\" \"D:\GIF FILES\" \"E:\MY TEST FILE\""
- Geben Sie Folgendes ein, um D:\TEST FILE anzugeben:
  - OBJECTS="\"D:\TEST FILE\""
- Geben Sie Folgendes ein, um D:TEST,FILE anzugeben:
  - OBJECTS="\"\"D:\TEST,FILE\"\""

 AIX-Betriebssysteme  Linux-Betriebssysteme Die folgenden Beispiele zeigen, wie einige Dateinamen angegeben werden:

- Geben Sie Folgendes ein, um /home/file 2, /home/gif files und /home/my test file anzugeben:
  - OBJECTS="\"/home/file 2\" \"/home/gif files\" \"/home/my test file\""
- Geben Sie Folgendes ein, um /home/test file anzugeben:
  - OBJECTS="\"/home/test file\""

 Windows-Betriebssysteme Tipp:

Für Windows-Clients, die im Stapelbetrieb ausgeführt werden: Ist die Verwendung von Anführungszeichen erforderlich, verwenden Sie den Dialogmodus oder Escapezeichen des Betriebssystems. Weitere Informationen liefern die folgenden Abschnitte:

- Eine Serie von Befehlen des Verwaltungsclients verarbeiten
- Einzelne Befehle mit dem Verwaltungsclient verarbeiten

#### PRIority

Gibt den Prioritätswert für einen Zeitplan an. Dieser Parameter ist wahlfrei. Zulässige Werte sind ganze Zahlen von 1 bis 10, wobei 1 die höchste Priorität und 10 die niedrigste Priorität angibt. Der Standardwert ist 5.

Wenn zwei oder mehr Zeitpläne dieselbe Fensterstartzeit haben, legt der angegebene Wert fest, wann IBM Spectrum Protect den Zeitplan verarbeitet. Der Zeitplan mit der höchsten Priorität startet zuerst. Ein Zeitplan mit PRIORITY=3 startet beispielsweise vor einem Zeitplan mit PRIORITY=5.

#### STARTDate

Gibt das Datum für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum. Diesen Parameter zusammen mit dem Parameter STARTTIME verwenden, um anzugeben, wann das Anfangsstartfenster des Zeitplans startet.

Sie können das Datum unter Verwendung der folgenden Werte angeben:

| Wert                            | Beschreibung  | Beispiel   |
|---------------------------------|---|--|
| MM/TT/JJJJ                      | Ein bestimmtes Datum  | 09/15/1998   |
| TODAY                           | Das aktuelle Datum  | TODAY  |
| TODAY+Tage <b>oder</b><br>+Tage | Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY +3 <b>oder</b> +3.   |
| EOLM (Ende des letzten Monats)  | Der letzte Tag des Vormonats.   | EOLM   |
| EOLM-Tage                       | Der letzte Tag des Vormonats minus angegebene Tage.   | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)     | Der erste Tag des aktuellen Monats.   | BOTM   |
| BOTM+Tage                       | Der erste Tag des aktuellen Monats plus angegebene Tage.  | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.      |

#### STARTTime

Gibt die Uhrzeit für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist die aktuelle Uhrzeit. Dieser Parameter gibt in Verbindung mit dem Parameter STARTDATE den Beginn des Anfangsstartfensters an.

Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

| Wert                             | Beschreibung   | Beispiel   |
|----------------------------------|--|--|
| HH:MM:SS                         | Eine bestimmte Uhrzeit   | 10:30:08   |
| NOW                              | Die aktuelle Uhrzeit   | NOW  |
| NOW+HH:MM <b>oder</b><br>+HH:MM  | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten  | NOW+02:00 <b>oder</b> +02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW+02:00 oder STARTTIME=+02:00 ausgegeben, beginnt das Startfenster um 7:00 Uhr. |
| NOW-HH:MM <b>oder</b> -<br>HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten | NOW-02:00 <b>oder</b> -02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW-02:00 oder STARTTIME=-02:00 ausgegeben, beginnt das Startfenster um 3:00 Uhr. |

#### DURation

Gibt die Anzahl Einheiten an, die die Länge des Startfensters der geplanten Operation definiert. Dieser Parameter ist wahlfrei. Dieser Wert muß zwischen 1 und 999 liegen. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter DURUNITS verwenden, um die Länge des Startfensters anzugeben. Werden beispielsweise DURATION=20 und DURUNITS=MINUTES angegeben, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Standardlänge des Startfensters beträgt 1 Stunde. Die Länge des Fensters muß kürzer sein, als der Zeitraum zwischen Fenstern.

Dieser Wert wird ignoriert, wenn DURUNITS=INDEFINITE angegeben wird.

Tipp: Definieren Sie Zeitpläne mit einer Dauer von mehr als 10 Minuten. Damit erhält der IBM Spectrum Protect-Scheduler genügend Zeit, den Zeitplan zu verarbeiten und den Client abzufragen.

#### DURUnits

Gibt die Zeiteinheiten an, mit denen die Dauer des Fensters bestimmt wird, in dem der Zeitplan starten kann. Dieser Parameter ist wahlfrei. Der Standardwert ist HOURS.

Diesen Parameter zusammen mit dem Parameter DURATION verwenden, um anzugeben, wie lange das Startfenster geöffnet bleibt, um den Zeitplan zu verarbeiten. Gilt beispielsweise DURATION=20 und DURUNITS=MINUTES, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Verarbeitung des Zeitplans muß nicht unbedingt innerhalb dieses Fensters enden. Wenn der Zeitplan aus irgendeinem Grund wiederholt werden muß, müssen die Wiederholungsversuche vor Ablauf des Startfensters beginnen; andernfalls wird die Operation nicht erneut gestartet.

Der Standardwert für die Länge des Startfensters ist 1 Stunde. Sie können einen der folgenden Werte angeben:

#### Minutes

Gibt an, daß die Dauer des Fensters in Minuten definiert wird.

#### Hours

Gibt an, daß die Dauer des Fensters in Stunden definiert wird.

#### Days

Gibt an, daß die Dauer des Fensters in Tagen definiert wird.

#### INDefinite

Gibt an, daß die Dauer des Startfensters der geplanten Operation unbegrenzt ist. Der Zeitplan kann bis zu seinem Verfall zu einem beliebigen Zeitpunkt nach der geplanten Startzeit ausgeführt werden. Sie können DURUNITS=INDEFINITE nur angeben, wenn Sie PERUNITS=ONETIME angeben. Der Wert INDEFINITE ist für erweiterte Zeitpläne nicht zulässig.

#### MAXRUNtime

Gibt die maximale Ausführungszeit an. Hierbei handelt es sich um die Anzahl Minuten, in denen alle Clientsitzungen, die von der geplanten Operation gestartet werden, abgeschlossen werden sollten. Sind Sitzungen nach Ablauf der maximalen Ausführungszeit noch aktiv, gibt der Server eine Warnung aus, aber die Ausführung der Sitzungen wird fortgesetzt.

Tipp: Die maximale Ausführungszeit wird ab dem Beginn des Startfensters und nicht ab der Zeit berechnet, zu der Sitzungen innerhalb des Startfensters gestartet werden.

Einschränkungen:

- Der Wert des Parameters wird nicht an Server verteilt, die von einem Manager für unternehmensweite Konfiguration verwaltet werden.
- Der Wert des Parameters wird nicht mit dem Befehl EXPORT exportiert.

Der Parameter ist wahlfrei. Sie können eine Zahl im Bereich von 0 bis 1440 angeben. Der Wert 0 bedeutet, dass die maximale Ausführungszeit unendlich ist und keine Warnung ausgegeben wird. Die maximale Ausführungszeit muss größer als die Dauer des Startfensters sein, die mit den Parametern DURATION und DURUNITS definiert wird.

Ist beispielsweise die Startzeit einer geplanten Operation 21:00 Uhr und beträgt die Dauer des Startfensters 2 Stunden, erstreckt sich das Startfenster von 21:00 Uhr bis 23:00 Uhr. Beträgt die maximale Ausführungszeit 240 Minuten (4 Stunden), sollten alle Clientsitzungen für diese Operation um 1:00 Uhr abgeschlossen sein. Sind eine oder mehrere Sitzungen nach 1:00 Uhr noch aktiv, gibt der Server eine Warnung aus.

Tipp: Alternativ können Sie den Wert 1:00 Uhr für *Ausführungszeitalert* im IBM Spectrum Protect Operations Center angeben.

#### SCHEDStyle

Dieser Parameter ist wahlfrei. SCHEDSTYLE definiert entweder das Intervall zwischen den Zeiten, zu denen ein Zeitplan ausgeführt werden kann, oder die Tage, an denen der Zeitplan ausgeführt werden kann. Die Darstellung kann entweder classic oder enhanced sein. Dieser Parameter muss angegeben werden, wenn Sie die Darstellung eines Zeitplans von klassisch in erweitert oder zurück in klassisch ändern. Andernfalls wird der Wert für den vorhandenen Zeitplan verwendet.

Für klassische Zeitpläne sind diese Parameter zulässig: PERIOD, PERUNITS und DAYOFWEEK. Diese Parameter sind nicht zulässig: MONTH, DAYOFMONTH und WEEKOFMONTH. War die vorherige Zeitplandarstellung erweitert, werden die Parameter MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK zurückgesetzt. DAYOFWEEK, PERIOD und PERUNITS werden auf die Standardwerte gesetzt, es sei denn, sie werden mit dem Aktualisierungsbefehl angegeben.

Für erweiterte Zeitpläne sind diese Parameter zulässig: MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK. Diese Parameter sind nicht zulässig: PERIOD und PERUNITS. War die vorherige Zeitplandarstellung klassisch, werden die Parameter DAYOFWEEK, PERIOD und PERUNITS zurückgesetzt. MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK werden auf die Standardwerte gesetzt, es sei denn, sie werden mit dem Aktualisierungsbefehl angegeben.

#### PERiod

Gibt den Zeitraum zwischen Startfenstern für diesen Zeitplan an. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Zulässige Werte sind ganze Zahlen von 1 bis 999. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter PERUNITS verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle fünf Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Zeitraum zwischen den Startfenstern muß länger sein als die Dauer jedes Fensters. Der Standardwert ist 1 Tag.

Dieser Wert wird ignoriert, wenn PERUNITS=ONETIME angegeben wird.

#### PERUnits

Gibt die Zeiteinheiten an, mit denen der Zeitraum zwischen Startfenstern für diesen Zeitplan bestimmt wird. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Der Standardwert ist DAYS.

Diesen Parameter zusammen mit dem Parameter PERIOD verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation

alle 5 Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Standardwert ist 1 Tag. Sie können einen der folgenden Werte angeben:

#### Hours

Gibt an, daß der Zeitraum zwischen Startfenstern in Stunden angegeben wird.

#### Days

Gibt an, daß der Zeitraum zwischen Startfenstern in Tagen angegeben wird.

#### Weeks

Gibt an, daß der Zeitraum zwischen Startfenstern in Wochen angegeben wird.

#### Months

Gibt an, daß der Zeitraum zwischen Startfenstern in Monaten angegeben wird.

Wird PERUNITS=MONTHS angegeben, wird die geplante Operation jeden Monat an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/04/1998 lautet, wird der Zeitplan danach am 4. jedes Monats verarbeitet. Wenn das Datum jedoch für den nächsten Monat nicht gültig ist, wird die geplante Operation am letzten gültigen Datum in dem Monat verarbeitet. Danach basieren nachfolgende Operationen auf diesem neuen Datum. Wenn das Startdatum beispielsweise 03/31/1998 lautet, wird die Operation des nächsten Monats für den 04/30/1998 geplant. Danach werden alle folgenden Operationen bis Februar am 30. des Monats ausgeführt. Da Februar nur 28 Tage hat, wird die Operation für das Datum 02/28/1999 geplant. Nachfolgende Operationen werden am 28. des Monats verarbeitet.

#### Years

Gibt an, daß der Zeitraum zwischen Startfenstern für den Zeitplan in Jahren angegeben wird.

Wird PERUNITS=YEARS angegeben, wird die geplante Operation jährlich in demselben Monat und an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/29/2004 lautet, wird die geplante Operation des nächsten Jahres am 02/28/2005 ausgeführt, da Februar nur 28 Tage hat. Danach werden folgende Operationen für den 28. Februar geplant.

#### Onetime

Gibt an, daß der Zeitplan einmal verarbeitet wird. Dieser Wert überschreibt den für den Parameter PERIOD angegebenen Wert.

#### DAYofweek

Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können verschiedene Optionen für den Parameter DAYofweek angeben, abhängig davon, ob die Zeitplandarstellung als 'Klassisch' oder 'Erweitert' definiert wurde:

##### Klassischer Zeitplan

Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können entweder einen Tag der Woche oder WEEKDAY, WEEKEND oder ANY angeben. Fallen Startdatum und Startzeit auf einen Tag, der nicht einem angegebenen Tag entspricht, werden das Startdatum und die Startzeit in 24-Stunden-Schritten vorverlegt, bis die Angabe im Parameter DAYOFWEEK erfüllt ist.

Wird für DAYOFWEEK nicht ANY angegeben, werden die Zeitpläne, je nach Angabe für PERIOD und PERUNITS, möglicherweise nicht zum erwarteten Zeitpunkt verarbeitet. Der Standardwert ist ANY.

##### Erweiterter Zeitplan

Gibt die Tage der Woche an, an denen der Zeitplan ausgeführt werden soll. Sie können entweder mehrere Tage, die durch Kommas und ohne Leerzeichen voneinander getrennt werden, oder WEEKDAY, WEEKEND oder ANY angeben. Werden mehrere Tage angegeben, wird der Zeitplan an jedem angegebenen Tag ausgeführt. Wird WEEKDAY oder WEEKEND angegeben, müssen Sie auch entweder WEEKOFMONTH=FIRST oder WEEKOFMONTH=LAST angeben, und der Zeitplan wird nur einmal pro Monat ausgeführt.

Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan an jedem Tag der Woche oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter DAYOFWEEK muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

Gültige Werte für den Parameter DAYofweek sind:

##### ANY

Das Startfenster kann an einem beliebigen Wochentag beginnen.

##### WEEKDay

Das Startfenster kann am Montag, Dienstag, Mittwoch, Donnerstag oder Freitag beginnen.

##### WEEKEnd

Das Startfenster kann am Samstag oder Sonntag beginnen.

##### Sunday

Das Startfenster beginnt am Sonntag.

Monday  
Das Startfenster beginnt am Montag.

Tuesday  
Das Startfenster beginnt am Dienstag.

Wednesday  
Das Startfenster beginnt am Mittwoch.

Thursday  
Das Startfenster beginnt am Donnerstag.

Friday  
Das Startfenster beginnt am Freitag.

Saturday  
Das Startfenster beginnt am Samstag.

#### MONTH

Gibt die Monate des Jahres an, in denen der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Geben Sie mehrere Werte an, indem Sie Kommas und keine Leerzeichen verwenden. Der Standardwert lautet ANY. Er bedeutet, dass der Zeitplan während aller Monate des Jahres ausgeführt wird.

#### DAYOFMONTH

Gibt den Tag des Monats an, an dem der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Sie können entweder ANY oder eine Zahl von -31 bis 31, ausschließlich Null, angeben. Ein negativer Wert gibt einen Tag an, bei dem vom Ende des Monats zurückgezählt wird. Beispiel: Der letzte Tag des Monats ist -1, der vorletzte Tag des Monats ist -2. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan an jedem angegebenen Tag des Monats ausgeführt. Geben mehrere Werte denselben Tag an, wird der Zeitplan nur einmal an diesem Tag ausgeführt.

Der Standardwert ist ANY. Dies bedeutet, dass der Zeitplan an jedem Tag des Monats oder an den Tagen ausgeführt wird, die durch andere Parameter des erweiterten Zeitplans bestimmt werden. Der Parameter DAYOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFWEEK oder WEEKOFMONTH verwendet wird.

Gibt ein vorhandener Zeitplan einen anderen Wert als ANY für DAYOFWEEK und WEEKOFMONTH an, und wird DAYOFMONTH aktualisiert, werden DAYOFWEEK und WEEKOFMONTH auf ANY zurückgesetzt.

#### WEEKOFMONTH

Gibt die Woche des Monats an, in der der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Eine Woche wird als beliebige 7-Tage-Periode betrachtet, die nicht an einem bestimmten Tag der Woche beginnt. Sie können FIRST, SECOND, THIRD, FOURTH, LAST oder ANY angeben. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan während jeder angegebenen Woche des Monats ausgeführt. Geben mehrere Werte dieselbe Woche an, wird der Zeitplan nur einmal während dieser Woche ausgeführt.

Der Standardwert ist ANY. ANY bedeutet, dass der Zeitplan während jeder Woche des Monats oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter WEEKOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

#### EXPIRATION

Gibt das Datum an, nach dem dieser Zeitplan nicht mehr verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NEVER. Sie können einen der folgenden Werte angeben:

##### Never

Gibt an, dass der Zeitplan nie abläuft.

##### Ablaufdatum

Gibt das Datum im Format MM/DD/YYYY an, an dem dieser Zeitplan abläuft. Wenn ein Ablaufdatum angegeben wird, läuft der Zeitplan um 23:59:59 Uhr am angegebenen Datum ab.

## Beispiel: Die Priorität eines Zeitplans aktualisieren

---

Für den Zeitplan MONTHLY\_BACKUP, der zur Maßnahmendomäne STANDARD gehört, soll der Wert für die Priorität auf 1 gesetzt werden.

```
update schedule standard monthly_backup priority=1
```

## Beispiel: Das Ablaufdatum eines Zeitplans aktualisieren

---



Der Zeitplan WEEKLY\_BACKUP, der zur Maßnahmendomäne EMPLOYEE\_RECORDS gehört, soll am 29. März 1999 (03/29/1999) ablaufen.

```
update schedule employee_records weekly_backup expiration=03/29/1999
```

## Beispiel: Einen Zeitplan aktualisieren, so dass die Archivierung am letzten Freitag eines Monats erfolgt

Einen Zeitplan, bei dem Dateien vierteljährlich am letzten Freitag des Monats archiviert werden, in einen Zeitplan aktualisieren, bei dem die Dateien am letzten Tag der angegebenen Monate archiviert werden.

```
update schedule employee_records quarterly_archive dayofmonth=-1
```

WEEKOFMONTH und DAYOFWEEK werden auf ANY zurückgesetzt.

## UPDATE SCHEDULE (Verwaltungszeitplan aktualisieren)

Mit diesem Befehl können ausgewählte Parameter für einen Verwaltungszeitplan aktualisiert werden.

Die Befehle MACRO und QUERY ACTLOG können nicht geplant werden.

Ein verwalteter Verwaltungszeitplan, der von einem Konfigurationsmanager aktualisiert wird, wird während der Konfigurationsaktualisierungsverarbeitung auf den verwalteten Servern in einen inaktiven Status versetzt. Er behält einen inaktiven Status, bis er auf diesen Servern in einen aktiven Status aktualisiert wird.

## Berechtigungsklasse

Zum Aktualisieren eines Verwaltungszeitplans ist Systemberechtigung erforderlich.

## Syntax

Klassischer Verwaltungszeitplan

```
(1)
>>-UPDate SChedule-----Zeitplanname----->
>--+-----+-----+-----+-----+----->
>  '-Type---Administrative-'  '-CMD---Befehl-'
>--+-----+-----+-----+-----+----->
>  '-ACTIVE---+Yes-+-'  '-DESCRiption---Beschreibung-'
>    '-No--'
>--+-----+-----+-----+-----+----->
>  '-PRIority---Zahl-'  '-STARTDate---Datum-'
>--+-----+-----+-----+-----+----->
>  '-STARTTime---Zeit-'  '-DURation---Zahl-'
>--+-----+-----+-----+-----+----->
>  '-DURUnits---+Minutes---+'  '-MAXRUNTime---Anzahl-'
>    +-Hours-----+
>    +-Days-----+
>    '-INDefinite-'
>--+-----+-----+-----+-----+----->
>  '-SCHEDStyle---Classic-'  '-PERiod---Zahl-'
>--+-----+-----+-----+-----+----->
>  '-PERUnits---+Hours---+'
>    +-Days-----+
>    +-Weeks---+
>    +-Months---+
>    +-Years---+
>    '-Onetime-'
>--+-----+-----+-----+-----+----->
>  '-DAYofweek---+ANY-----+'
>    +-WEEKDay---+
>    +-WEEKEnd---+
>    +-Sunday----+
```

```

+-Monday----+
+-Tuesday---+
+-Wednesday--+
+-Thursday--+
+-Friday----+
'-Saturday--'

```

```

>----->
'-EXPIration=---+-Never-+-'
'-Datum-'

```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.

## Syntax

### Erweiterter Verwaltungszeitplan

```

(1)
>>-UPDate SCHEDULE-----Zeitplanname----->
>----->
'-Type-----Administrative-' '-CMD-----Befehl-'
>----->
'-ACTIVE-----+-Yes-+-' '-DESCRIPTION-----Beschreibung-'
'-No--'
>----->
'-PRIority-----Zahl-' '-STARTDate-----Datum-'
>----->
'-STARTTime-----Zeit-' '-DURATION-----Zahl-'
>----->
'-DURUnits-----+-Minutes-+-' '-MAXRUNTime-----Anzahl-'
+-Hours----+
'-Days-----'
>----->
'-SCHEDStyle-----Enhanced-' '-MONth-----+-ANY-----+-'
+-January---+
+-February--+
+-MARch-----+
+-APril-----+
+-May-----+
+-JUNe-----+
+-JULy-----+
+-AUGust----+
+-September-+
+-October---+
+-November--+
'-December--'
>----->
'-DAYOFMonth-----+-ANY-+-' '-WEEKofmonth-----+-ANY-----+-'
'-Day-' +-First--+
+-Second--+
+-Third--+
+-FOurth--+
'-Last---'
>----->
'-DAYofweek-----+-ANY-----+-'
+-WEEKDay---+
+-WEEKEnd---+
+-SUNday----+
+-Monday----+
+-TUesday---+
+-WednesDay--+
+-THursday--+
+-Friday----+
'-SATurday--'

```

```
>-----<
'-EXPIration=--+Never-+-'
      '-Datum-'
```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.

## Parameter

Zeitplanname (Erforderlich)

Gibt den Namen des Zeitplans an, der aktualisiert werden soll.

Type=Administrative (Erforderlich)

Gibt an, daß ein Zeitplan für Verwaltungsbefehle aktualisiert wird.

CMD

Gibt den Verwaltungsbefehl an, der für die Verarbeitung geplant werden soll. Dieser Parameter ist wahlfrei. Der angegebene Befehl kann bis zu 512 Zeichen enthalten. Den Befehl in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

Es können keine Umleitungszeichen mit diesem Parameter angegeben werden.

ACTIVE

Gibt an, ob der Verwaltungsbefehl für die Verarbeitung auswählbar ist. Dieser Parameter ist wahlfrei. Ein Zeitplan für Verwaltungsbefehle wird erst verarbeitet, wenn er sich im aktiven Status befindet. Gültige Werte:

YES

Gibt an, daß der Verwaltungsbefehl für die Verarbeitung auswählbar ist.

NO

Gibt an, daß der Verwaltungsbefehl nicht für die Verarbeitung auswählbar ist.

DESCRiption

Gibt eine Beschreibung des Zeitplans an. Dieser Parameter ist wahlfrei. Für die Beschreibung können bis zu 255 Zeichen angegeben werden. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Soll eine zuvor definierte Beschreibung gelöscht werden, ist eine leere Zeichenfolge ("" ) anzugeben.

PRIority

Gibt den Prioritätswert für einen Zeitplan an. Dieser Parameter ist wahlfrei. Zulässige Werte sind ganze Zahlen von 1 bis 10, wobei 1 die höchste Priorität und 10 die niedrigste Priorität angibt. Der Standardwert ist 5.

Wenn zwei oder mehr Zeitpläne dieselbe Fensterstartzeit haben, legt der angegebene Wert fest, wann IBM Spectrum Protect den Zeitplan verarbeitet. Der Zeitplan mit der höchsten Priorität startet zuerst. Ein Zeitplan mit PRIORITY=3 startet beispielsweise vor einem Zeitplan mit PRIORITY=5.

STARTDate

Gibt das Datum für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum. Diesen Parameter zusammen mit dem Parameter STARTTIME verwenden, um anzugeben, wann das Anfangsstartfenster des Zeitplans startet.

Sie können das Datum unter Verwendung der folgenden Werte angeben:

| Wert                            | Beschreibung  | Beispiel   |
|---------------------------------|---|--|
| MM/TT/JJJJ                      | Ein bestimmtes Datum  | 09/15/1998   |
| TODAY                           | Das aktuelle Datum  | TODAY  |
| TODAY+Tage <b>oder</b><br>+Tage | Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999. | TODAY +3 <b>oder</b> +3.   |
| EOLM (Ende des letzten Monats)  | Der letzte Tag des Vormonats.   | EOLM   |
| EOLM-Tage                       | Der letzte Tag des Vormonats minus angegebene Tage.   | EOLM-1<br><br>Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren. |
| BOTM (Anfang dieses Monats)     | Der erste Tag des aktuellen Monats.   | BOTM   |

| Wert      | Beschreibung   | Beispiel  |
|-----------|--|---|
| BOTM+Tage | Der erste Tag des aktuellen Monats plus angegebene Tage. | BOTM+9<br><br>Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren. |

#### STARTTime

Gibt die Uhrzeit für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist die aktuelle Uhrzeit. Dieser Parameter gibt in Verbindung mit dem Parameter STARTDATE den Beginn des Anfangsstartfensters an.

Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

| Wert                         | Beschreibung   | Beispiel   |
|------------------------------|--|--|
| HH:MM:SS                     | Eine bestimmte Uhrzeit   | 10:30:08   |
| NOW                          | Die aktuelle Uhrzeit   | NOW  |
| NOW+HH:MM <b>oder</b> +HH:MM | Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten  | NOW+02:00 <b>oder</b> +02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW+02:00 oder STARTTIME=+02:00 ausgegeben, beginnt das Startfenster um 7:00 Uhr. |
| NOW-HH:MM <b>oder</b> -HH:MM | Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten | NOW-02:00 <b>oder</b> -02:00.<br><br>Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW-02:00 oder STARTTIME=-02:00 ausgegeben, beginnt das Startfenster um 3:00 Uhr. |

#### DURation

Gibt die Anzahl Einheiten an, die die Länge des Startfensters der geplanten Operation definiert. Dieser Parameter ist wahlfrei. Dieser Wert muß zwischen 1 und 999 liegen. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter DURUNITS verwenden, um die Länge des Startfensters anzugeben. Werden beispielsweise DURATION=20 und DURUNITS=MINUTES angegeben, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Standardlänge des Startfensters beträgt 1 Stunde. Die Länge des Fensters muß kürzer sein, als der Zeitraum zwischen Fenstern.

Dieser Wert wird ignoriert, wenn DURUNITS=INDEFINITE angegeben wird.

#### DURUnits

Gibt die Zeiteinheiten an, mit denen die Dauer des Fensters bestimmt wird, in dem der Zeitplan starten kann. Dieser Parameter ist wahlfrei. Der Standardwert ist HOURS.

Diesen Parameter zusammen mit dem Parameter DURATION verwenden, um anzugeben, wie lange das Startfenster geöffnet bleibt, um den Zeitplan zu verarbeiten. Gilt beispielsweise DURATION=20 und DURUNITS=MINUTES, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Verarbeitung des Zeitplans muß nicht unbedingt innerhalb dieses Fensters enden. Wenn der Zeitplan aus irgendeinem Grund wiederholt werden muß, müssen die Wiederholungsversuche vor Ablauf des Startfensters beginnen; andernfalls wird die Operation nicht erneut gestartet.

Der Standardwert für die Länge des Startfensters ist 1 Stunde. Sie können einen der folgenden Werte angeben:

#### Minutes

Gibt an, daß die Dauer des Fensters in Minuten definiert wird.

#### Hours

Gibt an, daß die Dauer des Fensters in Stunden definiert wird.

#### Days

Gibt an, daß die Dauer des Fensters in Tagen definiert wird.

#### INDefinite

Gibt an, daß die Dauer des Startfensters der geplanten Operation unbegrenzt ist. Der Zeitplan kann bis zu seinem Verfall zu einem beliebigen Zeitpunkt nach der geplanten Startzeit ausgeführt werden. Sie können DURUNITS=INDEFINITE nur angeben, wenn Sie PERUNITS=ONETIME angeben. Der Wert INDEFINITE ist für erweiterte Zeitpläne nicht zulässig.

#### MAXRUNtime

Gibt die maximale Ausführungszeit an. Hierbei handelt es sich um die Anzahl Minuten, in denen Serverprozesse, die von geplanten Befehlen gestartet werden, abgeschlossen werden müssen. Sind Prozesse nach Ablauf der maximalen Ausführungszeit noch aktiv, werden die Prozesse von der zentralen Zeitplanung abgebrochen.

Tipps:

- Möglicherweise werden die Prozesse nicht sofort beendet, wenn sie von der zentralen Zeitplanung abgebrochen werden. Sie werden beendet, wenn sie die Benachrichtigung über den Abbruch von der zentralen Zeitplanung registrieren.
- Die maximale Ausführungszeit wird ab dem Zeitpunkt berechnet, an dem der Serverprozess startet. Wenn mit dem Befehl für den Zeitplan mehr als ein Prozess gestartet wird, wird die maximale Ausführungszeit für jeden Prozess ab dem Zeitpunkt berechnet, an dem der jeweilige Prozess startet.
- Dieser Parameter gilt nicht für einige Prozesse, wie z. B. Prozesse zum Identifizieren doppelter Daten, deren Ausführung nach Ablauf der maximalen Ausführungszeit fortgesetzt werden kann.
- Dieser Parameter gilt nicht, wenn der geplante Befehl keinen Serverprozess startet.
- Einigen Befehlen kann eine andere Abbruchzeit zugeordnet werden. Beispielsweise kann der Befehl MIGRATE STGPOOL einen Parameter einschließen, der die Länge der Zeit angibt, die die Speicherpoolumlagerung ausgeführt wird, bevor die Umlagerung automatisch abgebrochen wird. Wenn Sie einen Befehl planen, für den eine Abbruchzeit definiert ist, und Sie außerdem eine maximale Ausführungszeit für den Zeitplan definieren, werden die Prozesse zu der Abbruchzeit abgebrochen, die zuerst erreicht wird.

Einschränkungen:

- Der Wert des Parameters wird nicht an Server verteilt, die von einem Manager für unternehmensweite Konfiguration verwaltet werden.
- Der Wert des Parameters wird nicht mit dem Befehl EXPORT exportiert.

Dieser Parameter ist wahlfrei. Sie können eine Zahl im Bereich von 0 bis 1440 angeben. Der Wert 0 bedeutet, dass die maximale Ausführungszeit unendlich ist und die zentrale Zeitplanung keine Prozesse abbricht. Die maximale Ausführungszeit muss größer als die Dauer des Startfensters sein, die mit den Parametern DURATION und DURUNITS definiert wird.

Ist beispielsweise die Startzeit eines geplanten Befehls 21:00 Uhr und beträgt die Dauer des Startfensters 2 Stunden, erstreckt sich das Startfenster von 21:00 Uhr bis 23:00 Uhr. Beträgt die maximale Ausführungszeit 240 Minuten (4 Stunden), müssen alle zutreffenden Serverprozesse, die von dem Befehl gestartet werden, um 1:00 Uhr abgeschlossen sein. Sind ein oder mehrere zutreffende Prozesse nach 1:00 Uhr noch aktiv, werden die Prozesse von der zentralen Zeitplanung abgebrochen.

Tipp: Alternativ können Sie eine *Endzeit* von 1:00 Uhr im IBM Spectrum Protect Operations Center angeben.

#### SCHEDStyle

Dieser Parameter ist wahlfrei. SCHEDSTYLE definiert entweder das Intervall zwischen den Zeiten, zu denen ein Zeitplan ausgeführt werden soll, oder die Tage, an denen der Zeitplan ausgeführt werden soll. Die Darstellung kann entweder classic oder enhanced sein. Dieser Parameter muss angegeben werden, wenn Sie die Darstellung eines Zeitplans von klassisch in erweitert oder zurück in klassisch ändern. Andernfalls wird der Wert für den vorhandenen Zeitplan verwendet.

Für klassische Zeitpläne sind diese Parameter zulässig: PERIOD, PERUNITS und DAYOFWEEK. Diese Parameter sind nicht zulässig: MONTH, DAYOFMONTH und WEEKOFMONTH. War die vorherige Zeitplandarstellung erweitert, werden die Parameter MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK zurückgesetzt. DAYOFWEEK, PERIOD und PERUNITS werden auf die Standardwerte gesetzt, es sei denn, sie werden mit dem Aktualisierungsbefehl angegeben.

Für erweiterte Zeitpläne sind diese Parameter zulässig: MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK. Diese Parameter sind nicht zulässig: PERIOD und PERUNITS. War die vorherige Zeitplandarstellung klassisch, werden die Parameter DAYOFWEEK, PERIOD und PERUNITS zurückgesetzt. MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK werden auf die Standardwerte gesetzt, es sei denn, sie werden mit dem Aktualisierungsbefehl angegeben.

#### PERiod

Gibt den Zeitraum zwischen Startfenstern für diesen Zeitplan an. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Zulässige Werte sind ganze Zahlen von 1 bis 999. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter PERUNITS verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle fünf Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Zeitraum zwischen den Startfenstern muß länger sein als die Dauer jedes Fensters. Der Standardwert ist 1 Tag.

Dieser Wert wird ignoriert, wenn PERUNITS=ONETIME angegeben wird.

#### PERUnits

Gibt die Zeiteinheiten an, mit denen der Zeitraum zwischen Startfenstern für diesen Zeitplan bestimmt wird. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Der Standardwert ist DAYS.

Diesen Parameter zusammen mit dem Parameter PERIOD verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle 5 Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Standardwert ist 1 Tag. Sie können einen der folgenden Werte angeben:

#### Hours

Gibt an, daß der Zeitraum zwischen Startfenstern in Stunden angegeben wird.

#### Days

Gibt an, daß der Zeitraum zwischen Startfenstern in Tagen angegeben wird.

#### Weeks

Gibt an, daß der Zeitraum zwischen Startfenstern in Wochen angegeben wird.

#### Months

Gibt an, daß der Zeitraum zwischen Startfenstern in Monaten angegeben wird.

Wird PERUNITS=MONTHS angegeben, wird die geplante Operation jeden Monat an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/04/1998 lautet, wird der Zeitplan danach am 4. jedes Monats verarbeitet. Wenn das Datum jedoch für den nächsten Monat nicht gültig ist, wird die geplante Operation am letzten gültigen Datum in dem Monat verarbeitet. Danach basieren nachfolgende Operationen auf diesem neuen Datum. Wenn das Startdatum beispielsweise 03/31/1998 lautet, wird die Operation des nächsten Monats für den 04/30/1998 geplant. Danach werden alle folgenden Operationen bis Februar am 30. des Monats ausgeführt. Da Februar nur 28 Tage hat, wird die Operation für das Datum 02/28/1999 geplant. Nachfolgende Operationen werden am 28. des Monats verarbeitet.

#### Years

Gibt an, daß der Zeitraum zwischen Startfenstern für den Zeitplan in Jahren angegeben wird.

Wird PERUNITS=YEARS angegeben, wird die geplante Operation jährlich in demselben Monat und an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/29/2004 lautet, wird die geplante Operation des nächsten Jahres am 02/28/2005 ausgeführt, da Februar nur 28 Tage hat. Danach werden folgende Operationen für den 28. Februar geplant.

#### Onetime

Gibt an, daß der Zeitplan einmal verarbeitet wird. Dieser Wert überschreibt den für den Parameter PERIOD angegebenen Wert.

#### DAYofweek

Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können verschiedene Optionen für den Parameter DAYofweek angeben, abhängig davon, ob die Zeitplandarstellung als 'Klassisch' oder 'Erweitert' definiert wurde:

##### Klassischer Zeitplan

Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können entweder einen Tag der Woche oder WEEKDAY, WEEKEND oder ANY angeben. Fallen Startdatum und Startzeit auf einen Tag, der nicht einem angegebenen Tag entspricht, werden das Startdatum und die Startzeit in 24-Stunden-Schritten vorverlegt, bis die Angabe im Parameter DAYOFWEEK erfüllt ist.

Wird für DAYOFWEEK nicht ANY angegeben, werden die Zeitpläne, je nach Angabe für PERIOD und PERUNITS, möglicherweise nicht zum erwarteten Zeitpunkt verarbeitet. Der Standardwert ist ANY.

##### Erweiterter Zeitplan

Gibt die Tage der Woche an, an denen der Zeitplan ausgeführt werden soll. Sie können entweder mehrere Tage, die durch Kommas und ohne Leerzeichen voneinander getrennt werden, oder WEEKDAY, WEEKEND oder ANY angeben. Werden mehrere Tage angegeben, wird der Zeitplan an jedem angegebenen Tag ausgeführt. Wird WEEKDAY oder WEEKEND angegeben, müssen Sie auch entweder WEEKOFMONTH=FIRST oder WEEKOFMONTH=LAST angeben, und der Zeitplan wird nur einmal pro Monat ausgeführt.

Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan an jedem Tag der Woche oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter DAYOFWEEK muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

Gültige Werte für den Parameter DAYofweek sind:

##### ANY

Das Startfenster kann an einem beliebigen Wochentag beginnen.

##### WEEKDay

Das Startfenster kann am Montag, Dienstag, Mittwoch, Donnerstag oder Freitag beginnen.

##### WEEKEnd

Das Startfenster kann am Samstag oder Sonntag beginnen.

##### SUNday

Das Startfenster beginnt am Sonntag.

##### Monday

Das Startfenster beginnt am Montag.

##### TUESday

Das Startfenster beginnt am Dienstag.

##### Wednesday

Das Startfenster beginnt am Mittwoch.

##### THursday

Das Startfenster beginnt am Donnerstag.  
Friday  
Das Startfenster beginnt am Freitag.  
Saturday  
Das Startfenster beginnt am Samstag.

#### MONth

Gibt die Monate des Jahres an, in denen der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Geben Sie mehrere Werte an, indem Sie Kommas und keine Leerzeichen verwenden. Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan in jedem Monat des Jahres ausgeführt wird.

#### DAYOFMonth

Gibt den Tag des Monats an, an dem der Zeitplan ausgeführt werden soll. Dieser Parameter kann nur für erweiterte Zeitpläne angegeben werden. Sie können entweder ANY oder eine Zahl von -31 bis 31, ausschließlich Null, angeben. Ein negativer Wert gibt einen Tag an, bei dem vom Ende des Monats zurückgezählt wird. Beispiel: Der letzte Tag des Monats ist -1, der vorletzte Tag des Monats ist -2 usw. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan an jedem angegebenen Tag des Monats ausgeführt. Geben mehrere Werte denselben Tag an, wird der Zeitplan nur einmal an diesem Tag ausgeführt.

Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan an jedem Tag des Monats oder an den Tagen ausgeführt wird, die durch andere Parameter des erweiterten Zeitplans bestimmt werden. Der Parameter DAYOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFWEEK oder WEEKOFMONTH verwendet wird.

#### WEEKofmonth

Gibt die Woche des Monats an, in der der Zeitplan ausgeführt werden soll. Dieser Parameter kann nur für erweiterte Zeitpläne angegeben werden. Eine Woche wird als beliebige 7-Tage-Periode betrachtet, die nicht an einem bestimmten Tag der Woche beginnt. Sie können FIRST, SECOND, THIRD, FOURTH, LAST oder ANY angeben. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan während jeder angegebenen Woche des Monats ausgeführt. Geben mehrere Werte dieselbe Woche an, wird der Zeitplan nur einmal während dieser Woche ausgeführt.

Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan während jeder Woche des Monats oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter WEEKOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

#### EXpiration

Gibt das Datum an, nach dem dieser Zeitplan nicht mehr verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NEVER. Sie können einen der folgenden Werte angeben:

##### Never

Gibt an, dass der Zeitplan nie abläuft.

##### Ablaufdatum

Gibt das Datum im Format MM/DD/YYYY an, an dem dieser Zeitplan abläuft. Wenn ein Ablaufdatum angegeben wird, läuft der Zeitplan um 23:59:59 Uhr am angegebenen Datum ab.

## Beispiel: Einen Sicherungszeitplan aktualisieren, so dass die Sicherung alle drei Tage erfolgt

---

Der bestehende Verwaltungszeitplan BACKUP\_BACKUPPOOL soll dahingehend aktualisiert werden, daß (ab heute) der primäre Speicherpool BACKUPPOOL alle drei Tage um 22 Uhr abends in den Kopierspeicherpool COPYSTG gesichert werden soll.

```
update schedule backup_backuppool type=administrative cmd="backup stgpool
backuppool copystg" active=yes starttime=22:00 period=3
```

## Beispiel: Einen Sicherungszeitplan aktualisieren, so dass die Sicherung an jedem ersten und dritten Freitag erfolgt

---

Den Zeitplan BACKUP\_ARCHIVEPOOL aktualisieren, der den primären Speicherpool ARCHIVEPOOL im Kopierspeicherpool RECOVERYPOOL sichert. Der vorhandene Zeitplan wird am ersten und zehnten Tag in jedem Monat ausgeführt. Den Zeitplan so aktualisieren, dass er am ersten und dritten Freitag in jedem Monat ausgeführt wird.

```
update schedule backup_archivepool
dayofweek=friday weekofmonth=first,third
```

DAYOFMONTH wird auf ANY zurückgesetzt.

## UPDATE SCRATCHPADENTRY (Scratchpadeintrag aktualisieren)

---

Mit diesem Befehl können Sie Daten in einer Zeile im Scratchpad aktualisieren.

### Berechtigungsklasse

---

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

---

```
>>-UPDate SCRATCHPadentry--übergeordnete_Kategorie----->
>--untergeordnete_Kategorie--Betreff--Line -===Nummer----->
>--Data-===Daten-----><
```

### Parameter

---

übergeordnete\_Kategorie (Erforderlich)

Gibt die übergeordnete Kategorie an, in der Daten aktualisiert werden sollen. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

untergeordnete\_Kategorie (Erforderlich)

Gibt die untergeordnete Kategorie an, in der Daten aktualisiert werden sollen. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

Betreff (Erforderlich)

Gibt den Betreff an, unter dem Daten aktualisiert werden sollen. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

Line (Erforderlich)

Gibt die Nummer der Zeile an, in der Daten aktualisiert werden sollen.

Data (Erforderlich)

Gibt die neuen Daten an, die in der Zeile gespeichert werden sollen. Vorherige Daten werden gelöscht. Sie können bis zu 1000 Zeichen eingeben. Schließen Sie die Daten in Anführungszeichen ein, wenn die Daten ein oder mehrere Leerzeichen enthalten. Bei den Daten muss die Groß-/Kleinschreibung beachtet werden.

### Beispiel: Scratchpadeintrag aktualisieren

---

Aktualisieren Sie Kontaktinformationen für die Abwesenheit eines Administrators, Jane, in einer Datenbank, in der Informationen zu den Standorten aller Administratoren gespeichert sind:

```
update scratchpadentry admin_info location jane line=2 data=
"Nicht im Büro bis 18.11."
```

### Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für UPDATE SCRATCHPADENTRY

| Befehl                  | Beschreibung  |
|-------------------------|---|
| DEFINE SCRATCHPADENTRY  | Erstellt eine Zeile mit Daten im Scratchpad.                    |
| DELETE SCRATCHPADENTRY  | Löscht eine Zeile mit Daten aus dem Scratchpad.                 |
| QUERY SCRATCHPADENTRY   | Zeigt Informationen an, die im Scratchpad enthalten sind.       |
| SET SCRATCHPADRETENTION | Gibt den Zeitraum an, den Scratchpadeinträge aufbewahrt werden. |

## UPDATE SCRIPT (IBM Spectrum Protect-Prozedur aktualisieren)

---

Mit diesem Befehl kann eine Befehlszeile geändert oder einer IBM Spectrum Protect-Prozedur eine neue Befehlszeile hinzugefügt werden.

Einschränkung: Die Ausgabe eines Befehls innerhalb einer IBM Spectrum Protect-Prozedur kann nicht umgeleitet werden. Führen Sie stattdessen die Prozedur aus und geben Sie dann die Befehlsumleitung an. Soll beispielsweise die Ausgabe von script1 in das



Verzeichnis c:\temp\test.out übertragen werden, führen Sie wie im folgenden Beispiel die Prozedur aus und geben Sie die Befehlsumleitung an:

```
run script1 > c:\temp\test.out
```

## Berechtigungsklasse

---

Um diesen Befehl ausgeben zu können, muß der Administrator die Prozedur zuvor definiert oder die Systemberechtigung haben.

## Syntax

---

```
>>-UPDate SCRIPT--Prozedurname----->
>+-----+----->
  '-Befehlszeile--+-----+'
                    '-Line ---Nummer-'
>+-----+-----><
  '-DESCription----Beschreibung-'
```

## Parameter

---

### Prozedurname (Erforderlich)

Gibt den Namen der Prozedur an, die aktualisiert werden soll.

### Befehlszeile

Gibt einen neuen oder aktualisierten Befehl an, der in einer Prozedur verarbeitet werden soll. Wird dieser Befehl ausgegeben, muss ein Befehl und/oder eine Beschreibung aktualisiert werden.

Der Befehl kann Substitutionsvariablen enthalten und über mehrere Zeilen fortgesetzt werden, wenn als letztes Zeichen in dem Befehl ein Fortsetzungszeichen (-) angegeben wird. Für den Befehl können bis zu 1200 Zeichen angegeben werden. Den Befehl in Anführungszeichen einschließen, wenn er Leerzeichen enthält. Wird dieser Parameter angegeben, kann der folgende Parameter wahlweise angegeben werden.

Sie haben die Optionen, Befehle seriell, parallel oder seriell und parallel auszuführen, indem Sie den Prozedurbefehl SERIAL oder PARALLEL für diesen Parameter angeben. Sie können mehrere Befehle parallel ausführen und auf deren Beendigung warten, bevor Sie mit dem nächsten Befehl fortfahren. Befehle werden seriell ausgeführt, bis der parallele Befehl gefunden wird.

Ablaufanweisungen mit bedingter Logik können verwendet werden. Diese Anweisungen schließen IF, EXIT und GOTO ein.

### Line

Gibt die Zeilennummer für den Befehl an. Wird keine Zeilennummer angegeben, wird die Befehlszeile an die bestehende Befehlszeilenfolge angehängt. Der angehängten Befehlszeile wird eine Zeilennummer zugeordnet, die um fünf höher ist als die letzte Befehlszeilennummer. Hat beispielsweise die letzte Zeile in der Prozedur die Nummer 015, wird der angehängten Befehlszeile die Zeilennummer 020 zugeordnet.

Bei Angabe einer Zeilennummer ersetzt der Befehl eine vorhandene Zeile (wenn die Nummer mit der einer bestehenden Zeile identisch ist). Andernfalls fügt der Befehl die angegebene Zeile ein (wenn die Zeilennummer nicht einer vorhandenen Zeilennummer in der Befehlszeilenfolge entspricht).

### DESCription

Gibt eine Beschreibung für die Prozedur an. Für die Beschreibung können bis zu 255 Zeichen angegeben werden. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält.

## Beispiel: Einen Befehl am Ende eines Scripts hinzufügen

---

Angenommen, Sie haben das folgende Script mit drei Zeilen (QSAMPLE) definiert und möchten den Befehl QUERY SESSION am Ende des Scripts hinzufügen.

```
001 /* Dies ist eine Beispielprozedur */
005 QUERY STATUS
010 QUERY PROCESS
```

```
update script qsample "query session"
```

Nach der Verarbeitung des Befehls besteht das Script aus den folgenden Zeilen:

```

001 /* Dies ist eine Beispielprozedur */
005 QUERY STATUS
010 QUERY PROCESS
015 QUERY SESSION

```

## Beispiel: Eine bestimmte Zeile in einem Script aktualisieren

Unter Verwendung des Scripts aus dem vorherigen Beispiel Zeile 010 ändern, so dass der Befehl QUERY STGPOOL an Stelle des Befehls QUERY PROCESS verarbeitet wird:

```
update script qsample "query stgpool" line=010
```

Nach der Verarbeitung des Befehls besteht das Script aus den folgenden Zeilen:

```

001 /* Dies ist eine Beispielprozedur */
005 QUERY STATUS
010 QUERY STGPOOL
015 QUERY SESSION

```

## Beispiel: Einen Befehl in der Mitte eines Scripts einfügen

Unter Verwendung des Scripts aus dem vorherigen Beispiel eine neue Befehlszeile (QUERY NODE) hinter der Befehlszeile QUERY STATUS in dem Script QSAMPLE einfügen:

```
update script qsample "query node"
line=007
```

Nach der Verarbeitung des Befehls besteht das Script aus den folgenden Zeilen:

```

001 /* Dies ist eine Beispielprozedur */
005 QUERY STATUS
007 QUERY NODE
010 QUERY STGPOOL
015 QUERY SESSION

```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE SCRIPT

| Befehl        | Beschreibung  |
|---------------|---|
| COPY SCRIPT   | Erstellt eine Kopie einer Prozedur.                           |
| DEFINE SCRIPT | Definiert eine Prozedur für den IBM Spectrum Protect-Server.  |
| DELETE SCRIPT | Löscht eine Prozedur oder einzelne Zeilen aus einer Prozedur. |
| QUERY SCRIPT  | Zeigt Informationen über Prozeduren an.                       |
| RENAME SCRIPT | Vergibt einen neuen Namen für eine Prozedur.                  |
| RUN           | Führt ein Script aus.   |

### Zugehörige Tasks:

Befehle parallel oder seriell ausführen  
 Logikablaufanweisungen in ein Script einschließen  
 Tasks gleichzeitig auf mehreren Servern ausführen  
 Server-Script definieren

### Zugehörige Verweise:

Rückkehrcodes für die Verwendung in IBM Spectrum Protect-Scripts

## UPDATE SERVER (Server aktualisieren, der für die Übertragung zwischen Servern definiert ist)

Mit diesem Befehl kann eine Serverdefinition aktualisiert werden.

Einschränkung: Ist dieser Server ein Quellenserver für eine Operation mit virtuellem Datenträger, kann das Ändern dieser Werte Auswirkungen auf die Fähigkeit des Quellenservers haben, auf die Daten zuzugreifen und die Daten zu verwalten, die auf dem entsprechenden Zielservers gespeichert sind. Wird der Servername mit dem Befehl SET SERVERNAME geändert, kann dies abhängig vom Betriebssystem zusätzliche Auswirkungen haben. Nachfolgend sind einige Beispiele aufgeführt:



- Kennwörter können ungültig gemacht werden

- Einheitendaten können betroffen sein
- Angaben aus der Registrierungsdatenbank zu Windows-Betriebssystemen können sich ändern

## Berechtigungsklasse


Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax für:

- **Unternehmensweite Konfiguration**
- **Unternehmensweite Ereignisprotokollierung**
- **Befehlsweiterleitung**
- **Speicheragent**
- **Quellen- und Zielsever für Knotenreplikation**
-  AIX-Betriebssysteme  Linux-Betriebssysteme **z/OS Media-Server**

```
>>-UPDate--SERver--Servername----->
>--+-----+----->
  '-SERVERPAssword---Kennwort-'
>--+-----+----->
  '-HLAddress---IP-Adresse-'
>+-----+-----+----->
  '-LLAddress---TCP-Anschluss-'  '-COMMmethod---TCPIP-'
>+-----+-----+----->
  '-URL---URL-'  '-ALLOWReplace---Yes+-'
                                     '-No--'
>+-----+-----+----->
  '-DESCription---Beschreibung-'
>+-----+-----+----->
  '-FORCESync---Yes+-'
                                     '-No--'
>+-----+-----+----->
  | (1) |
  '-VALIDateprotocol---No--+'
                                     '-All-'
>+-----+-----+----->
  '-SSL---No--+'
                                     '-Yes-'
.-SESSIONSECurity---TRANSitional-.
>+-----+-----+----->
  '-SESSIONSECurity---STRICT---+'
                                     '-TRANSitional-'
.-TRANSFERMethod---Tcpi-----.
>+-----+-----+----->
  '-TRANSFERMethod---Tcpi---+'
                                     | (2) |
                                     '-Fasp-----'
```

Anmerkungen:

1. Der Parameter VALIDATEPROTOCOL ist veraltet und gilt nur für Speicheragentendefinitionen.
2.  Linux-Betriebssysteme Der Parameter TRANSFERMETHOD ist nur auf Betriebssystemen Linux x86\_64 verfügbar.

### Syntax für virtuelle Datenträger

```
>>-UPDate--SERver--Servername----->
                                     '-PAssword---Kennwort-'
>+-----+-----+----->
  '-HLAddress---IP-Adresse-'
```

```

>--+-----+-----+-----+----->
  '-LLAddress-----TCP-Anschluss-' '-COMMmethod-----TCPIP-'

>--+-----+-----+-----+----->
  '-URL-----URL-' '-DELgraceperiod-----Tage-'

>--+-----+-----+-----+----->
  '-NODENAME-----Knotenname-' '-SSL-----Yes-'

.-SESSIONSECURITY-----TRANSITIONAL-----.
>--+-----+-----+-----+----->
  '-SESSIONSECURITY-----+STRict-----+-'
                                '-TRANSITIONAL-'

>--+-----+-----+-----+----->
  '-FORCESync-----+Yes+-'
                                '-No--'

>--+-----+-----+-----+-----<
  '-DESCRIPTION-----Beschreibung-'

```

## Parameter

### Servername (Erforderlich)

Gibt den Namen des Servers an, der aktualisiert werden soll. Dieser Parameter ist erforderlich.

### PAssword

Gibt das Kennwort an, das für die Anmeldung am Zielsystem für virtuelle Datenträger verwendet wird. Dieser Parameter ist wahlfrei.

### SERVERPAssword

Gibt das Serverkennwort an, das für unternehmensweite Konfiguration, Befehlsweiterleitung und Ereignisprotokollierung zwischen Servern verwendet wird. Das Kennwort muss mit dem Serverkennwort übereinstimmen, das mit dem Befehl SET SERVERPASSWORD definiert wurde. Dieser Parameter ist wahlfrei.

### HLAddress

Gibt die IP-Adresse des Servers an (in der Schreibweise mit Trennzeichen). Dieser Parameter ist wahlfrei.

### LLAddress

Gibt die Adresse der unteren Ebene des Servers an. Diese Adresse stimmt normalerweise mit der Adresse in der Serveroption TCPPORT des Zielsystems überein. Bei SSL=YES muss der Anschluss bereits für die SSL-Übertragung auf dem Zielsystem definiert sein.

### COMMmethod

Gibt die Übertragungsmethode an, mit der die Verbindung zum Server hergestellt wird. Dieser Parameter ist wahlfrei.

### URL

Gibt die URL-Adresse an, die für den Zugriff auf diesen Server vom Administration Center aus verwendet wird. Der Parameter ist wahlfrei.

### DELgraceperiod

Gibt die Anzahl Tage an, die ein Objekt auf dem Zielsystem verbleibt, nachdem es zum Löschen markiert wurde. Sie können einen Wert von 0 bis 9999 angeben. Der Standardwert ist 5. Dieser Parameter ist optional.

### NODENAME

Gibt einen Knotennamen an, den der Server für die Verbindung zum Zielsystem verwenden soll. Dieser Parameter ist wahlfrei.

### DESCRIPTION

Gibt eine Beschreibung des Servers an. Dieser Parameter ist wahlfrei. Die Beschreibung kann bis zu 255 Zeichen umfassen. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge (") angeben.

### FORCESync

Gibt an, ob der Serverprüfchlüssel zurückgesetzt werden soll, wenn sich der Quellenserver das nächste Mal beim Zielsystem anmeldet. Mit einem gültigen Prüfchlüssel kann ein Quellenserver Objekte auf den Zielsystem stellen, den Wert für die Verweildauer bis zum Löschen verwalten und das Kennwort aktualisieren, wenn das aktuelle Kennwort bekannt ist und der Prüfchlüssel übereinstimmt. Der Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

#### Yes

Gibt an, dass ein neuer Prüfchlüssel an den Zielsystem gesendet und vom Zielsystem akzeptiert wird, wenn ein gültiges Kennwort empfangen wird.

#### No

Gibt an, dass kein neuer Prüfchlüssel an den Zielsystem gesendet wird.

### VALIDateprotocol (veraltet)

Gibt an, ob eine zyklische Blockprüfung die Daten validiert, die zwischen dem Speicheragenten und dem IBM Spectrum Protect-Server gesendet werden. Der Parameter ist wahlfrei. Der Standardwert ist NO.

Wichtig: Ab IBM Spectrum Protect Version 8.1.2 und Tivoli Storage Manager Version 7.1.8 wird die durch diesen Parameter aktivierte Validierung durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter SESSIONSECURITY durchgesetzt wird. Der Parameter VALIDATEPROTOCOL wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

#### ALLOWReplace

Gibt an, ob eine durch einen verwalteten Server definierte Serverdefinition durch eine Definition vom Konfigurationsmanager ersetzt werden kann. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

Yes

Gibt an, dass eine Serverdefinition durch eine Definition vom Konfigurationsmanager ersetzt werden kann.

No

Gibt an, dass eine Serverdefinition nicht durch die Definition vom Konfigurationsmanager ersetzt werden kann.

#### SSL

Gibt den Kommunikationsmodus des Servers an.

Wichtig: Ab IBM Spectrum Protect Version 8.1.2 und Tivoli Storage Manager Version 7.1.8 wird SSL verwendet, um einen Teil der Kommunikation mit dem angegebenen Server zu verschlüsseln, auch wenn Sie NO angeben.

Die folgenden Bedingungen und Hinweise gelten, wenn Sie den Parameter SSL angeben:

- Selbst signierte Zertifikate der Partnerserver müssen sich in der Schlüsseldatenbankdatei (cert.kdb) jedes Servers befinden, bevor die Server gestartet werden.
- Sie können mehrere Servernamen mit verschiedenen Parametern für denselben Zielsever definieren.

Sie können einen der folgenden Werte angeben:

No

Gibt eine SSL-Sitzung für die gesamte Kommunikation mit dem angegebenen Server an, außer wenn der Server Objektdaten sendet oder empfängt. Objektdaten werden mithilfe von TCP/IP gesendet und empfangen. Wird ausgewählt, dass die Objektdaten nicht verschlüsselt werden, ähnelt die Serverleistung der Kommunikation über eine TCP/IP-Sitzung und die Sitzung ist sicher.

Yes

Gibt eine SSL-Sitzung für die gesamte Kommunikation mit dem angegebenen Server an, auch wenn der Server Objektdaten sendet und empfängt.

#### SESSIONSECurity

Gibt an, ob der Server, der definiert wird, die sichersten Einstellungen verwenden muss, um mit einem IBM Spectrum Protect-Server zu kommunizieren. Dieser Parameter ist wahlfrei.

Sie können einen der folgenden Werte angeben:

#### STRict

Gibt an, dass die striktesten Sicherheitseinstellungen für den Server, der definiert wird, durchgesetzt werden. Der Wert STRICT verwendet das sicherste Kommunikationsprotokoll, das verfügbar ist. Dies ist derzeit TLS 1.2. Das TLS 1.2-Protokoll wird für SSL-Sitzungen zwischen dem angegebenen Server und einem IBM Spectrum Protect-Server verwendet. Für die Verwendung des Werts STRICT müssen die folgenden Anforderungen erfüllt werden, um sicherzustellen, dass sich der angegebene Server mit dem IBM Spectrum Protect-Server authentifizieren kann:

- Der Server, der definiert wird, und der IBM Spectrum Protect-Server müssen IBM Spectrum Protect-Software verwenden, die den Parameter SESSIONSECURITY unterstützt.
- Der Server, der definiert wird, muss für die Verwendung des TLS 1.2-Protokolls für SSL-Sitzungen zwischen sich selbst und dem IBM Spectrum Protect-Server konfiguriert werden.

Server, für die der Wert STRICT definiert ist und die diese Anforderungen nicht erfüllen, können sich nicht mit dem IBM Spectrum Protect-Server authentifizieren.


#### TRANSitional

Gibt an, dass die vorhandenen Sicherheitseinstellungen für den Server durchgesetzt werden. Dies ist der Standardwert. Dieser Wert ist für die temporäre Verwendung bestimmt, während Sie Ihre Sicherheitseinstellungen aktualisieren, um die Anforderungen für den Wert STRICT zu erfüllen.

Ist SESSIONSECURITY=TRANSITIONAL definiert und hat der Server nie die Anforderungen für den Wert STRICT erfüllt, authentifiziert sich der Server weiterhin mithilfe des Werts TRANSITIONAL. Wenn ein Server jedoch die Anforderungen für den Wert STRICT erfüllt, wird der Wert des Parameters SESSIONSECURITY automatisch von TRANSITIONAL in STRICT aktualisiert. Der Server kann sich dann nicht mehr mit einer Version des Clients oder mit einem SSL/TLS-Protokoll authentifizieren, die bzw. das die Anforderungen für STRICT nicht erfüllt. Nachdem sich ein Server erfolgreich mit einem Kommunikationsprotokoll authentifiziert hat, das mehr Sicherheit bietet, kann sich der Server nicht mehr mit einem weniger sicheren Protokoll authentifizieren. Beispiel: Wenn ein Server, der nicht SSL verwendet, aktualisiert wird und sich mithilfe von TLS 1.2 erfolgreich authentifiziert, kann sich der Server nicht mehr ohne SSL-Protokoll oder mithilfe von TLS 1.1 authentifizieren. Diese Einschränkung gilt auch bei Verwendung von Funktionen wie z. B. virtuelle Datenträger,

Befehlsweiterleitung oder Export zwischen Servern, wenn sich ein Knoten oder Administrator beim IBM Spectrum Protect-Server als Knoten oder Administrator von einem anderen Server authentifiziert.

#### Linux-BetriebssystemeTRANSFERMETHOD

 Linux-BetriebssystemeGibt die Methode an, die für die Datenübertragung zwischen Servern verwendet wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

##### Tcpip

Gibt an, dass TCP/IP für die Übertragung von Daten verwendet wird. Dies ist der Standardwert.

##### Fasp

Gibt an, dass die Aspera FASP-Technologie (Fast Adaptive Secure Protocol) für die Übertragung von Daten verwendet wird. Mit der Aspera FASP-Technologie kann die Datenübertragung in einem Weitverkehrsnetz (WAN) optimiert werden. Einschränkungen:

- Bevor Sie die Aspera FASP-Technologie aktivieren, müssen Sie bestimmen, ob die Technologie für Ihre Systemumgebung geeignet ist, und die entsprechenden Lizenzen installieren. Anweisungen finden Sie unter Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann. Wenn die Lizenzen fehlen oder abgelaufen sind, schlagen Datenübertragungsoperationen fehl.
- Wenn die WAN-Leistung Ihre Geschäftsanforderungen erfüllt, aktivieren Sie nicht die Aspera FASP-Technologie.
- Wenn Sie TRANSFERMETHOD=FASP im Befehl PROTECT STGPOOL oder REPLICATE NODE angeben, überschreibt dieser Wert den Parameter TRANSFERMETHOD in den Befehlen DEFINE SERVER und UPDATE SERVER.

## Beispiel: Karenzzeit bis zum Löschen für einen Server aktualisieren

Die Definition von SERVER2 aktualisieren, um anzugeben, dass Objekte noch 10 Tage auf dem Zielserver verbleiben sollen, nachdem sie zum Löschen markiert wurden.

```
update server server2 delgraceperiod=10
```

## Beispiel: Den URL für einen Server aktualisieren

Die Definition von NEWSERVER aktualisieren, um seine URL-Adresse als http://newserver:1580/ anzugeben.

```
update server newserver url=http://newserver:1580/
```

## Beispiel: Alle Server für die Kommunikation mit einem IBM Spectrum Protect-Server unter Verwendung der Sitzungssicherheit 'strict' aktualisieren

Die Definition aller Server für die Verwendung der striktesten Sicherheitseinstellungen aktualisieren, um sich mit dem IBM Spectrum Protect-Server zu authentifizieren.

```
update server * sessionsecurity=strict
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE SERVER

| Befehl            | Beschreibung   |
|-------------------|--|
| DEFINE DEVCLASS   | Definiert eine Einheitenklasse.  |
| DEFINE SERVER     | Definiert einen Server für die Übertragung zwischen Servern.   |
| DELETE DEVCLASS   | Löscht eine Einheitenklasse.   |
| DELETE FILESPACE  | Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt. |
| DELETE SERVER     | Löscht die Definition eines Servers.   |
| QUERY NODE        | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.  |
| QUERY SERVER      | Zeigt Informationen über Server an.  |
| RECONCILE VOLUMES | Stimmt Definitionen von virtuellen Datenträgern auf dem Quellenserver mit Archivierungsobjekten des Zielservers ab.  |

| Befehl          | Beschreibung   |
|-----------------|--|
| REGISTER NODE   | Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.          |
| REMOVE NODE     | Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne. |
| UPDATE DEVCLASS | Ändert die Attribute einer Einheitenklasse.  |
| UPDATE NODE     | Ändert die Attribute, die einem Clientknoten zugeordnet sind.                                    |

## UPDATE SERVERGROUP (Beschreibung einer Servergruppe aktualisieren)

Mit diesem Befehl kann die Beschreibung einer Server-Gruppe aktualisiert werden.

### Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

### Syntax

```
>>-UPDate SERVERGroup--Gruppenname----->
>--DEscription----Beschreibung-----<<
```

### Parameter

Gruppenname (Erforderlich)

Gibt die Server-Gruppe an, die aktualisiert werden soll.

DEscription (Erforderlich)

Gibt eine Beschreibung der Server-Gruppe an. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält.

### Beispiel: Die Beschreibung einer Servergruppe aktualisieren

Die Beschreibung der Servergruppe WEST\_COMPLEX in "Western Region Complex" aktualisieren.

```
update servergroup west_complex
description="western region complex"
```

### Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE SERVERGROUP

| Befehl             | Beschreibung                               |
|--------------------|--|
| COPY SERVERGROUP   | Erstellt eine Kopie einer Servergruppe.    |
| DEFINE SERVERGROUP | Definiert eine neue Servergruppe.          |
| DELETE SERVERGROUP | Löscht eine Servergruppe.                  |
| QUERY SERVERGROUP  | Zeigt Informationen über Servergruppen an. |
| RENAME SERVERGROUP | Benennt eine Servergruppe um.              |

## UPDATE SPACETRIGGER (Speicherbereichsauslöser aktualisieren)

Mit diesem Befehl können Einstellungen für Auslöser aktualisiert werden, die festlegen, wann und wie der Server Speicherbereichsmängel in Speicherpools behebt, die die Einheitenklassen FILE mit sequenziellem Zugriff und DISK mit wahlfreiem Zugriff verwenden.

Für Speicherpools mit dem Parameter RECLAMATIONTYPE=SNAPLOCK werden keine Speicherbereichsauslöser aktiviert.

Wichtig: Bei Speicherbereichsauslöserfunktionen und Berechnungen des Speicherbereichs im Speicherpool wird der Speicherbereich berücksichtigt, der in jedem Verzeichnis verbleibt. Idealerweise sollten Sie jedem Verzeichnis ein separates Dateisystem zuordnen.

Wenn Sie mehrere Verzeichnisse für eine Einheitenklasse angeben und sich die Verzeichnisse in demselben Dateisystem befinden, berechnet der Server den Speicherbereich durch Hinzufügen von Werten, die den Speicherbereich darstellen, der in jedem Verzeichnis verbleibt. Diese Speicherbereichsberechnungen sind ungenau. Anstatt einen Speicherpool mit ausreichend Speicherbereich für eine Operation auszuwählen, kann der Server den falschen Speicherpool auswählen und frühzeitig über keinen Speicherbereich mehr verfügen. Bei Speicherbereichsauslösern kann eine ungenaue Berechnung zu einem Fehler bei der Erweiterung des Speicherbereichs führen, der in einem Speicherpool verfügbar ist. Ein Fehler bei der Erweiterung des Speicherbereichs in einem Speicherpool ist eine der Bedingungen, die zur Inaktivierung eines Auslösers führen kann. Wird ein Auslöser inaktiviert, da der Speicherbereich in einem Speicherpool nicht erweitert werden konnte, können Sie den Auslöser erneut aktivieren, indem Sie den folgenden Befehl angeben: `update spacetrigger stg`. Es sind keine weiteren Änderungen an dem Speicherbereichsauslöser erforderlich.

Weitere Informationen befinden sich unter dem Befehl `DEFINE SPACETRIGGER`.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-UPDate SPACETrigger--STG--+-+-----+----->
                                     '-Fullpct----Prozent-'
>+-----+----->
  '-SPACEexpansion----Prozent-'
>+-----+----->
  '-EXPansionprefix----Präfix-'
>+-----+-----><
  '-STGPOOL----Speicherpoolname-'
```

## Parameter

### STG (Erforderlich)

Gibt einen Speicherbereichsauslöser für den Speicherpool an.

### Fullpct

Dieser Parameter gibt den Auslastungsprozentsatz des Speicherpools an.



Wird dieser Wert überschritten, erstellt der Speicherbereichsauslöser neue Datenträger.

Sie können die Auslastung des Speicherpools bestimmen, indem Sie den Befehl `QUERY STGPOOL` mit `FORMAT=DETAILED` ausgeben. Der Prozentsatz der Speicherpoolauslastung für den Speicherpool wird im Feld "Ausl. für Speicherbereichsauslöser" angezeigt. Die Berechnung dieses Prozentsatzes schließt keine potenziellen Arbeitsdatenträger ein. Die Berechnung der prozentualen Auslastung bei der Umlagerung und Wiederherstellung schließt jedoch potenzielle Arbeitsdatenträger ein.

### SPACEexpansion

Für Speicherbereichsauslöser für Speicherpools des Typs `FILE` mit sequenziellem Zugriff wird dieser Parameter bei der Bestimmung der Anzahl zusätzlicher Datenträger verwendet, die in dem Speicherpool erstellt werden. Datenträger werden unter Verwendung des Werts für `MAXCAPACITY` aus der Einheitenklasse des Speicherpools erstellt. Für Speicherbereichsauslöser für `DISK`-Speicherpools mit wahlfreiem Zugriff erstellt der Speicherbereichsauslöser einen einzelnen Datenträger unter Verwendung von `EXPANSIONPREFIX`.



### EXPansionprefix


Dieser Parameter gibt das Präfix an, das der Server zum Erstellen neuer Speicherpooldateien verwendet. Dieser Parameter ist wahlfrei und gilt nur für Einheitenklassen `DISK` mit wahlfreiem Zugriff. Das Standardpräfix ist der Serverinstallationspfad. Das Präfix kann ein oder mehrere Verzeichnistrennzeichen enthalten. Beispiel:  AIX-Betriebssysteme  Linux-Betriebssysteme

`/opt/tivoli/tsm/server/bin/`

 Windows-Betriebssysteme

`c:\Programme\tivoli\tsm\`

 AIX-Betriebssysteme  Linux-Betriebssysteme Es können bis zu 250 Zeichen angegeben werden. Wenn Sie ein ungültiges Präfix angeben, kann die automatische Erweiterung fehlschlagen.

 Windows-Betriebssysteme Sie können bis zu 200 Zeichen angeben. Wird der Server als Windows-Dienst ausgeführt, ist das Standardpräfix das Verzeichnis `c:\wnnt\system32`. Wenn Sie ein ungültiges Präfix angeben, kann die automatische Erweiterung



fehlschlagen.

Dieser Parameter ist für Speicherbereichsauslöser für FILE-Speicherpools mit sequenziellem Zugriff nicht gültig. Es werden Präfixe der Verzeichnisse verwendet, die mit der zugeordneten Einheitenklasse angegeben sind.

#### STGPOOL

Gibt den Speicherpool an, der diesem Speicherbereichsauslöser zugeordnet ist. Wird der Parameter STGPOOL nicht angegeben, wird der standardmäßige Speicherbereichsauslöser für den Speicherpool aktualisiert.

Dieser Parameter gilt nicht für Speicherpools mit dem Parameter RECLAMATIONTYPE=SNAPLOCK.

## Beispiel: Den Speicherbereich für einen Speicherpool vergrößern

Den Speicherbereich in einem Speicherpool um 50 Prozent vergrößern, wenn der Speicherpool zu 80 Prozent mit vorhandenen Datenträgern belegt ist. Speicherbereich wird in den Verzeichnissen erstellt, die der Einheitenklasse zugeordnet sind.

```
update spacetrigger stg spaceexpansion=50 stgpool=file
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE SPACETRIGGER

| Befehl              | Beschreibung  |
|---------------------|---|
| DEFINE SPACETRIGGER | Definiert einen Speicherbereichsauslöser zum Erweitern des Speicherbereichs für einen Speicherpool. |
| DELETE SPACETRIGGER | Löscht den Speicherbereichsauslöser für den Speicherpool.   |
| QUERY SPACETRIGGER  | Zeigt Informationen zu einem Speicherbereichsauslöser für den Speicherpool an.                      |

## UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)

Mit diesem Befehl können Sie einen vorhandenen Schwellenwert für die Statusüberwachung aktualisieren.

Mit Statusüberwachungsschwellenwerten werden die definierten Bedingungen mit den Serverabfragen für die Statusüberwachung verglichen und die Ergebnisse in die Statusüberwachungstabelle eingefügt.

Es können mehrere Schwellenwerte für eine Aktivität definiert werden. Sie können beispielsweise einen Schwellenwert erstellen, der einen Warnstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 80 % ist. Sie können dann einen anderen Schwellenwert erstellen, der einen Fehlerstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 90 % ist.

Anmerkung: Wenn bereits ein Schwellenwert für eine Bedingung EXISTS definiert ist, können Sie keinen anderen Schwellenwert mit einem der anderen Bedingungstypen definieren.

## Syntax

```
>>-UPDate STATusthreshold--Schwellenwertname-+-----+-->
                                     '-Activity---Name der Aktivität-'
>--+-----+-----+-----+-----+-----+----->
  '-Condition---+EXists+-' '-Value-----Wert-'
          +-GT-----+
          +-GE-----+
          +-LT-----+
          +-LE-----+
          '-Equal--'
>--+-----+-----+-----+-----+-----+-----<
  '-Status-----+Normal--+'
          +-Warning-+
          '-Error---'
```

## Parameter

#### Schwellenwertname (Erforderlich)

Gibt den Schwellenwertnamen an, der aktualisiert werden soll. Der Name darf 48 Zeichen nicht überschreiten.

#### Activity

Geben Sie diesen Wert an, um die Aktivität für einen vorhandenen Schwellenwert zu ändern. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

##### PROCESSSUMMARY

Gibt die Anzahl Prozesse an, die gegenwärtig aktiv sind.

##### SESSIONSUMMARY

Gibt die Anzahl Sitzungen an, die gegenwärtig aktiv sind.

##### CLIENTSESSIONSUMMARY

Gibt die Anzahl Clientsitzungen an, die gegenwärtig aktiv sind.

##### SCHEDCLIENTSESSIONSUMMARY

Gibt die Anzahl geplanter Clientsitzungen an.

##### DBUTIL

Gibt die prozentuale Datenbankauslastung an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

##### DBFREESPACE

Gibt den freien Speicherbereich in Gigabyte an, der in der Datenbank verfügbar ist.

##### DBUSEDSPACE

Gibt den verwendeten Datenbankbereich in Gigabyte an.

##### ARCHIVELOGFREESPACE

Gibt den freien Speicherbereich in Gigabyte an, der im Archivprotokoll verfügbar ist.

##### STGPOOLUTIL

Gibt die prozentuale Auslastung des Speicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

##### STGPOOLCAPACITY

Gibt die Speicherpoolkapazität in Gigabyte an.

##### AVGSTGPOOLUTIL

Gibt die durchschnittliche prozentuale Speicherpoolauslastung für alle Speicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

##### TOTSTGPOOLCAPACITY

Gibt die Gesamtspeicherpoolkapazität in Gigabyte für alle verfügbaren Speicherpools an.

##### TOTSTGPOOLS

Gibt die Anzahl der definierten Speicherpools an.

##### TOTRWSTGPOOLS

Gibt die Anzahl der definierten Speicherpools an, die lesbar oder änderbar sind.

##### TOTNOTRWSTGPOOLS

Gibt die Anzahl der definierten Speicherpools an, die nicht lesbar oder änderbar sind.

##### STGPOOLINUSEANDDEFINED

Gibt die Gesamtzahl der definierten Datenträger an, die im Gebrauch sind.

##### ACTIVELOGUTIL

Gibt die aktuelle prozentuale Auslastung der aktiven Protokolldatei an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

##### ARCHLOGUTIL

Gibt die aktuelle Auslastung des Archivprotokolls an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

##### CPYSTGPOOLUTIL

Gibt die prozentuale Auslastung eines Kopierspeicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

##### PMRYSTGPOOLUTIL

Gibt die prozentuale Auslastung eines primären Speicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

##### DEVCLASSPCTDRVOFFLINE

Gibt die prozentuale Auslastung von Laufwerken an (nach Einheitenklasse), die offline sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

##### DEVCLASSPCTDRVPOLLING

Gibt den Sendeaufruf für Laufwerke nach Einheitenklasse an. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

##### DEVCLASSPCTLIBPATHSOFFLINE

Gibt die Kassettenarchivpfade an (nach Einheitenklasse), die offline sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

##### DEVCLASSPCTPATHSOFFLINE

Gibt den Prozentsatz der Einheitenklassenpfade an (nach Einheitenklasse), die offline sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

#### DEVCLASSPCTDISKSNOTRW

Gibt den Prozentsatz der Platten an, die für die Einheitenklasse DISK nicht beschreibbar sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

#### DEVCLASSPCTDISKSUNAVAILABLE

Gibt den Prozentsatz der Plattendatenträger an (nach Einheitenklasse), die nicht verfügbar sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

#### FILEDEVCLASSPCTSCRUNALLOCATABLE

Gibt den Prozentsatz der Arbeitsdatenträger an, die der Server für eine bestimmte Einheitenklasse FILE, die nicht gemeinsam genutzt wird, nicht zuordnen kann. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

#### Condition

Geben Sie diesen Wert an, um die Bedingung eines vorhandenen Schwellenwerts zu ändern. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

##### EXists

Erstellt einen Statusüberwachungsanzeiger, wenn die Aktivität vorhanden ist.

##### GT

Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis größer als der angegebene Wert ist.

##### GE

Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis größer-gleich dem angegebenen Wert ist.

##### LT

Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis kleiner als der angegebene Wert ist.

##### LE

Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis kleiner-gleich dem angegebenen Wert ist.

##### EQual

Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis gleich dem angegebenen Wert ist.

#### Value

Geben Sie diesen Parameter an, um den Wert zu ändern, der mit der Aktivitätsausgabe für die angegebene Bedingung verglichen wird. Sie können eine ganze Zahl im Bereich von 0 bis 9999999999999999 angeben.

#### Status

Geben Sie diesen Wert an, um den Status des Anzeigers zu ändern, der bei der Statusüberwachung erstellt wird, wenn die Bedingung, die ausgewertet wird, erfüllt ist. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

##### Normal

Gibt an, dass der Statusanzeiger einen normalen Statuswert hat.

##### Warnung

Gibt an, dass der Statusanzeiger einen Warnstatuswert hat.

##### Fehler

Gibt an, dass der Statusanzeiger einen Fehlerstatuswert hat.

## Einen vorhandenen Statusschwellenwert aktualisieren

Mit dem folgenden Befehl einen Statusschwellenwert für die durchschnittliche prozentuale Speicherpoolauslastung aktualisieren:

```
update statusthreshold avgstgpl "AVGSTGPOOLUTIL" value=90 condition=gt status=error
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE STATUSTHRESHOLD

| Befehl   | Beschreibung   |
|--|--|
| DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)   | Löscht einen Schwellenwert für die Statusüberwachung.  |
| QUERY MONITORSTATUS (Überwachungsstatus abfragen)  | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an. |
| QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen) | Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an. |
| QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)  | Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.                             |
| SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)  | Gibt an, ob die Statusüberwachung aktiviert werden soll.   |

| Befehl  | Beschreibung   |
|---|--|
| SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)        | Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.         |
| SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)   | Gibt das Aktualisierungsintervall für die Statusüberwachung an.  |
| SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll) | Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll. |
| UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)  | Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.   |

## UPDATE STGPOOL (Speicherpool aktualisieren)

Mit diesem Befehl kann ein Speicherpool geändert werden.

Einschränkung: Wenn ein Client die Funktion für gleichzeitiges Schreiben und die Datendeduplizierung verwendet, wird das Feature für die Datendeduplizierung während der Ausführung von Sicherungen in einem Speicherpool inaktiviert.

Der Befehl UPDATE STGPOOL verwendet sieben Formen. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für UPDATE STGPOOL

| Befehl                    | Beschreibung  |
|---------------------------|---|
| BACKUP STGPOOL            | Sichert einen primären Speicherpool in einem Kopierspeicherpool.  |
| COPY ACTIVATEDATA         | Kopiert aktive Sicherungsdaten.   |
| DEFINE COLLOGROUP         | Definiert eine Kollokationsgruppe.  |
| DEFINE COLLOCMEMBER       | Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.   |
| DEFINE STGPOOL            | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.  |
| DELETE COLLOGROUP         | Löscht eine Kollokationsgruppe.   |
| DELETE COLLOCMEMBER       | Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.   |
| DELETE STGPOOL            | Löscht einen Speicherpool aus dem Serverspeicher.   |
| MOVE DRMEDIA              | Versetzt DRM-Datenträger vor Ort und lagert sie aus.  |
| MOVE MEDIA                | Versetzt Speicherpooldatenträger, die von einem automatisierten Kassettenarchive verwaltet werden.                                  |
| QUERY COLLOGROUP          | Zeigt Informationen zu Kollokationsgruppen an.  |
| QUERY DRMEDIA             | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.                                       |
| QUERY NODEDATA            | Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.   |
| QUERY SHREDSTATUS         | Zeigt Informationen zu Daten an, die auf das Schreddern warten.   |
| QUERY STGPOOL             | Zeigt Informationen zu Speicherpools an.  |
| RESTORE STGPOOL           | Schreibt Dateien aus Kopierspeicherpools in einen primären Speicherpool zurück.   |
| RESTORE VOLUME            | Schreibt Dateien, die auf angegebenen Datenträgern in einem primären Speicherpool gespeichert sind, aus Kopierspeicherpools zurück. |
| SET DRMDBBACKUPEXPIREDAYS | Gibt die Kriterien für den Verfall von Datenbanksicherungsreihen an.  |

| Befehl            | Beschreibung   |
|-------------------|--|
| SHRED DATA        | Startet manuell den Prozess zum Schreddern gelöschter Daten. |
| UPDATE COLLOGROUP | Aktualisiert die Beschreibung einer Kollokationsgruppe.      |

- UPDATE STGPOOL (Cloud-Containerspeicherpool aktualisieren)  
Mit diesem Befehl können Sie einen Containerspeicherpool in einer Cloudumgebung aktualisieren. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.
- UPDATE STGPOOL (Verzeichniscontainerspeicherpool aktualisieren)  
Mit diesem Befehl kann ein Verzeichniscontainerspeicherpool aktualisiert werden.
- UPDATE STGPOOL (Containerkopienspeicherpool aktualisieren)  
Mit diesem Befehl kann ein Containerkopienspeicherpool aktualisiert werden.
- UPDATE STGPOOL (Primären Speicherpool mit wahlfreiem Zugriff aktualisieren)  
Mit diesem Befehl kann ein Speicherpool mit wahlfreiem Zugriff aktualisiert werden.
- UPDATE STGPOOL (Primären Speicherpool mit sequenziellem Zugriff aktualisieren)  
Mit diesem Befehl kann ein primärer Speicherpool mit sequenziellem Zugriff aktualisiert werden.
- UPDATE STGPOOL (Kopienspeicherpool mit sequenziellem Zugriff aktualisieren)  
Mit diesem Befehl kann ein Kopienspeicherpool mit sequenziellem Zugriff aktualisiert werden.
- UPDATE STGPOOL (Pool für aktive Daten mit sequenziellem Zugriff aktualisieren)  
Mit diesem Befehl kann ein Pool für aktive Daten aktualisiert werden.

## UPDATE STGPOOL (Cloud-Containerspeicherpool aktualisieren)

Mit diesem Befehl können Sie einen Containerspeicherpool in einer Cloudumgebung aktualisieren. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.

Die bevorzugte Methode zum Definieren und Konfigurieren eines Cloud-Containerspeicherpools ist die Verwendung des Operations Center. Anweisungen und Hinweise für das Operations Center und die Befehlszeilenschnittstelle finden Sie in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-UPDate STGpool--Poolname--+-+-----+---->
                                     '-DESCRiption-----Beschreibung-'
>+-----+-----+-----+-----+-----+----->
  '-CLOUDType-----+Swift-----+-'
                                     +-Softlayer+-
                                     '-V1Swift---'
>+-----+-----+-----+-----+-----+----->
  '-CLOUDUrl-----Cloud-URL-' | (1) |
                                     '-IDentity-----Cloud-ID-----'
>+-----+-----+-----+-----+-----+----->
  '-PAssword-----Kennwort-'
>+-----+-----+-----+-----+-----+----->
  '-CLOUDLocation-----+Offpremise-+-'
                                     '-ONpremise--'
>+-----+-----+-----+-----+-----+----->
  | (2) |
  '-BUCKETName-----Bucketname-----'
>+-----+-----+-----+-----+-----+----->
  '-ACCess-----+READWrite---+-'
                                     +-READOnly-----+
                                     +-UNAVailable+-
                                     '-DESTroyed---'
>+-----+-----+-----+-----+-----+----->
  '-MAXWriters-----+NOLimit-----+--'
```

```

'-maximale_Anzahl_Writer-'
>----->
'-REUsedelay----Tage-'
>-----<
|
| .-COMPReSSion----Yes-----|
'-ENCRypt----Yes-----+'
'-No--' '-COMPReSSion----Yes-----+'
'-No--'

```

Anmerkungen:

1. Wenn Sie CLOUDTYPE=AZURE angegeben haben, geben Sie nicht den Parameter IDENTITY an.
2. Dieser Parameter ist nur gültig, wenn Sie CLOUDTYPE=S3 angeben.

## Parameter

### Poolname (Erforderlich)

Gibt den Speicherpool an, der aktualisiert werden soll. Dieser Parameter ist erforderlich.

### DEscription

Gibt eine Beschreibung des Speicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge ("" ) angeben.

### CLOUDType

Gibt den Typ der Cloudumgebung an, in der ein Speicherpool konfiguriert wird. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

#### SOftlayer

Gibt an, dass der Speicherpool ein Cloud-Computing-System 'IBM® SoftLayer' (IBM Bluemix) mit einem Cloud-Computing-System 'OpenStack Swift' verwendet.

#### SWift

Gibt an, dass der Speicherpool ein Cloud-Computing-System 'OpenStack Swift' verwendet. Dieser Wert gibt auch an, dass der Speicherpool Version 2 des Protokolls für die Authentifizierung bei der Cloud verwendet. Die URL der Cloud enthält normalerweise die Versionsnummer des verwendeten Protokolls.

#### V1Swift

Gibt an, dass der Speicherpool ein Cloud-Computing-System 'OpenStack Swift' verwendet. Dieser Wert gibt auch an, dass der Speicherpool Version 1 des Protokolls für die Authentifizierung bei der Cloud verwendet. Die URL der Cloud enthält normalerweise die Versionsnummer des verwendeten Protokolls.

Einschränkung: Wenn Sie den Befehl DEFINE STGPOOL verwendet haben, um einen Speicherpool mit CLOUDTYPE=S3 (S3 = Simple Storage Service) zu definieren, können Sie mithilfe des Befehls UPDATE STGPOOL nicht zu einem anderen Cloudtyp wechseln. Außerdem können Sie nicht den Cloudtyp eines Nicht-S3-Speicherpools in S3 ändern, indem Sie den Befehl UPDATE STGPOOL verwenden.

### CLOUDURL

Gibt die URL der Cloudumgebung an, in der der Speicherpool konfiguriert wird. Auf der Basis Ihres Cloud-Providers können Sie eine Regionsendpunkt-URL, eine Accesser-IP-Adresse, einen Endpunkt für öffentliche Authentifizierung (Public Authentication Endpoint) oder einen ähnlichen Wert für diesen Parameter verwenden. Stellen Sie sicher, dass das Protokoll wie z. B. `https://` oder `http://` am Anfang der URL eingefügt wird. Die maximale Länge der Webadresse beträgt 870 Zeichen. Der Parameter CLOUDURL wird erst geprüft, wenn die erste Sicherung beginnt.

Weitere Informationen zum Ermitteln dieser Werte erhalten Sie, wenn Sie Ihren Cloud-Service-Provider in der Liste auf der Seite Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren auswählen.

Tipp: Um mehrere IBM Cloud Object Storage-Accesser zu verwenden, listen Sie die Accesser-IP-Adressen getrennt durch einen vertikalen Balken (|) ohne Leerzeichen auf. Beispiel:

```
CLOUDURL=<Accesser-URL1>|<Accesser-URL2>|<Accesser-URL3>
```

Die Verwendung mehrerer Accesser verbessert die Leistung. Wenn Sie die IBM SoftLayer Cloud Object Store S3-Lösung verwenden, wird nur ein Accesser benötigt.

### IDentity

Gibt die Benutzer-ID für die Cloud an, die im Parameter STGTYPE=CLOUD angegeben ist. Dieser Parameter ist für alle unterstützten Cloud-Computing-Systeme außer Azure erforderlich. Wenn Sie CLOUDTYPE=AZURE angegeben haben, geben Sie nicht den Parameter IDENTITY an. Auf der Basis Ihres Cloud-Providers können Sie eine Zugriffsschlüssel-ID, einen Benutzernamen, einen Tenantnamen und Benutzernamen oder einen ähnlichen Wert für diesen Parameter verwenden. Die maximale Länge der Benutzer-ID beträgt 255 Zeichen.

### PASSword (Erforderlich)

Gibt das Kennwort für die Cloud an, die im Parameter STGTYPE=CLOUD angegeben ist. Auf der Basis Ihres Cloud-Providers können Sie ein SAS-Token (SAS = Shared Access Signature), einen geheimen Zugriffsschlüssel, einen API-Schlüssel, ein Kennwort oder einen ähnlichen Wert für diesen Parameter verwenden. Dieser Parameter ist erforderlich. Die maximale Länge des Kennworts beträgt 255 Zeichen. Die Parameter IDENTITY und PASSWORD werden erst geprüft, wenn die erste Sicherung beginnt.

#### CLOUDLocation

Gibt die physische Position der Cloud an, die im Parameter CLOUD angegeben ist. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

- OFFpremise
- ONpremise

#### BUCKETName

Gibt den Namen für ein Amazon Web Services-Bucket (AWS-Bucket) oder eine IBM Cloud Object Storage-Vault an, das bzw. die mit diesem Speicherpool verwendet werden soll. AWS-Buckets und IBM Cloud Object Storage-Vaults werden auf dieselbe Art und Weise wie Container in einem Cloud-Containerspeicherpool verwendet. Dieser Parameter ist optional und ist nur gültig, wenn dieser Speicherpool den Cloudtyp S3 hat. Wenn der von Ihnen angegebene Name nicht vorhanden ist, erstellt der Server ein Bucket oder eine Vault mit dem angegebenen Namen, bevor das Bucket bzw. die Vault verwendet wird. Beachten Sie die Einschränkungen Ihres Cloud-Providers bei der Benennung, wenn Sie diesen Parameter angeben. Überprüfen Sie die Berechtigungen für das Bucket oder die Vault und stellen Sie sicher, dass die Berechtigungsnachweise für diesen Speicherpool über die Berechtigung zum Lesen, Schreiben, Auflisten und Löschen von Objekten in diesem Bucket oder dieser Vault haben. Einschränkung: Sie können das Bucket oder die Vault nicht ändern, wenn in diesem Speicherpool Cloud-Container vorhanden sind.

#### ACCess

Gibt an, wie Clientknoten und Serverprozesse auf den Speicherpool zugreifen. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

##### READWrite

Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff für den Speicherpool haben.

##### READOnly

Gibt an, dass Clientknoten und Serverprozesse nur Lesezugriff für den Speicherpool haben.

##### UNAVailable

Gibt an, dass Clientknoten und Serverprozesse nicht auf den Speicherpool zugreifen können. Aus diesem Grund schlagen Sicherungen und Zurückschreibungen für diesen Speicherpool fehl. Mit diesem Wert können Sie angeben, dass der Cloud-Service-Provider vorübergehend nicht verfügbar ist.

##### DESTroyed

Gibt an, dass Clientknoten und Serverprozesse nicht auf den Speicherpool zugreifen können, da der Cloud-Service-Provider permanent nicht verfügbar ist. Sicherungen und Zurückschreibungen schlagen für diesen Speicherpool fehl, aber alle Versuche, Objekte und Container aus diesem Speicherpool zu löschen, werden erfolgreich ausgeführt.

#### MAXWriters

Gibt die maximale Anzahl der Schreibsitzungen an, die gleichzeitig für den Speicherpool ausgeführt werden können. Geben Sie eine maximale Anzahl von Schreibsitzungen an, um zu steuern, dass die Leistung des Cloudspeicherpools keine negativen Auswirkungen auf andere Systemressourcen hat. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

##### NOLimit

Gibt an, dass für die Anzahl der Writer, die Sie verwenden können, kein Grenzwert für die maximale Größe vorhanden ist. Dieser Wert ist der Standardwert.

##### maximale\_Anzahl\_Writer

Begrenzt die maximale Anzahl der Writer, die Sie verwenden können. Geben Sie eine ganze Zahl im Bereich von 1 bis 99999 an.

#### REUsedelay

Gibt die Anzahl Tage an, die verstreichen müssen, nachdem alle deduplizierte Speicherbereiche aus einem Cloudspeicherpool entfernt wurden. Dieser Parameter steuert die Dauer, die deduplizierte Speicherbereiche einem Cloudspeicherpool zugeordnet sind. Wenn der für den Parameter angegebene Wert abläuft, werden die deduplizierte Speicherbereiche aus dem Cloudspeicherpool gelöscht. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

##### 1

Gibt an, dass deduplizierte Speicherbereiche nach 1 Tag aus einem Cloudspeicherpool gelöscht werden.

##### Tage

Sie können eine ganze Zahl im Bereich von 0 bis 9999 angeben.

Tipp: Setzen Sie diesen Parameter auf einen Wert, der größer als die für den Befehl SET DRMDBBACKUPEXPIREDDAYS angegebene Anzahl ist. Wird dieser Parameter auf einen höheren Wert gesetzt, können Sie sicherstellen, dass Verweise auf Dateien im Speicherpool noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird.

#### ENCRypt

Gibt an, ob der Server Clientdaten verschlüsselt, bevor er sie in den Speicherpool schreibt. Sie können die folgenden Werte angeben:

Yes

Gibt an, dass Clientdaten vom Server verschlüsselt werden.

No

Gibt an, dass Clientdaten nicht vom Server verschlüsselt werden.

Dieser Parameter ist wahlfrei. Der Standardwert ist von der physischen Position der Cloud abhängig, die durch den Parameter CLOUDLOCATION angegeben wird. Wenn sich die Cloud außerhalb des Unternehmens (off premise) befindet, werden Daten standardmäßig vom Server verschlüsselt. Wenn sich die Cloud vor Ort (on premises) befindet, werden Daten standardmäßig nicht vom Server verschlüsselt.

COMPRession

Gibt an, ob Daten in dem Speicherpool komprimiert werden. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass Daten in dem Speicherpool nicht komprimiert werden.

Yes

Gibt an, dass Daten in dem Speicherpool komprimiert werden. Dies ist der Standardwert.

## Beispiel 1: Einen Cloudspeicherpool aktualisieren, um eine maximale Anzahl von Datensitzungen anzugeben

Einen Cloudspeicherpool mit dem Namen STGPOOL1 aktualisieren und ein Maximum von 10 Datensitzungen angeben.

```
update stgpool stgpool1 maxwriters=10
```




## Beispiel 2: Die Beschreibung eines Cloud-Containerspeicherpools aktualisieren

Einen Cloud-Containerspeicherpool mit dem Namen STGPOOL2 aktualisieren. Die vorhandene Beschreibung aus dem Speicherpool entfernen.

```
update stgpool stgpool2 cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=protect8991 description=""
```

### Zugehörige Tasks:

Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## UPDATE STGPOOL (Verzeichniscontainerspeicherpool aktualisieren)

Mit diesem Befehl kann ein Verzeichniscontainerspeicherpool aktualisiert werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-UPDate STGpool--Poolname--+-----+---->
                                     '-DESCRIPTION---Beschreibung-'

    .-ACCESS----READWrite-----.
>-+-----+----->
    '-ACCESS----+READWrite---+'
                                     +-READOnly----+
                                     '-UNAVailable-'

    .-MAXSIze---NOLimit-----.
>-+-----+----->
    '-MAXSIze---+maximale Dateigröße-+'
                                     '-NOLimit-----'

    .-MAXWriters----NOLimit-----.
```



```

>----->
'-MAXWriters-----+maximale_Anzahl_Writer+-'
                    '-NOLimit-----'

>----->
'-NEXTstgpool-----Poolname-'

>----->
'-PROTECTstgpool-----Zielspeicherpool-'

>----->
|                                     .-,-----|. |
|                                     v          | |
'-PROTECTLOCALstgpools-----lokaler_Zielspeicherpool+-'

.-REUsedelay-----1----.
>----->
'-REUsedelay-----Tage-' '-ENCRypt-----+Yes+-'
                              '-No--'

.-COMPRession-----Yes-----.
>-----<
'-COMPRession-----+Yes+-'
                              '-No--'

```

## Parameter

### Poolname (Erforderlich)

Gibt den Speicherpool an, der aktualisiert werden soll. Dieser Parameter ist erforderlich. Die maximale Länge des Namens beträgt 30 Zeichen.

### DESCRiption

Gibt eine Beschreibung des Speicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge ("" ) angeben.

### ACCess

Gibt an, wie Clientknoten und Serverprozesse auf Dateien in dem Speicherpool zugreifen. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

#### READWrite

Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff für den Speicherpool haben. Dies ist der Standardwert.

#### READOnly

Gibt an, dass Clientknoten und Serverprozesse nur Lesezugriff für den Speicherpool haben.

#### UNAVailable

Gibt an, dass Clientknoten und Serverprozesse nicht auf den Speicherpool zugreifen können.

### MAXSIze

Gibt die maximale Größe einer physischen Datei an, die der Server in dem Speicherpool speichern kann. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Geben Sie einen der folgenden Werte an:

#### NOLimit

Gibt an, dass für die im Speicherpool gespeicherten physischen Dateien keine Größenbeschränkung besteht.

#### maximale\_Dateigröße

Begrenzt die maximale Größe für physische Dateien. Geben Sie eine ganze Zahl im Bereich von 1 bis 999999 gefolgt von einem Maßstabsfaktor an. MAXSIZE=5G gibt z. B. an, dass die maximale Dateigröße für diesen Speicherpool 5 GB ist. Verwenden Sie einen der folgenden Maßstabsfaktoren:

**Tabelle 1. Maßstabsfaktor für die maximale Dateigröße**

| Maßstabsfaktor | Bedeutung |
|----------------|-----------|
| K              | Kilobyte  |
| M              | Megabyte  |
| G              | Gigabyte  |
| T              | Terabyte  |

Tipp: Wenn Sie keine Maßeinheit für die maximale Dateigröße angeben, wird der Wert in Byte angegeben.

Wenn die physische Größe des Speicherpools den Wert des Parameters MAXSIZE überschreitet, zeigt die folgende Tabelle an, wo Dateien normalerweise gespeichert werden.

Tabelle 2. Position einer Datei gemäß der Dateigröße und dem angegebenen Pool

| Angegebener Pool  | Ergebnis   |
|---|--|
| Es ist kein Pool als nächster Speicherpool in der Hierarchie angegeben. | Die Datei wird vom Server nicht gespeichert.                                 |
| Ein Pool ist als nächster Speicherpool in der Hierarchie angegeben.     | Der Server speichert die Datei in dem Speicherpool, den Sie angegeben haben. |

Tipp: Wenn Sie auch den Parameter NEXTstgpool angeben, aktualisieren Sie einen einzelnen Speicherpool in Ihrer Hierarchie so, dass er keine Begrenzung hinsichtlich der maximalen Dateigröße hat, indem Sie den Parameter MAXSIZE=NOLimit angeben. Wenn mindestens ein Pool keine Größenbegrenzung hat, wird sichergestellt, dass der Server die Datei unabhängig von ihrer Größe speichern kann.

Werden während der Dateneduplizierungsverarbeitung mehrere Dateien gesendet, betrachtet der Server die Größe des Dateneduplizierungsprozesses als Dateigröße. Wenn die Gesamtgröße aller Dateien in dem Prozess die maximale Größe überschreitet, werden die Dateien vom Server nicht in dem Speicherpool gespeichert.

#### MAXWriters

Gibt die maximale Anzahl E/A-Threads an, die gleichzeitig für den Speicherpool ausgeführt werden können. Geben Sie eine maximale Anzahl E/A-Threads an, um die Anzahl E/A-Threads zu steuern, die gleichzeitig in den Verzeichniscontainerspeicherpool geschrieben werden. Dieser Parameter ist wahlfrei. Verwenden Sie als Best Practice den Standardwert NOLIMIT. Sie können einen der folgenden Werte angeben:

#### NOLimit

Gibt an, dass keine maximale Anzahl E/A-Threads in den Speicherpool geschrieben wird.

#### maximale\_Anzahl\_Writer

Begrenzt die maximale Anzahl der E/A-Threads, die Sie verwenden können. Geben Sie eine ganze Zahl im Bereich von 1 bis 99999 an.

#### NEXTstgpool

Gibt den Namen eines Speicherpools mit wahlfreiem Zugriff oder eines primären sequenziellen Speicherpools an, in dem Dateien gespeichert werden, wenn der Verzeichniscontainerspeicherpool voll ist. Dieser Parameter ist wahlfrei.

Einschränkungen:

- Um sicherzustellen, dass keine Speicherpoolkette erstellt wird, die zu einer Endlosschleife führt, geben Sie mindestens einen Speicherpool in der Hierarchie ohne Wert an.
- Wenn Sie einen Pool mit sequenziellem Zugriff als nächsten Speicherpool angeben, muss der Pool entweder das Datenformat NATIVE oder NONBLOCK haben.
- Geben Sie keinen Verzeichniscontainer- oder Cloud-Containerspeicherpool an.
- Verwenden Sie diesen Parameter nicht, um einen Speicherpool für die Datenumlagerung anzugeben.

#### PROTECTstgpool

Gibt den Namen des Verzeichniscontainerspeicherpools auf dem Zielserver an, in dem die Daten gesichert werden, wenn Sie den Befehl PROTECT STGPOOL für diesen Speicherpool verwenden. Dieser Parameter ist wahlfrei.

#### PROTECTLOCALstgpools

Gibt den Namen des Containerkopierspeicherpools auf einer lokalen Einheit an, in dem die Daten gesichert werden. Dieser Containerkopierspeicherpool ist ein lokaler Zielspeicherpool, wenn Sie den Befehl PROTECT STGPOOL verwenden. Sie können maximal zwei zu aktualisierende Containerkopierspeicherpoolnamen angeben. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Die maximale Länge jedes Namens beträgt 30 Zeichen. Dieser Parameter ist wahlfrei.

Um Containerkopierspeicherpools hinzuzufügen oder zu entfernen, geben Sie die Namen der Containerkopierspeicherpools an, die eingeschlossen werden sollen. Lautet der vorhandene Containerkopierspeicherpool beispielsweise COPY1 und soll COPY2 hinzugefügt werden, geben Sie PROTECTLOCALSTGPOOLS=COPY1,COPY2 an. Sollen alle vorhandenen Containerkopierspeicherpools entfernt werden, die dem primären Speicherpool zugeordnet sind, geben Sie eine Nullzeichenfolge ("" ) an. Beispiel: COPYSTGPOOLS="".

#### REUsedelay

Gibt die Anzahl Tage an, die verstreichen müssen, bevor alle deduplizierten Speicherbereiche aus einem Verzeichniscontainerspeicherpool entfernt werden. Dieser Parameter steuert die Dauer, die deduplizierte Speicherbereiche einem Verzeichniscontainerspeicherpool zugeordnet sind. Wenn der für den Parameter angegebene Wert abläuft, werden die deduplizierten Speicherbereiche aus dem Verzeichniscontainerspeicherpool gelöscht. Der Standardwert ist 1. Geben Sie einen der folgenden Werte an:

#### Tage

Geben Sie eine ganze Zahl im Bereich von 0 bis 9999 an.

1

Gibt an, dass deduplizierte Speicherbereiche nach 1 Tag aus einem Verzeichniscontainerspeicherpool gelöscht werden.

Tipp: Setzen Sie diesen Parameter auf einen Wert, der größer als der Wert ist, der als Datenbanksicherungsperiode angegeben ist, um sicherzustellen, dass Datenbereiche noch gültig sind, wenn die Datenbank auf eine andere Stufe zurückgeschrieben wird.

#### ENCRypt

Gibt an, ob der Server Clientdaten verschlüsselt, bevor der Server die Daten in den Speicherpool schreibt. Sie können die folgenden Werte angeben:

Yes

Gibt an, dass Clientdaten vom Server verschlüsselt werden.

No

Gibt an, dass Clientdaten nicht vom Server verschlüsselt werden.

#### COMPRession

Gibt an, ob Daten in dem Speicherpool komprimiert werden. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass Daten in dem Speicherpool nicht komprimiert werden.

Yes

Gibt an, dass Daten in dem Speicherpool komprimiert werden. Dies ist der Standardwert.

### Beispiel: Einen Speicherpool aktualisieren, um eine maximale Anzahl Datensitzungen anzugeben

Einen Speicherpool mit dem Namen STGPOOL1 aktualisieren und ein Maximum von 10 Datensitzungen angeben.

```
update stgpool stgpool1 maxwriters=10
```

### Beispiel: Einen Speicherpool aktualisieren, um die maximale Größe anzugeben

Einen Speicherpool mit dem Namen STGPOOL2 aktualisieren. Der Speicherpool gibt als maximale Dateigröße 100 Megabyte an, die der Server im Speicherpool speichern kann.




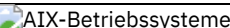
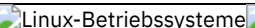
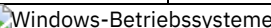
```
update stgpool stgpool2 maxsize=100M
```

### Beispiel: Die Beschreibung eines Speicherpools aktualisieren

Einen Speicherpool mit dem Namen STGPOOL3 aktualisieren. Die vorhandene Beschreibung aus dem Speicherpool entfernen.

```
update stgpool stgpool3 description=""
```

Tabelle 3. Zugehörige Befehle für UPDATE STGPOOL

| Befehl   | Beschreibung  |
|--|---|
| DEFINE STGPOOL   | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.                      |
| DEFINE STGPOOLDIRECTORY  | Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool. |
| PROTECT STGPOOL  | Schützt einen Verzeichniscontainerspeicherpool.   |
| QUERY CONTAINER  | Zeigt Informationen zu einem Container an.  |
| QUERY STGPOOL  | Zeigt Informationen zu Speicherpools an.  |
| REPAIR STGPOOL   | Repariert einen Verzeichniscontainerspeicherpool.   |
|  <br> UPDATE STGPOOLDIRECTORY | Ändert die Attribute eines Speicherpoolverzeichnisses.  |
|                               |   |

## UPDATE STGPOOL (Containerkopierspeicherpool aktualisieren)

Mit diesem Befehl kann ein Containerkopierspeicherpool aktualisiert werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool, der aktualisiert werden soll, erforderlich.

## Syntax

---

```
>>-UPDate STGpool--Poolname-----+----->
                               '-MAXSCRatch----Anzahl-'
>-----+----->
  '-DESCription----Beschreibung-'
>-----+----->
  '-ACCess-----+READWrite----+'
                    '+READOnly----+'
                    '-UNAVailable-'
>-----+-----+-----+----->
  '-PROTECTPRocess---Anzahl-'  '-REclaim---Prozent-'
>-----+-----+-----+----->
  '-RECLAIMLIMIT---+NOLimit-----+-'
                    '-Datenträgergrenzwert-'
>-----+-----+-----><
  '-REUsedelay----Tage-'
```

## Parameter

---

### Poolname (Erforderlich)

Gibt den Namen des Speicherpools an, der aktualisiert werden soll.

### MAXSCRatch

Gibt die maximale Anzahl der Arbeitsdatenträger an, die der Server für diesen Speicherpool anfordern kann. Sie können eine ganze Zahl im Bereich von 0 bis 100000000 angeben. Wenn der Server Arbeitsdatenträger nach Bedarf anfordern kann, müssen Sie nicht jeden zu verwendenden Datenträger definieren.

Mit dem Wert dieses Parameters wird die Gesamtzahl der im Speicherpool verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Speicherpools geschätzt.

### DESCription

Gibt eine Beschreibung des Speicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge ("" ) angeben.

### ACCess

Gibt an, wie Serverprozesse, wie z. B. Speicherpoolschutz und Reparatur, auf Daten in dem Speicherpool zugreifen können. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

#### READWrite

Gibt an, dass der Server Lese- und Schreibzugriff auf Datenträger in dem Speicherpool hat.

#### READOnly

Gibt an, dass der Server nur Lesezugriff auf Datenträger in dem Speicherpool hat. Der Server kann Daten in dem Speicherpool verwenden, um Bereiche in Verzeichniscontainerspeicherpools zurückzuschreiben. Operationen, mit denen Daten in den Containerkopierspeicherpool geschrieben werden, sind nicht zulässig.

#### UNAVailable

Gibt an, dass der Server nicht auf Daten zugreifen kann, die auf Datenträgern im Speicherpool gespeichert sind.

### PROTECTPRocess

Gibt die maximale Anzahl paralleler Prozesse an, die verwendet werden, wenn Sie den Befehl PROTECT STGPOOL ausgeben, um Daten aus einem Verzeichniscontainerspeicherpool in diesen Pool zu kopieren. Dieser Parameter ist wahlfrei. Geben Sie einen Wert im Bereich von 1 bis 20 ein.

Die Zeit, die für die Ausführung der Kopieroperation erforderlich ist, kann durch die Verwendung mehrerer Prozesse verringert werden. Sind mehrere Prozesse aktiv, müssen jedoch in einigen Fällen ein oder mehrere Prozesse auf die Verwendung eines Datenträgers warten, der bereits von einem anderen Prozess verwendet wird.

Berücksichtigen Sie bei der Festlegung dieses Werts die Anzahl der logischen und physischen Laufwerke, die dieser Operation zugeordnet werden können. Für den Zugriff auf einen Banddatenträger verwendet der Server einen Mountpunkt und ein Laufwerk. Die Anzahl verfügbarer Mountpunkte und Laufwerke ist von dem Mountlimit der Einheitenklasse für den Speicherpool und von anderen Server- und Systemaktivitäten abhängig.

Wenn Sie die Voranzeigeoption im Befehl PROTECT STGPOOL verwenden, wird nur ein Prozess verwendet und es werden keine Mountpunkte oder Laufwerke benötigt.

#### REClaim

Gibt an, wann ein Datenträger für die Konsolidierung und Wiederverwendung auswählbar ist. Geben Sie die Auswählbarkeit als Prozentsatz des Speicherbereichs eines Datenträgers an, der von Bereichen belegt ist, die nicht mehr im zugeordneten Verzeichniscontainerspeicherpool gespeichert werden. Bei der Konsolidierung werden alle Bereiche, die noch im zugeordneten Verzeichniscontainerspeicherpool gespeichert werden, von auswählbaren Datenträgern auf andere Datenträger versetzt. Die Konsolidierung erfolgt nur, wenn mit einem Befehl PROTECT STGPOOL Daten in diesem Speicherpool gespeichert werden.

Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl im Bereich von 1 bis 100 angeben. Der Wert 100 gibt an, dass keine Datenträger in diesem Speicherpool konsolidiert werden.

Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

Wird der Wert für 'Reclaim' auf 50 Prozent oder höher gesetzt, belegen Daten, die von zwei konsolidierten Datenträgern versetzt werden, maximal das Äquivalent eines neuen Datenträgers.

Gehen Sie mit Vorsicht vor, wenn Sie die Konsolidierung mit Containerkopierspeicherpools verwenden, die über ausgelagerte Datenträger verfügen. Wenn ein ausgelagerter Datenträger für die Konsolidierung auswählbar wird, werden die Bereiche auf dem Datenträger vom Server an den Standort vor Ort zurückversetzt. Wenn vor Ort ein Katastrophenfall eintritt, kann der Server Bereiche vom ausgelagerten Datenträger anfordern, wenn die zurückgeschriebene Datenbank auf Bereiche auf dem ausgelagerten Datenträger verweist. Stellen Sie daher zu Zwecken der Wiederherstellung nach einem Katastrophenfall sicher, dass Sie die Ausführung von Datenbanksicherungen planen, nachdem Speicherpoolschutzzeitpläne und DRM-Versetzungszeitpläne ausgeführt wurden, und stellen Sie sicher, dass alle Datenbanksicherungsdatenträger zusammen mit den DRM-Datenträgern ausgelagert werden.

Tipp: Definieren Sie verschiedene Konsolidierungswerte für Containerkopierspeicherpools an einem anderen Standort und Containerkopierspeicherpools vor Ort. Da Containerkopierspeicherpools deduplizierte Daten speichern, sind die Datenbereiche auf mehrere Banddatenträger verteilt. Wenn Sie einen Schwellenwert für die Konsolidierung für eine Kopie an einem anderen Standort auswählen, beachten Sie sorgfältig die Anzahl verfügbarer Mountpunkte und die Anzahl Banddatenträger, die abgerufen werden müssen, wenn ein Katastrophenfall eintritt. Wird ein höherer Schwellenwert definiert, bedeutet dies, dass Sie mehr Datenträger abrufen müssen als bei einem niedrigeren Konsolidierungswert. Bei Verwendung eines niedrigeren Schwellenwerts wird die Anzahl der Mountpunkte reduziert, die in einem Katastrophenfall erforderlich sind. Die bevorzugte Methode ist die Angabe des Konsolidierungswerts 60 für Kopien an einem anderen Standort. Für Kopien vor Ort liegt er im Bereich von 90 bis 100.

#### RECLAIMLimit

Gibt die maximale Anzahl von Datenträgern an, die der Server konsolidiert, wenn Sie den Befehl PROTECT STGPOOL ausgeben und die Option RECLAIM=YESLIMITED oder RECLAIM=ONLYLIMITED angeben. Dieser Parameter ist nur für Containerkopierspeicherpools gültig. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

##### NOLimit

Gibt an, dass alle Datenträger im Containerkopierspeicherpool für die Konsolidierung verarbeitet werden.

##### Datenträgergrenzwert

Gibt die maximale Anzahl der Datenträger im Containerkopierspeicherpool an, die konsolidiert werden. Der von Ihnen angegebene Wert bestimmt, wie viele neue Arbeitsbänder nach Abschluss der Konsolidierungsverarbeitung verfügbar sind. Sie können eine Zahl im Bereich von 1 bis 100000 angeben.

#### REUsedelay

Gibt die Anzahl Tage an, die nach dem Löschen aller Bereiche von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerstatus versetzt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl im Bereich von 0 bis 9999 angeben. Der Wert 0 bedeutet, dass ein Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerstatus versetzt werden kann, sobald alle Bereiche auf dem Datenträger gelöscht wurden.

Tipp: Mit diesem Parameter kann sichergestellt werden, dass Datenbankverweise auf Bereiche im Speicherpool noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird. Dieser Parameter muss auf einen Wert gesetzt werden, der größer als die Anzahl der Tage ist, die die älteste Datenbanksicherung aufbewahrt werden soll. Wenn Sie Disaster Recovery Manager verwenden, muss die für diesen Parameter angegebene Anzahl Tage mit der für den Befehl SET DRMDBBACKUPEXPIREDDAYS angegebenen Anzahl übereinstimmen.

## Beispiel: Einen Containerkopierspeicherpool aktualisieren, um die Verzögerungszeit für die Datenträgerwiederverwendung in 30 Tage zu ändern

Den Speicherpool mit dem Namen CONTAINER1\_COPY2 aktualisieren, um die Verzögerungszeit für die Datenträgerwiederverwendung in 30 Tage zu ändern.

```
update stgpool container1_copy2 reusedelay=30
```

## Beispiel: Einen Containerkopierspeicherpool aktualisieren, um die Anzahl der konsolidierten Banddatenträger auf 10 zu begrenzen

Den Speicherpool mit dem Namen CONTAINER1\_COPY2 aktualisieren, um den Konsolidierungsgrenzwert in 10 Datenträger zu ändern.

```
update stgpool container1_copy2 reclaimlimit=10
```

Tabelle 1. Zugehörige Befehle für UPDATE STGPOOL (Containerkopierspeicherpool aktualisieren)

| Befehl                                | Beschreibung  |
|---------------------------------------|---|
| DEFINE STGPOOL (Containerkopie)       | Definiert einen Containerkopierspeicherpool, in dem Kopien von Daten aus einem Verzeichniscontainerspeicherpool gespeichert werden. |
| PROTECT STGPOOL                       | Schützt einen Verzeichniscontainerspeicherpool.   |
| QUERY STGPOOL                         | Zeigt Informationen zu Speicherpools an.  |
| REPAIR STGPOOL                        | Repariert einen Verzeichniscontainerspeicherpool.   |
| UPDATE STGPOOL (Verzeichniscontainer) | Aktualisiert einen Verzeichniscontainerspeicherpool.  |

## UPDATE STGPOOL (Primären Speicherpool mit wahlfreiem Zugriff aktualisieren)

Mit diesem Befehl kann ein Speicherpool mit wahlfreiem Zugriff aktualisiert werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool, der aktualisiert werden soll, erforderlich.

### Syntax

```
>>-UPdate STGpool--Poolname--+-+-----+-----+----->
                                     '-DESCRiption---Beschreibung-'
>--+-----+-----+-----+-----+----->
   '-ACCess-----+READWrite----+'
                                     +-READOnly----+
                                     '-UNAVailable-'
>--+-----+-----+-----+-----+----->
   '-MAXSIze-----+maximale_Dateigröße-+-'
                                     '-NOLimit-----'
>--+-----+-----+-----+-----+----->
   '-CRCData-----+Yes-+-'   '-NEXTstgpool-----Poolname-'
                                     '-No--'
>--+-----+-----+-----+-----+----->
   '-Highmig-----Prozent-'   '-LOWmig-----Prozent-'
>--+-----+-----+-----+-----+----->
   '-CACHe-----+Yes-+-'   '-MIGPProcess-----Anzahl-'
                                     '-No--'
>--+-----+-----+-----+-----+----->
   '-MIGDelay-----Tage-'   '-MIGContinue-----+Yes-+-'
                                     '-No--'
>--+-----+-----+-----+-----+----->
   '-AUTOCopy-----+None-----+-'
                                     +-CLient----+
                                     +-MIGRation-+
                                     '-All-----'
>--+-----+-----+-----+-----+----->
   |                                     .-,-----+-----+-----|
   |                                     v                                     | |
```



Der Client schätzt die Größe der Dateien, die an den Server gesendet werden. Die Schätzung des Clients wird verwendet und nicht das tatsächliche Datenvolumen, das an den Server gesendet wird. Clientoptionen, wie z. B. Deduplizierung, Komprimierung und Verschlüsselung, können zur Folge haben, dass das tatsächliche Datenvolumen, das an den Server gesendet wird, größer oder kleiner als die Größenschätzung ist. Beispielsweise kann eine komprimierte Datei kleiner als die Schätzung sein, sodass weniger Daten als der Schätzwert gesendet werden. Des Weiteren kann eine Binärdatei nach der Komprimierungsverarbeitung größer sein, sodass mehr Daten als der Schätzwert gesendet werden.

Die folgende Tabelle enthält Informationen zur Speicherposition einer Datei, wenn ihre Größe den Wert des Parameters MAXSIZE überschreitet.

Tabelle 1. Speicherposition einer Datei gemäß der Dateigröße und dem angegebenen Pool

| Dateigröße                       | Angegebener Pool   | Ergebnis   |
|----------------------------------|--|--|
| Überschreitet die maximale Größe | Es ist kein Pool als nächster Speicherpool in der Hierarchie angegeben | Die Datei wird vom Server nicht gespeichert  |
|                                  | Ein Pool ist als nächster Speicherpool in der Hierarchie angegeben     | Der Server speichert die Datei im nächsten Speicherpool, der die Dateigröße akzeptiert |

Wenn Sie den Parameter für den nächsten Speicherpool angeben, definieren Sie einen einzelnen Speicherpool in Ihrer Hierarchie so, dass er keine Begrenzung hinsichtlich der maximalen Dateigröße hat. Verfügt mindestens ein Pool über keinen Grenzwert hinsichtlich der Größe, wird sichergestellt, dass der Server die Datei unabhängig von ihrer Größe speichern kann.

Bei mehreren Dateien, die in einer einzelnen Transaktion gesendet werden, betrachtet der Server die Größe der Transaktion als Dateigröße. Wenn die Gesamtgröße aller Dateien in der Transaktion die maximale Größe überschreitet, werden die Dateien vom Server nicht in dem Speicherpool gespeichert.

#### CRCData

Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCData auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

#### Yes

Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da mehr Aufwand erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

#### No

Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

#### NEXTstgpool

Gibt einen primären Speicherpool an, in den Dateien umgelagert werden. Dieser Parameter ist wahlfrei.

Soll ein bestehender Speicherpool aus der Speicherhierarchie entfernt werden, ist eine Nullzeichenfolge ("" ) für diesen Wert anzugeben.

Wird kein nächster Speicherpool angegeben, gilt Folgendes:

- Der Server kann keine Dateien aus diesem Speicherpool umlagern
- Der Server kann keine Dateien, die die maximale Größe für diesen Speicherpool überschreiten, in einem anderen Speicherpool speichern

#### Einschränkungen:

- Um sicherzustellen, dass keine Speicherpoolkette erstellt wird, die zu einer Endlosschleife führt, geben Sie mindestens einen Speicherpool in der Hierarchie ohne Wert an.
- Wenn Sie einen Pool mit sequenziellem Zugriff als nächsten Speicherpool angeben, muss der Pool entweder das Datenformat NATIVE oder NONBLOCK haben.
- Geben Sie keinen Verzeichniscontainer- oder Cloud-Containerspeicherpool an.
- Verwenden Sie diesen Parameter nicht, um einen Speicherpool für die Datenumlagerung anzugeben.

#### HIGHmig

Gibt an, dass der Server die Umlagerung für diesen Speicherpool startet, wenn der Datenumfang in dem Pool diesen Prozentsatz der geschätzten Kapazität des Pools erreicht. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 100 angeben.

Wenn der Speicherpool die obere Umlagerungsschwelle überschreitet, kann der Server die Umlagerung von Dateien in den nächsten Speicherpool (wie im Parameter NEXTSTGPOOL definiert) nach Knotennamen starten. Bei Angabe von HIGHMIG=100 wird die Umlagerung für diesen Speicherpool verhindert.



## LOWmig

Gibt an, dass der Server die Umlagerung für diesen Speicherpool stoppt, wenn der Datenumfang in dem Pool diesen Prozentsatz der geschätzten Kapazität des Pools erreicht. Sie können eine ganze Zahl von 0 bis 99 für diesen optionalen Parameter angeben.

Wenn die Umlagerung nach Knoten oder Dateibereich erfolgt (abhängig von der Kollokation), kann der Wert für den Speicherpool unter den für diesen Parameter angegebenen Wert fallen. Um den Speicherpool zu leeren, definieren Sie LOWMIG=0.

## CAChe

Gibt an, ob der Umlagerungsprozess eine Cachekopie einer Datei in diesem Speicherpool zurücklässt, nachdem die Datei in den nächsten Speicherpool umgelagert wurde. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

Yes

Caching ist aktiviert.

No

Caching ist inaktiviert.

Die Verwendung von Cache kann die Abrufbarkeit von Dateien verbessern, kann jedoch die Leistung anderer Prozesse negativ beeinflussen.

## MIGPProcess

Gibt die Anzahl Prozesse an, die zum Umlagern von Dateien aus diesem Speicherpool verwendet werden. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 999 angeben.

Während der Umlagerung werden diese Prozesse parallel ausgeführt, um die Umlagerungsgeschwindigkeit zu verbessern.

Tipps:

- Die Anzahl der Umlagerungsprozesse ist von den folgenden Einstellungen abhängig:
  - Einstellung des Parameters MIGPROCESS
  - Kollokationseinstellung des nächsten Pools
  - Anzahl der Knoten oder Anzahl der Kollokationsgruppen mit Daten in dem Speicherpool, der umgelagert wirdFür dieses Beispiel wird angenommen, dass MIGPROCESS =6 angegeben und der Parameter COLLOCATE für den nächsten Pool auf NODE gesetzt ist, aber nur zwei Knoten mit Daten in dem Speicherpool vorhanden sind. Die Umlagerungsverarbeitung besteht nur aus zwei, nicht sechs Prozessen. Wird der Parameter COLLOCATE auf GROUP gesetzt und befinden sich beide Knoten in derselben Gruppe, besteht die Umlagerungsverarbeitung nur aus einem Prozess. Wird der Parameter COLLOCATE auf NO oder FILESPACE gesetzt und hat jeder Knoten zwei Dateibereiche mit Sicherungsdaten, besteht die Umlagerungsverarbeitung nur aus vier Prozessen.
- Beachten Sie bei der Angabe dieses Parameters, ob die Funktion für simultanes Schreiben für die Serverdatenumlagerung aktiviert ist. Jeder Umlagerungsprozess erfordert einen Mountpunkt und ein Laufwerk für jeden Kopierspeicherpool und Pool für aktive Daten, der für den Zielspeicherpool definiert ist.

## MIGDelay

Gibt die Mindestanzahl Tage an, die eine Datei in einem Speicherpool verbleiben muss, bevor sie für die Umlagerung ausgewählt werden kann. Um einen Wert zu berechnen, der mit dem angegebenen Wert für MIGDELAY verglichen wird, zählt der Server:

- Die Anzahl der Tage, die die Datei im Speicherpool war
- Die Anzahl der Tage (falls zutreffend), seit die Datei von einem Client abgerufen wurde

Der kleinere der beiden Werte wird mit dem angegebenen Wert für MIGDELAY verglichen. Beispiel: Sind alle folgenden Bedingungen wahr, wird eine Datei nicht umgelagert:

- Eine Datei war fünf Tage in einem Speicherpool.
- Auf die Datei wurde innerhalb der letzten drei Tage von einem Client zugegriffen.
- Der für den Parameter MIGDELAY angegebene Wert beträgt vier Tage.

Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Standardwert 0 gibt an, dass die Umlagerung nicht verzögert werden soll.

Soll der Server die Anzahl der Tage ab dem Tag zählen, an dem eine Datei gespeichert wurde, und nicht ab dem Tag, an dem sie abgerufen wurde, die Serveroption NORETRIEVEDATE verwenden.

## MIGContinue

Gibt an, ob der Server Dateien umlagern darf, die der Verzögerungszeit für die Umlagerung nicht entsprechen. Dieser Parameter ist wahlfrei.

Da angegeben werden kann, dass Dateien eine Mindestanzahl Tage in dem Speicherpool verbleiben müssen, kann der Server alle auswählbaren Dateien in den nächsten Speicherpool umlagern, obwohl sie dem Wert für die untere Umlagerungsschwelle nicht entsprechen. Mit diesem Parameter kann angegeben werden, ob der Server den Umlagerungsprozess fortsetzen darf, indem Dateien umgelagert werden, die der Verzögerungszeit für die Umlagerung nicht entsprechen.

Sie können einen der folgenden Werte angeben:

Yes

Muss die untere Umlagerungsschwelle eingehalten werden, gibt dieser Wert an, dass der Server mit der Umlagerung von Dateien fortfährt, die der Verzögerungszeit für die Umlagerung nicht entsprechen.

Sind mehrere Umlagerungsprozesse für den Speicherpool zulässig, werden einige Dateien, die der Verzögerungszeit für die Umlagerung nicht entsprechen, unter Umständen unnötigerweise umgelagert. Während ein Prozess Dateien umlagert, die der Verzögerungszeit für die Umlagerung entsprechen, könnte ein zweiter Prozess mit der Umlagerung von Dateien beginnen, die der Verzögerungszeit für die Umlagerung nicht entsprechen, um die untere Umlagerungsschwelle einzuhalten. Der erste Prozess, der noch Dateien umlagert, die der Verzögerungszeit für die Umlagerung entsprechen, könnte selbst die Einhaltung der unteren Umlagerungsschwelle bewirkt haben.

No

Gibt an, dass der Server die Umlagerung stoppt, wenn keine auswählbaren Dateien mehr für die Umlagerung verfügbar sind; dies gilt auch vor Erreichen der unteren Umlagerungsschwelle. Der Server lagert nur Dateien um, die der Verzögerungszeit für die Umlagerung entsprechen.

AUTOCopy

Gibt an, wann IBM Spectrum Protect Operationen für gleichzeitiges Schreiben in Kopierspeicherpools und Pools für aktive Daten ausführt. Dieser Parameter betrifft die folgenden Operationen:

- Clientspeichersitzungen
- Serverimportprozesse
- Serverdatenumlagerungsprozesse

Tritt ein Fehler auf, wenn Daten während eines Umlagerungsprozesses gleichzeitig in einen Kopierspeicherpool oder einen Pool für aktive Daten geschrieben werden, stoppt der Server das Schreiben in die fehlerhaften Speicherpools für den Rest des Prozesses. Der Server speichert jedoch weiterhin Dateien in dem primären Speicherpool und in allen verbleibenden Kopierspeicherpools oder Pools für aktive Daten. Diese Pools bleiben für die Dauer des Umlagerungsprozesses aktiv. Kopierspeicherpools werden mit dem Parameter COPYSTGPOLS angegeben. Pools für aktive Daten werden mit dem Parameter ACTIVEDATAPOOLS angegeben.

Sie können einen der folgenden Werte angeben:

None

Gibt an, dass die Funktion für simultanes Schreiben inaktiviert ist.

Client

Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen oder Serverimportprozessen gleichzeitig in Kopierspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverimportprozessen werden Daten nur gleichzeitig in Kopierspeicherpools geschrieben. Daten werden während der Ausführung von Serverimportprozessen nicht in Pools für aktive Daten geschrieben.

MIGRATION

Gibt an, dass Daten nur während der Umlagerung in diesen Speicherpool gleichzeitig in Kopierspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverdatenumlagerungsprozessen werden Daten in Kopierspeicherpools und Pools für aktive Daten nur dann gleichzeitig geschrieben, wenn die Daten in diesen Pools nicht vorhanden sind. Knoten, deren Daten umgelagert werden, müssen sich in einer Domäne befinden, die einem Pool für aktive Daten zugeordnet ist. Befinden sich die Knoten nicht in einer Domäne, die einem Pool für aktive Daten zugeordnet ist, können die Daten nicht in den Pool geschrieben werden.

All

Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen, Serverimportprozessen oder Serverdatenumlagerungsprozessen gleichzeitig in Kopierspeicherpools und Pools für aktive Daten geschrieben werden. Mit diesem Wert wird sichergestellt, dass Daten immer dann gleichzeitig geschrieben werden, wenn dieser Pool ein Ziel für eine der auswählbaren Operationen ist.

COPYSTGPools

Gibt die Namen von Kopierspeicherpools an, in die der Server gleichzeitig Daten schreibt. Sie können maximal drei Kopienpoolnamen angeben, die durch Kommas voneinander getrennt werden müssen. Leerzeichen zwischen den Namen der Kopienpools sind nicht zulässig. Um einen oder mehrere Kopierspeicherpools hinzuzufügen oder zu entfernen, geben Sie den oder die Poolnamen an, der bzw. die in der aktualisierten Liste enthalten sein soll(en). Enthält die vorhandene Kopienpoolliste beispielsweise COPY1 und COPY2 und soll COPY3 hinzugefügt werden, geben Sie COPYSTGPOLS=COPY1,COPY2,COPY3 an. Um alle vorhandenen Kopierspeicherpools zu entfernen, die dem primären Speicherpool zugeordnet sind, geben Sie eine Nullzeichenfolge ("" ) für den Wert an (beispielsweise COPYSTGPOLS="").

Wenn Sie einen Wert für den Parameter COPYSTGPOLS angeben, können Sie auch einen Wert für den Parameter COPYCONTINUE angeben. Weitere Informationen enthält die Beschreibung des Parameters COPYCONTINUE.

Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSGTPOOLS und ACTIVEATAPOOLS angegeben sind, darf drei nicht überschreiten.

Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Kopierspeicherpools und den Wert für COPYCONTINUE aus dem primären Speicherpool. Der primäre Speicherpool wird durch die Kopiergruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

Der Server kann bei den folgenden Operationen Daten gleichzeitig in Kopierspeicherpools schreiben:

- Sicherungs- und Archivierungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder Anwendungsclients, die die IBM Spectrum Protect-API verwenden
- Umlagerungsoperationen durch IBM Spectrum Protect for Space Management-Clients
- Importoperationen, die das Kopieren von exportierten Dateidaten von externen Datenträgern in einen primären Speicherpool einbeziehen, der einer Kopierspeicherpoolliste zugeordnet ist

Einschränkungen: Die Funktion für simultanes Schreiben wird für die folgenden Speicheroperationen nicht unterstützt:

- Wenn die Operation die LAN-unabhängige Datenversetzung verwendet. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch akzeptiert.
- NAS-Sicherungsoperationen. Sind für den primären Speicherpool, der in DESTINATION oder TOCDESTINATION in der Kopiergruppe der Verwaltungsklasse angegeben ist, Kopierspeicherpools definiert, werden
  - die Kopierspeicherpools ignoriert.
  - die Daten nur im primären Speicherpool gespeichert.

Achtung: Die mit dem Parameter COPYSTGPOOLS zur Verfügung gestellte Funktion soll nicht den Befehl BACKUP STGPOOL ersetzen. Wird der Parameter COPYSTGPOOLS verwendet, verwenden Sie weiterhin den Befehl BACKUP STGPOOL, um sicherzustellen, dass die Kopierspeicherpools vollständige Kopien des primären Speicherpools sind. Es gibt Fälle, in denen eine Kopie möglicherweise nicht erstellt wird. Weitere Informationen enthält die Beschreibung des Parameters COPYCONTINUE.

#### COPYContinue

Gibt an, wie der Server auf einen Fehler beim Schreiben in einen der Kopierspeicherpools reagiert, die im Parameter COPYSTGPOOLS aufgelistet sind. Dieser Parameter ist wahlfrei. Wenn Sie den Parameter COPYCONTINUE angeben, muss entweder eine COPYSTGPOOLS-Liste vorhanden sein oder der Parameter COPYSTGPOOLS muss ebenfalls angegeben werden. Sie können die folgenden Werte angeben:

#### Yes

Ist der Parameter COPYCONTINUE auf YES gesetzt, stoppt der Server das Schreiben in die fehlerhaften Kopienpools für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Kopienpools fort. Die Liste der Kopierspeicherpools ist nur für die Dauer der Clientsitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.

#### No

Ist der Parameter COPYCONTINUE auf NO gesetzt, wird die aktuelle Transaktion vom Server nicht ausgeführt und die Speicheroperation nicht fortgesetzt.

Einschränkungen:

- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf Pools für aktive Daten. Tritt für einen der Pools für aktive Daten ein Schreibfehler auf, stoppt der Server das Schreiben in den fehlerhaften Pool für aktive Daten für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Pools für aktive Daten und Kopierspeicherpools fort. Die Liste der Pools für aktive Daten ist nur für die Dauer der Sitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.
- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Ausführung eines Serverimportprozesses. Werden Daten gleichzeitig geschrieben und tritt für den primären Speicherpool oder einen Kopierspeicherpool ein Schreibfehler auf, schlägt der Serverimportprozess fehl.
- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Serverdatenumlagerung. Werden Daten gleichzeitig geschrieben und tritt für einen Kopierspeicherpool oder Pool für aktive Daten ein Schreibfehler auf, wird der fehlerhafte Speicherpool entfernt und der Datenumlagerungsprozess wird fortgesetzt. Bei Schreibfehlern für den primären Speicherpool schlägt der Umlagerungsprozess fehl.

#### ACTIVEATApools

Gibt die Namen der Pools für aktive Daten an, in die der Server während einer Clientsicherungsoperation gleichzeitig Daten schreibt. Der Parameter ACTIVEATAPOOLS ist optional. Leerzeichen zwischen den Namen der Pools für aktive Daten sind nicht zulässig.

Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSGTPOOLS und ACTIVEATAPOOLS angegeben sind, darf drei nicht überschreiten.

Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Pools für aktive Daten aus dem Zielspeicherpool, der in der Kopiengruppe angegeben ist. Der primäre Speicherpool wird durch die Kopiengruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

Der Server kann nur während Sicherungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder durch Anwendungsclients, die die IBM Spectrum Protect-API verwenden, Daten gleichzeitig in Pools für aktive Daten schreiben. Einschränkungen:

1. Dieser Parameter ist nur für primäre Speicherpools verfügbar, die das Datenformat "NATIVE" oder "NONBLOCK" verwenden. Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
  - o NETAPPDUMP
  - o CELERRADUMP
  - o NDMPDUMP
2. Das simultane Schreiben in Pools für aktive Daten wird nicht unterstützt, wenn die LAN-unabhängige Datenversetzung verwendet wird. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch berücksichtigt.
3. Die Funktion für simultanes Schreiben wird nicht unterstützt, wenn eine NAS-Sicherungsoperation eine Inhaltsverzeichnisdatei schreibt. Sind für den primären Speicherpool, der in TOCDESTINATION in der Kopiengruppe der Verwaltungsklasse angegeben ist, Pools für aktive Daten definiert, werden
  - o die Pools für aktive Daten ignoriert.
  - o die Daten nur im primären Speicherpool gespeichert.
4. Die Funktion für simultanes Schreiben kann mit CENTERA-Speichereinheiten nicht verwendet werden.
5. Daten, die importiert werden, werden nicht in Pools für aktive Daten gespeichert. Verwenden Sie nach einer Importoperation den Befehl COPY ACTIVE DATA, um die importierten Daten in einem Pool für aktive Daten zu speichern.

Achtung: Die mit dem Parameter ACTIVE DATA POOLS zur Verfügung gestellte Funktion soll nicht den Befehl COPY ACTIVE DATA ersetzen. Wird der Parameter ACTIVE DATA POOLS verwendet, verwenden Sie den Befehl COPY ACTIVE DATA, um sicherzustellen, dass die Pools für aktive Daten alle aktiven Daten des primären Speicherpools enthalten.

#### SHRED

Gibt an, ob Daten beim Löschen physisch überschrieben werden. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 10 angeben.

Wird der Wert Null angegeben, löscht der Server die Daten aus der Datenbank. Der Speicher, in dem die Daten gespeichert waren, wird jedoch nicht überschrieben, und die Daten sind weiterhin im Speicher vorhanden, bis dieser Speicher für andere Daten wiederverwendet wird. Möglicherweise können die Daten nach dem Löschen erkannt und wiederhergestellt werden. Die Änderung des Werts (beispielsweise das Zurücksetzen auf 0) hat keinen Einfluss auf Daten, die gelöscht wurden und gegenwärtig darauf warten, überschrieben zu werden.

Wenn Sie einen Wert größer als 0 angeben, löscht der Server die Daten sowohl logisch als auch physisch. Der Server überschreibt den Speicher, in dem die Daten gespeichert waren, so oft wie angegeben wurde. Durch das Überschreiben wird es schwieriger, die Daten zu erkennen und wiederherzustellen, nachdem sie gelöscht wurden.

Um sicherzustellen, dass alle Kopien der Daten geschreddert werden, geben Sie einen SHRED-Wert größer als Null für den im Parameter NEXT STG POOL angegebenen Speicherpool an. Geben Sie nicht COPY STG POOLS oder ACTIVE DATA POOLS an. Durch die Angabe relativ hoher Werte für die Anzahl Überschreibungen wird im Allgemeinen die Sicherheitsstufe erhöht, aber sie kann umgekehrt die Leistung beeinflussen.

Das Überschreiben gelöschter Daten wird asynchron ausgeführt, nachdem die Löschoption abgeschlossen ist. Daher bleibt der durch die gelöschten Daten belegte Speicherbereich für einige Zeit belegt. Der Speicherbereich ist nicht als freier Speicherbereich für neue Daten verfügbar.

Ein SHRED-Wert größer als null kann nicht verwendet werden, wenn der Parameter CACHE den Wert YES hat. Soll das Schreddern für einen vorhandenen Speicherpool aktiviert werden, für den das Caching bereits aktiviert ist, müssen Sie den Wert des Parameters CACHE in NO ändern. Vorhandene zwischengespeicherte Dateien verbleiben im Speicher, so dass nachfolgende Abrufanforderungen schnell erfüllt werden können. Wird Speicherbereich zum Speichern neuer Daten benötigt, werden die vorhandenen zwischengespeicherten Dateien gelöscht, so dass der von ihnen belegte Speicherbereich für die neuen Daten verwendet werden kann. Die vorhandenen zwischengespeicherten Dateien werden nach dem Löschen nicht geschreddert. Wichtig: Nachdem eine Exportoperation die Identifizierung von Dateien für den Export beendet hat, werden alle Änderungen des Werts SHRED für den Speicherpool ignoriert. Eine Exportoperation, die ausgesetzt ist, behält während der gesamten Operation den ursprünglichen SHRED-Wert. Möglicherweise möchten Sie Ihre Exportoperation abbrechen, wenn Änderungen des Werts SHRED für den Speicherpool die Operation gefährden. Sie können den Exportbefehl nach einer erforderlichen Bereinigung erneut ausgeben.

### **Beispiel: Einen Speicherpool mit wahlfreiem Zugriff aktualisieren, um das Caching zu erlauben**

Den Speicherpool mit wahlfreiem Zugriff mit dem Namen BACKUPPOOL aktualisieren, um Caching zu erlauben, wenn der Server Dateien in den nächsten Speicherpool umlagert.

```
update stgpool backuppool cache=yes
```

## UPDATE STGPOOL (Primären Speicherpool mit sequenziellem Zugriff aktualisieren)

Mit diesem Befehl kann ein primärer Speicherpool mit sequenziellem Zugriff aktualisiert werden.

Einschränkungen:

1. Sie können diesen Befehl nicht verwenden, um das Datenformat für den Speicherpool zu ändern.
2. Hat DATAFORMAT den Wert NETAPPDUMP, CELERRADUMP oder NDMPDUMP, können Sie nur die folgenden Attribute ändern:
  - o DESCRIPTION
  - o ACCESS
  - o COLLOCATE
  - o MAXSCRATCH
  - o REUSEDELAY

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool, der aktualisiert werden soll, erforderlich.

### Syntax

```
>>-UPDate STGpool--Poolname--+-+-----+-----+-----+----->
                                     '-DESCription-----Beschreibung-'
>+-----+-----+-----+-----+-----+-----+-----+----->
  '-ACCess-----+READWrite-----+'
                    +-READOnly-----+
                    '-UNAVailable-'
>+-----+-----+-----+-----+-----+-----+-----+----->
  |                                     (1) (2) |
  '-MAXSIze-----+maximale_Dateigröße+-----+'
                    '-NOLimit-----+'
>+-----+-----+-----+-----+-----+-----+-----+----->
  |                                     (1) |
  '-CRCData-----+Yes+-----+'
                    '-No--'
>+-----+-----+-----+-----+-----+-----+-----+----->
  |                                     (1) (2) |
  '-NEXTstgpool-----Poolname-----+'
>+-----+-----+-----+-----+-----+-----+-----+----->
  |                                     (1) (2) |
  '-HIghmig-----Prozent-----+'
>+-----+-----+-----+-----+-----+-----+-----+----->
  |                                     (1) (2) |
  '-LOWmig-----Prozent-----+'
>+-----+-----+-----+-----+-----+-----+-----+----->
  |                                     (1) (2) |
  '-REClaim-----Prozent-----+'
>+-----+-----+-----+-----+-----+-----+-----+----->
  |                                     (1) (2) |
  '-RECLAIMPRocess-----Anzahl-----+'
>+-----+-----+-----+-----+-----+-----+-----+----->
  |                                     (1) (2) |
  '-RECLAIMSTGpool-----Poolname-----+'
>+-----+-----+-----+-----+-----+-----+-----+----->
```

```

| (2) |
|'-COLlocate--==+-No-----+'
|   +-GrouP-----+
|   +-NODe-----+
|   '-Filespace-'
>----->
| (2) | | (2) |
|'-MAXSCRatch----Anzahl-----' '-REUsedelay----Tage-----'
>----->
| (1) (2) |
|'-OVFLocation----Standort-----'
>----->
| (1) (2) |
|'-MIGDelay----Tage-----'
>----->
| (1) (2) |
|'-MIGContinue----+Yes-----+'
|   '-No--'
>----->
| (1) (2) |
|'-MIGPRocess----Anzahl-----'
>----->
|'-AUTOCopy----+None-----+'
|   +-CLient----+
|   +-MIGRation+
|   '-All-----'
>----->
| .-,-----+ |
| V (1) (2) | |
|'-COPYSTGpools----Name_des_Kopienpools-----+'
>----->
| (1) (2) |
|'-COPYContinue----+Yes-----+'
|   '-No--'
>----->
| .-,-----+ |
| V | |
|'-ACTIVEDATApools----Name_des_Pools_für_aktive_Daten-----+'
>----->
|'-DEDuplicate----+No-----+'
|   | (3) |
|   '-Yes-----'
>-----<
| (4) |
|'-IDENTIFYPRocess----Anzahl-----'

```

#### Anmerkungen:

1. Dieser Parameter ist für Speicherpools, die das Datenformat NETAPPDUMP, CELERRADUMP oder NDMPDUMP verwenden, nicht verfügbar.
2. Dieser Parameter ist für CENTERA-Speicherpools nicht verfügbar.
3. Dieser Parameter ist nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.
4. Dieser Parameter ist nur verfügbar, wenn der Parameter DEDUPLICATE den Wert YES hat.

## Parameter

#### Poolname (Erforderlich)

Gibt den Namen des Speicherpools an, der aktualisiert werden soll.

#### DESCRIPTION

Gibt eine Beschreibung des Speicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge ("" ) angeben.

#### ACCESS

Gibt an, wie Clientknoten und Serverprozesse (wie Umlagerung und Wiederherstellung) auf Dateien im Speicherpool zugreifen können. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

**READWrite**

Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff auf Dateien haben, die auf Datenträgern in dem Speicherpool gespeichert sind.

**READOnly**

Gibt an, dass Clientknoten Dateien auf den Datenträgern im Speicherpool nur lesen können.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Für die Datenträger in dem Speicherpool sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig.

Wenn dieser Speicherpool als untergeordneter Speicherpool angegeben (mit dem Parameter NEXTSTGPOOL) und als *readonly (schreibgeschützt)* definiert wurde, wird der Speicherpool übersprungen, wenn Serverprozesse versuchen, Dateien in den Speicherpool zu schreiben.

**UNAVailable**

Gibt an, dass Clientknoten nicht auf Dateien, die auf Datenträgern im Speicherpool gespeichert sind, zugreifen können.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Außerdem können sie Dateien aus diesem Speicherpool in einen anderen Speicherpool versetzen oder kopieren. Für die Datenträger in dem Speicherpool sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig.

Wenn dieser Speicherpool als untergeordneter Speicherpool angegeben (mit dem Parameter NEXTSTGPOOL) und als *unavailable (nicht verfügbar)* definiert wurde, wird der Speicherpool übersprungen, wenn Serverprozesse versuchen, Dateien in den Speicherpool zu schreiben.

**MAXSIze**

Gibt die maximale Größe einer physischen Datei an, die der Server in dem Speicherpool speichern kann. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

**NOLimit**

Gibt an, dass für die im Speicherpool gespeicherten physischen Dateien keine Größenbeschränkung besteht.

**maximale\_Dateigröße**

Begrenzt die maximale Größe für physische Dateien. Geben Sie eine ganze Zahl zwischen 1 und 999999 Terabyte gefolgt von einem Maßstabsfaktor an. MAXSIZE=5G gibt z. B. an, dass die maximale Dateigröße für diesen Speicherpool 5 Gigabyte ist. Maßstabsfaktoren sind:

| Maßstabsfaktor | Bedeutung |
|----------------|-----------|
| K              | Kilobyte  |
| M              | Megabyte  |
| G              | Gigabyte  |
| T              | Terabyte  |

Der Client schätzt die Größe der Dateien, die an den Server gesendet werden. Die Schätzung des Clients wird verwendet und nicht das tatsächliche Datenvolumen, das an den Server gesendet wird. Clientoptionen, wie z. B. Deduplizierung, Komprimierung und Verschlüsselung, können zur Folge haben, dass das tatsächliche Datenvolumen, das an den Server gesendet wird, größer oder kleiner als die Größenschätzung ist. Beispielsweise kann eine komprimierte Datei kleiner als die Schätzung sein, sodass weniger Daten als der Schätzwert gesendet werden. Des Weiteren kann eine Binärdatei nach der Komprimierungsverarbeitung größer sein, sodass mehr Daten als der Schätzwert gesendet werden.

Wenn die physische Größe des Speicherpools den Wert des Parameters MAXSIZE überschreitet, zeigt die folgende Tabelle an, wo Dateien normalerweise gespeichert werden.

**Tabelle 1. Position einer Datei gemäß der Dateigröße und dem angegebenen Pool**

| Dateigröße                       | Angegebener Pool   | Ergebnis   |
|----------------------------------|--|--|
| Überschreitet die maximale Größe | Es ist kein Pool als nächster Speicherpool in der Hierarchie angegeben | Die Datei wird vom Server nicht gespeichert  |
|                                  | Ein Pool ist als nächster Speicherpool in der Hierarchie angegeben     | Der Server speichert die Datei im nächsten Speicherpool, der die Dateigröße akzeptiert |

Tipp: Wenn Sie auch den Parameter NEXTstgpool angeben, definieren Sie einen einzelnen Speicherpool in Ihrer Hierarchie so, dass er keine Begrenzung hinsichtlich der maximalen Dateigröße hat, indem Sie den Parameter MAXSIZE=NOLimit angeben. Wenn mindestens ein Pool keine Größenbegrenzung hat, wird sichergestellt, dass der Server die Datei unabhängig von ihrer Größe speichern kann.

Bei mehreren Dateien, die in einer einzelnen Transaktion gesendet werden, betrachtet der Server die Größe der Transaktion als Dateigröße. Wenn die Gesamtgröße aller Dateien in der Transaktion die maximale Größe überschreitet, werden die Dateien vom Server nicht in dem Speicherpool gespeichert.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### CRCData

Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist nur für Speicherpools mit dem Datenformat NATIVE gültig. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCDATA auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

Yes

Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da eine zusätzliche Verarbeitung erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

No

Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

Tipp:

Für Speicherpools, die dem Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet sind, bietet der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust als die CRC-Überprüfung für einen Speicherpool. Wenn Sie die CRC-Überprüfung für einen Speicherpool angeben, werden Daten nur während der Ausführung von Datenträgerprüfungsoperationen überprüft. Fehler werden identifiziert, nachdem Daten auf Band geschrieben wurden.

Um den Schutz logischer Blöcke zu aktivieren, geben Sie den Wert READWRITE für den Parameter LBPROTECT in den Befehlen DEFINE DEVCLASS und UPDATE DEVCLASS für den Einheitentyp 3592, LTO oder ECARTRIDGE an. Der Schutz logischer Blöcke wird nur für die folgenden Typen von Laufwerken und Datenträgern unterstützt:

- IBM® LTO5 und höher
- IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
- Oracle StorageTek T10000C- und T10000D-Laufwerke

#### NEXTstgpool

Gibt einen primären Speicherpool an, in den Dateien umgelagert werden. Sie können keine Daten aus einem Speicherpool mit sequenziellem Zugriff in einen Speicherpool mit wahlfreiem Zugriff umlagern. Dieser Parameter ist wahlfrei. Der nächste Speicherpool muss ein primärer Speicherpool sein.

Soll ein vorhandener Wert entfernt werden, eine Nullzeichenfolge ("" ) angeben.

Verfügt dieser Speicherpool nicht über einen nächsten Speicherpool, kann der Server nicht Dateien aus diesem Speicherpool umlagern und Dateien, die die maximale Größe für diesen Speicherpool überschreiten, nicht in einem anderen Speicherpool speichern.

Ist in dem aktuellen Speicherpool nicht genügend Speicherbereich verfügbar, erlaubt der Parameter NEXTSTGPOOL für Speicherpools mit sequenziellem Zugriff nicht das Speichern von Daten im nächsten Pool. In diesem Fall gibt der Server eine Nachricht aus, und die Transaktion schlägt fehl.

Für nächste Speicherpools mit dem Einheitentyp FILE führt der Server eine vorläufige Überprüfung durch, um zu bestimmen, ob genügend Speicherbereich verfügbar ist. Ist kein Speicherbereich verfügbar, springt der Server zum nächsten Speicherpool in der Hierarchie. Ist Speicherbereich verfügbar, versucht der Server, Daten in diesem Pool zu speichern. Die Speicheroperation kann jedoch fehlschlagen, wenn zum Zeitpunkt der tatsächlichen Speicheroperation der Speicherbereich nicht mehr verfügbar ist.

Einschränkungen:

- Um sicherzustellen, dass keine Speicherpoolkette erstellt wird, die zu einer Endlosschleife führt, geben Sie mindestens einen Speicherpool in der Hierarchie ohne Wert an.
- Wenn Sie einen Pool mit sequenziellem Zugriff als nächsten Speicherpool angeben, muss der Pool entweder das Datenformat NATIVE oder NONBLOCK haben.
- Geben Sie keinen Verzeichniscontainer- oder Cloud-Containerspeicherpool an.
- Verwenden Sie diesen Parameter nicht, um einen Speicherpool für die Datenumlagerung anzugeben.
- Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
  - NETAPPDUMP



- CELERRADUMP
- NDMPDUMP

#### Highmig

Gibt an, dass der Server die Umlagerung startet, wenn die Speicherpoolauslastung diesen Prozentsatz erreicht. Für Plattenspeicherpools mit sequenziellem Zugriff (FILE) ist die Auslastung das Verhältnis der Daten in einem Speicherpool zur Summe der geschätzten Datenkapazität des Pools, einschließlich der Kapazität aller für den Pool angegebenen Arbeitsdatenträger. Für Speicherpools, die Banddatenträger verwenden, ist die Auslastung das Verhältnis der Datenträger, die Daten enthalten, zur Gesamtzahl der Datenträger in dem Speicherpool. Die Gesamtzahl der Datenträger schließt die maximale Anzahl Arbeitsdatenträger ein. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 100 angeben.

Wenn der Speicherpool die obere Umlagerungsschwelle überschreitet, kann der Server die Umlagerung von Dateien in den nächsten definierten Speicherpool nach Datenträger starten. Die obere Umlagerungsschwelle kann auf 100 gesetzt werden, um die Umlagerung für den Speicherpool zu verhindern.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### LOwmig

Gibt an, dass der Server die Umlagerung stoppt, wenn die Speicherpoolauslastung diesen Prozentsatz erreicht oder unter diesem Prozentsatz liegt. Für Plattenspeicherpools mit sequenziellem Zugriff (FILE) ist die Auslastung das Verhältnis der Daten in einem Speicherpool zur Summe der geschätzten Datenkapazität des Pools, einschließlich der Kapazität aller für den Pool angegebenen Arbeitsdatenträger. Für Speicherpools, die Banddatenträger verwenden, ist die Auslastung das Verhältnis der Datenträger, die Daten enthalten, zur Gesamtzahl der Datenträger in dem Speicherpool. Die Gesamtzahl der Datenträger schließt die maximale Anzahl Arbeitsdatenträger ein. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 99 angeben.

Wenn der Speicherpool die untere Umlagerungsschwelle erreicht, wird die Umlagerung von Dateien von einem anderen Datenträger von dem Server nicht gestartet. Die Angabe von 0 für die untere Umlagerungsschwelle erlaubt eine Umlagerung, um den Speicherpool zu leeren.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP


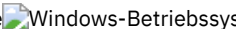
#### REclaim

Gibt an, wann der Server einen Datenträger auf der Basis des Prozentsatzes wiederherstellbaren Speicherbereichs auf einem Datenträger zurückfordert. Der wiederherstellbare Speicherbereich ist der Speicherbereich, der durch Dateien belegt ist, die verfallen sind oder aus der IBM Spectrum Protect-Datenbank gelöscht wurden.

Bei der Wiederherstellung wird der zerstückelte Speicherbereich auf Datenträgern durch Versetzen der restlichen nicht verfallenen Dateien von einem Datenträger auf einen anderen wieder verwendbar, wodurch der ursprüngliche Datenträger wiederverwendet werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 100 angeben.

Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

Einen Wert von 50 Prozent oder höher für diesen Parameter angeben, so dass Dateien, die auf zwei Datenträgern gespeichert sind, auf einem einzigen Ausgabedatenträger gespeichert werden können.

  Für Speicherpools, die eine Einheitenklasse WORM verwenden, kann der Standardwert 100 verringert werden. Damit wird es dem Server ermöglicht, Daten bei Bedarf auf weniger Datenträger zusammenzulegen. Datenträger, die durch die Wiederherstellung geleert werden, können aus dem Kassettenarchiv entnommen werden, wodurch Schächte für neue Datenträger freigegeben werden. Da die Datenträger nur einmal beschrieben werden können, ist eine Wiederverwendung der Datenträger nicht möglich.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### RECLAIMProcess

Gibt die Anzahl paralleler Prozesse für das Wiederherstellen der Datenträger in diesem Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein. Sie können einen oder mehrere Wiederherstellungsprozesse für jeden primären Speicherpool mit sequenziellem Zugriff angeben.

Berücksichtigen Sie bei der Berechnung des Werts für diesen Parameter die folgenden Ressourcen, die für die Wiederherstellungsverarbeitung erforderlich sind:

- Die Anzahl sequenzieller Speicherpools
- Die Anzahl logischer und physischer Laufwerke, die der Operation zugeordnet werden kann

Für den Zugriff auf Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk.

Beispiel: Angenommen, Sie möchten die Datenträger aus zwei Speicherpools mit sequenziellem Zugriff gleichzeitig wiederherstellen und Sie möchten vier Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Wenn der Parameter RECLAIMSTGPOOL nicht angegeben ist oder der Wiederherstellungsspeicherpool dieselbe Einheitenklasse wie der Speicherpool hat, der wiederhergestellt wird, benötigt jeder Prozess zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um acht Wiederherstellungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 16 Mountpunkte und 16 Laufwerke. Die Einheitenklasse für die beiden Speicherpools muss einen Grenzwert für Ladeanforderungen von mindestens 16 haben.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### RECLAIMSTGpool

Gibt einen anderen primären Speicherpool als Ziel für wiederhergestellte Daten aus diesem Speicherpool an. Dieser Parameter ist wahlfrei. Wenn der Server Datenträger für den Speicherpool zurückfordert, werden nicht verfallene Daten von den Datenträgern, die zurückgefordert werden, in den Speicherpool versetzt, der mit diesem Parameter angegeben wird.

Soll ein vorhandener Wert entfernt werden, eine Nullzeichenfolge ("" ) angeben.

Ein Wiederherstellungsspeicherpool ist besonders nützlich für einen Speicherpool, der nur ein Laufwerk in seinem Kassettenarchiv hat. Wird dieser Parameter angegeben, versetzt der Server alle Daten von den zurückgeforderten Datenträgern in den Wiederherstellungsspeicherpool, unabhängig von der Anzahl der Laufwerke in dem Kassettenarchiv.

Um die Daten aus dem Wiederherstellungsspeicherpool wieder in den ursprünglichen Speicherpool zu versetzen, ist die Speicherpoolhierarchie zu verwenden. Den ursprünglichen Speicherpool als nächsten Speicherpool für den Wiederherstellungsspeicherpool angeben.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### COLlocate

Gibt an, ob der Server versucht, Daten, die zu den folgenden Kandidaten gehören, auf möglichst wenig Datenträgern zu speichern:

- Ein einzelner Clientknoten
- Eine Gruppe von Dateibereichen
- Eine Gruppe von Clientknoten
- Ein Clientdateibereich

Dieser Parameter ist wahlfrei.

Die Kollokation reduziert die Anzahl der Ladevorgänge für Datenträger mit sequenziellem Zugriff für Zurückschreibungs-, Abruf- und Rückrufoperationen. Die Kollokation erfordert jedoch mehr Serverzeit, um Dateien zum Speichern zusammenzufassen, sowie eine größere Anzahl Datenträger. Die Kollokation kann sich auch auf die Anzahl Prozesse zum Umlagern von Platten in den sequenziellen Pool auswirken.

Sie können eine der folgenden Optionen angeben:

No

Gibt an, dass die Kollokation inaktiviert ist. Während der Umlagerung von Platte werden Prozesse auf einer Dateibereichsebene erstellt.

GRoup

Gibt an, dass die Kollokation auf Gruppenebene für Clientknoten oder Dateibereiche aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten für Knoten oder Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf so wenig Datenträgern wie möglich zu speichern.

Wenn Sie COLLOCATE=GROUP angeben, aber keine Kollokationsgruppen definieren, oder wenn Sie keine Knoten oder Dateibereiche zu einer Kollokationsgruppe hinzufügen, werden Daten nach Knoten durch Kollokation zusammengefasst. Ziehen Sie die Verwendung von Bändern in Betracht, wenn Sie Clientknoten oder Dateibereiche in Kollokationsgruppen zusammenfassen.

Besteht beispielsweise ein bandbasierter Speicherpool aus Daten von Knoten, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst die Daten für gruppierte Knoten nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Knoten gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten für nicht gruppierte Knoten nach Knoten zusammen. Wenn möglich, speichert der Server die Daten für einen einzelnen Knoten auf einem einzelnen Band. Alle verfügbaren Bänder, die bereits Daten für den Knoten enthalten, werden verwendet, bevor verfügbarer Speicherbereich auf einem anderen Band verwendet wird.
- Während der Umlagerung von Platte erstellt der Server Umlagerungsprozesse auf der Kollokationsgruppenebene für gruppierte Knoten und auf der Knotenebene für nicht gruppierte Knoten.

Besteht ein bandbasierter Speicherpool aus Daten aus gruppierten Dateibereichen, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst nur die Daten für gruppierte Dateibereiche nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Dateibereichen gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Dateibereich können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten nach Knoten zusammen (für Dateibereiche, die nicht explizit für eine Dateibereichskollokationsgruppe definiert sind). Beispiel: Knoten1 hat die Dateibereiche A, B, C, D und E. Die Dateibereiche A und B gehören zu einer Dateibereichskollokationsgruppe, die Dateibereiche C, D und E dagegen nicht. Die Dateibereiche A und B werden nach Dateibereichskollokationsgruppe zusammengefasst, während die Dateibereiche C, D und E nach Knoten zusammengefasst werden.
- Während der Umlagerung von Platte erstellt der Server Umlagerungsprozesse auf der Kollokationsgruppenebene für gruppierte Dateibereiche.

Daten werden auf so wenig Datenträger mit sequenziellm Zugriff wie möglich zusammengefasst.

#### NODE

Gibt an, dass die Kollokation auf Clientknotenebene aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten eines Knotens auf so wenig Datenträgern wie möglich zu speichern. Verfügt der Knoten über mehrere Dateibereiche, versucht der Server nicht, diese Dateibereiche durch Kollokation zusammenzufassen. Für die Kompatibilität mit früheren Versionen wird COLLOCATE=YES noch vom Server akzeptiert, um die Kollokation auf der Clientknotenebene anzugeben.

Enthält ein Speicherpool Daten für einen Knoten, der Teil einer Kollokationsgruppe ist, und geben Sie COLLOCATE=NODE an, werden die Daten nach Knoten durch Kollokation zusammengefasst.

Bei COLLOCATE=NODE erstellt der Server Prozesse auf der Knotenebene, wenn Daten von Platte umgelagert werden.

#### Filespace

Gibt an, dass die Kollokation auf der Dateibereichsebene für Clientknoten aktiviert ist. Der Server versucht, Daten eines Knotens und eines Dateibereichs auf so wenig Datenträgern wie möglich zu speichern. Verfügt ein Knoten über mehrere Dateibereiche, versucht der Server, Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern zu speichern.

Bei COLLOCATE=FILESPACE erstellt der Server Prozesse auf der Dateibereichsebene, wenn Daten von Platte umgelagert werden.

#### MAXSCRatch

Gibt die maximale Anzahl Arbeitsdatenträger an, die der Server anfordern kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 100000000 angeben. Wird dem Server das Anfordern von Arbeitsdatenträgern erlaubt, muss der Benutzer nicht jeden zu verwendenden Datenträger definieren.

Mit dem für diesen Parameter angegebenen Wert wird die Gesamtzahl der im Speicherpool verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Speicherpools geschätzt.

Arbeitsdatenträger werden automatisch aus dem Speicherpool gelöscht, sobald sie leer sind. Wenn Arbeitsdatenträger mit dem Einheitentyp FILE gelöscht werden, wird der von den Datenträgern belegte Speicherbereich von dem Server freigegeben und an das Dateisystem zurückgegeben.

Tipp: Für serverübergreifende Operationen, die virtuelle Datenträger verwenden und ein kleines Datenvolumen speichern, sollte ein Wert für den Parameter MAXSCRATCH angegeben werden, der höher als der Wert ist, der normalerweise für Schreiboperationen für andere Datenträgertypen angegeben wird. Nach einer Schreiboperation auf einem virtuellen Datenträger markiert IBM Spectrum Protect den Datenträger als FULL, auch wenn der Wert des Parameters MAXCAPACITY in der Einheitenklassendefinition noch nicht erreicht wurde. Der Server behält virtuelle Datenträger nicht im Status FILLING und hängt keine Daten an. Ist der Wert des Parameters MAXSCRATCH zu niedrig, können serverübergreifende Operationen fehlschlagen.

#### REUsedelay

Gibt die Anzahl Tage an, die nach dem Löschen aller Dateien von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerpool zurückgestellt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Wert 0 bedeutet, dass ein Datenträger wieder beschrieben bzw. als Arbeitsdatenträger zurückgegeben werden kann, sobald alle Dateien auf dem Datenträger gelöscht wurden.

Durch Angabe dieses Parameters kann sichergestellt werden, dass die Datenbank auf einem früheren Stand wiederhergestellt werden kann und Datenbankverweise auf Dateien im Speicherpool weiterhin gültig wären.

#### OVFLocation

Gibt den Überlaufstandort für den Speicherpool an. Der Server ordnet diesen Standortnamen einem Datenträger zu, der durch den Befehl MOVE MEDIA aus dem Kassettenarchiv ausgegeben wird. Dieser Parameter ist wahlfrei. Der Standortname darf maximal 255 Zeichen lang sein. Den Standortnamen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

Soll ein vorhandener Wert entfernt werden, eine Nullzeichenfolge ("" ) angeben.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### MIGDelay

Gibt die Mindestanzahl Tage an, die eine Datei in einem Speicherpool verbleiben muss, bevor sie für die Umlagerung ausgewählt werden kann. Alle Dateien auf einem Datenträger müssen für die Umlagerung auswählbar sein, bevor der Server den Datenträger für die Umlagerung auswählt. Um einen Wert zu berechnen, der mit dem angegebenen Wert für MIGDELAY verglichen wird, zählt der Server die Anzahl der Tage, die die Datei im Speicherpool war.

Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben.

Soll der Server die Anzahl der Tage nur ab dem Tag zählen, an dem eine Datei gespeichert wurde, und nicht ab dem Tag, an dem sie abgerufen wurde, die Serveroption NORETRIEVEDATE verwenden.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### MIGContinue

Gibt an, ob der Server Dateien umlagern darf, die der Verzögerungszeit für die Umlagerung nicht entsprechen. Dieser Parameter ist wahlfrei.

Da angegeben werden kann, dass Dateien eine Mindestanzahl Tage in dem Speicherpool verbleiben müssen, kann der Server alle auswählbaren Dateien in den nächsten Speicherpool umlagern, obwohl sie dem Wert für die untere Umlagerungsschwelle nicht entsprechen. Mit diesem Parameter kann angegeben werden, ob der Server die Umlagerung fortsetzen darf, indem Dateien umgelagert werden, die der Verzögerungszeit für die Umlagerung nicht entsprechen.

Sie können einen der folgenden Werte angeben:

#### Yes

Muss die untere Umlagerungsschwelle eingehalten werden, gibt dieser Wert an, dass der Server die Umlagerung von Dateien fortsetzt, die noch nicht die Anzahl Tage in dem Speicherpool gespeichert sind, die durch die Umlagerungsverzögerung angegeben ist.

#### No

Gibt an, dass der Server die Umlagerung stoppt, wenn keine auswählbaren Dateien mehr für die Umlagerung verfügbar sind; dies gilt auch vor Erreichen der unteren Umlagerungsschwelle. Der Server lagert nur Dateien um, die die durch die Umlagerungsverzögerung angegebene Anzahl Tage in dem Speicherpool gespeichert sind.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP

- NDMPDUMP

#### MIGProcess

Gibt die Anzahl paralleler Prozesse für das Umlagern der Dateien von den Datenträgern in diesen Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein.

Bei der Berechnung des Werts für diesen Parameter ist die Anzahl der sequenziellen Speicherpools, die von der Umlagerung betroffen sind, und die Anzahl der logischen und physischen Laufwerke zu berücksichtigen, die der Operation zugeordnet werden können. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl der verfügbaren Mountpunkte und Laufwerke ist von anderen IBM Spectrum Protect- und Systemaktivitäten sowie von den Grenzwerten für Ladeanforderungen der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die von der Umlagerung betroffen sind.

Beispiel: Angenommen, Sie möchten gleichzeitig die Dateien von Datenträgern in zwei primären sequenziellen Speicherpools umlagern und Sie möchten drei Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Hat der Speicherpool, in den Dateien umgelagert werden, dieselbe Einheitenklasse wie der Speicherpool, aus dem Dateien umgelagert werden, benötigt jeder Prozess zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um sechs Umlagerungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 12 Mountpunkte und 12 Laufwerke. Die Einheitenklasse für die Speicherpools muss einen Grenzwert für Ladeanforderungen von mindestens 12 haben.

Überschreitet die angegebene Anzahl der Umlagerungsprozesse die Anzahl der verfügbaren Mountpunkte oder Laufwerke, warten die Prozesse, die keine Mountpunkte oder Laufwerke anfordern können, bis Mountpunkte oder Laufwerke verfügbar werden. Werden Mountpunkte oder Laufwerke innerhalb der MOUNTWAIT-Zeit nicht verfügbar, werden die Umlagerungsprozesse beendet. Informationen zur Angabe der MOUNTWAIT-Zeit befinden sich in DEFINE DEVCLASS (Einheitenklasse definieren).

Der IBM Spectrum Protect-Server startet die angegebene Anzahl der Umlagerungsprozesse, unabhängig von der Anzahl der Datenträger, die für die Umlagerung ausgewählt werden können. Geben Sie beispielsweise zehn Umlagerungsprozesse an und können nur sechs Datenträger für die Umlagerung ausgewählt werden, startet der Server zehn Prozesse, von denen vier beendet werden, ohne dass ein Datenträger verarbeitet wird.

Anmerkung: Beachten Sie bei der Angabe dieses Parameters, ob die Funktion für simultanes Schreiben für die Serverdatenumlagerung aktiviert ist. Jeder Umlagerungsprozess erfordert einen Mountpunkt und ein Laufwerk für jeden Kopienspeicherpool und Pool für aktive Daten, der für den Zielspeicherpool definiert ist.

#### AUTOCopy

Gibt an, wann IBM Spectrum Protect Operationen mit simultanem Schreiben ausführt. Dieser Parameter betrifft die folgenden Operationen:

- Clientspeichersitzungen
- Serverimportprozesse
- Serverdatenumlagerungsprozesse

Wenn die Option AUTOCOPY auf ALL oder CLIENT gesetzt wird und mindestens ein Speicherpool vorhanden ist, der in der Option COPYSTGPOLLS oder ACTIVEDATAPOOLS aufgelistet ist, wird die clientseitige Deduplizierung inaktiviert.

Tritt ein Fehler auf, wenn Daten während eines Umlagerungsprozesses gleichzeitig in einen Kopienspeicherpool oder einen Pool für aktive Daten geschrieben werden, stoppt der Server das Schreiben in die fehlerhaften Speicherpools für den Rest des Prozesses. Der Server speichert jedoch weiterhin Dateien in dem primären Speicherpool und in allen verbleibenden Kopienspeicherpools oder Pools für aktive Daten. Diese Pools bleiben für die Dauer des Umlagerungsprozesses aktiv. Kopienspeicherpools werden mit dem Parameter COPYSTGPOLLS angegeben. Pools für aktive Daten werden mit dem Parameter ACTIVEDATAPOOLS angegeben.

Sie können einen der folgenden Werte angeben:

#### None

Gibt an, dass die Funktion für simultanes Schreiben inaktiviert ist.

#### Client

Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen oder Serverimportprozessen gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverimportprozessen werden Daten nur gleichzeitig in Kopienspeicherpools geschrieben. Daten werden während der Ausführung von Serverimportprozessen nicht in Pools für aktive Daten geschrieben.

#### MIGRation

Gibt an, dass Daten nur während der Umlagerung in diesen Speicherpool gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverdatenumlagerungsprozessen werden Daten in Kopienspeicherpools und Pools für aktive Daten nur dann gleichzeitig geschrieben, wenn die Daten in diesen Pools nicht vorhanden sind. Knoten, deren Daten umgelagert werden, müssen sich in einer Domäne befinden, die einem Pool für aktive Daten zugeordnet ist. Befinden sich die Knoten nicht in einer Domäne, die einem Pool für aktive Daten zugeordnet ist, können die Daten nicht in den Pool geschrieben werden.

All

Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen, Serverimportprozessen oder Serverdatenumlagerungsprozessen gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Mit diesem Wert wird sichergestellt, dass Daten immer dann gleichzeitig geschrieben werden, wenn dieser Pool ein Ziel für eine der auswählbaren Operationen ist.

#### COPYSTGpools

Gibt die Namen von Kopienspeicherpools an, in die der Server gleichzeitig Daten schreibt. Sie können maximal drei Kopienpoolnamen angeben, die durch Kommas voneinander getrennt werden müssen. Leerzeichen zwischen den Namen der Kopienpools sind nicht zulässig. Um einen oder mehrere Kopienspeicherpools hinzuzufügen oder zu entfernen, geben Sie den oder die Poolnamen an, der bzw. die in der aktualisierten Liste enthalten sein soll(en). Enthält die vorhandene Kopienpoolliste beispielsweise COPY1 und COPY2 und soll COPY3 hinzugefügt werden, geben Sie COPYSTGPOOLS=COPY1,COPY2,COPY3 an. Um alle vorhandenen Kopienspeicherpools zu entfernen, die dem primären Speicherpool zugeordnet sind, geben Sie eine Nullzeichenfolge ("" ) für den Wert an (beispielsweise COPYSTGPOOLS="").

Wenn Sie einen Wert für den Parameter COPYSTGPOOLS angeben, können Sie auch einen Wert für den Parameter COPYCONTINUE angeben. Weitere Informationen enthält die Beschreibung des Parameters COPYCONTINUE.

Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSGTPOOLS und ACTIVEDATAPOOLS angegeben sind, darf drei nicht überschreiten.

Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Kopienspeicherpools und den Wert für COPYCONTINUE aus dem primären Speicherpool. Der primäre Speicherpool wird durch die Kopiengruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

Der Server kann während der Ausführung der folgenden Operationen Daten gleichzeitig in Kopienspeicherpools schreiben:

- Sicherungs- und Archivierungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder Anwendungsclients, die die IBM Spectrum Protect-API verwenden
- Umlagerungsoperationen durch IBM Spectrum Protect for Space Management-Clients
- Importoperationen, die das Kopieren von exportierten Dateidaten von externen Datenträgern in einen primären Speicherpool einbeziehen, der einer Kopienspeicherpoolliste zugeordnet ist

Einschränkungen:

1. Dieser Parameter ist nur für primäre Speicherpools verfügbar, die das Datenformat NATIVE oder NONBLOCK verwenden. Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP
2. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch akzeptiert.
3. Die Funktion für simultanes Schreiben wird für NAS-Sicherungsoperationen nicht unterstützt. Sind für den primären Speicherpool, der in DESTINATION oder TOCDESTINATION in der Kopiengruppe der Verwaltungsklasse angegeben ist, Kopienspeicherpools definiert, werden die Kopienspeicherpools ignoriert und die Daten werden nur im primären Speicherpool gespeichert.
4. Die Funktion für simultanes Schreiben kann mit CENTERA-Speichereinheiten nicht verwendet werden.

Achtung: Die mit dem Parameter COPYSTGPOOLS zur Verfügung gestellte Funktion soll nicht den Befehl BACKUP STGPOOL ersetzen. Wird der Parameter COPYSTGPOOLS verwendet, verwenden Sie weiterhin den Befehl BACKUP STGPOOL, um sicherzustellen, dass die Kopienspeicherpools vollständige Kopien des primären Speicherpools sind. Es gibt Fälle, in denen eine Kopie möglicherweise nicht erstellt wird. Weitere Informationen enthält die Beschreibung des Parameters COPYCONTINUE.

#### COPYContinue

Gibt an, wie der Server auf einen Fehler beim Schreiben in einen der Kopienspeicherpools reagiert, die im Parameter COPYSTGPOOLS aufgelistet sind. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Wenn Sie den Parameter COPYCONTINUE angeben, muss entweder eine COPYSTGPOOLS-Liste vorhanden sein oder der Parameter COPYSTGPOOLS muss ebenfalls angegeben werden.

Der Parameter COPYCONTINUE hat keine Auswirkung auf die Funktion für simultanes Schreiben während der Umlagerung.

Sie können die folgenden Werte angeben:

Yes

Ist der Parameter COPYCONTINUE auf YES gesetzt, stoppt der Server das Schreiben in die fehlerhaften Kopienpools für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Kopienpools fort. Die Liste der Kopienspeicherpools ist nur für die Dauer der Clientsitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.

No

Ist der Parameter COPYCONTINUE auf NO gesetzt, wird die aktuelle Transaktion vom Server nicht ausgeführt und die Speicheroperation nicht fortgesetzt.

Einschränkungen:

- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf Pools für aktive Daten. Tritt für einen der Pools für aktive Daten ein Schreibfehler auf, stoppt der Server das Schreiben in den fehlerhaften Pool für aktive Daten für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Pools für aktive Daten und Kopierspeicherpools fort. Die Liste der Pools für aktive Daten ist nur für die Dauer der Sitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.
- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Ausführung eines Serverimportprozesses. Werden Daten gleichzeitig geschrieben und tritt für den primären Speicherpool oder einen Kopierspeicherpool ein Schreibfehler auf, schlägt der Serverimportprozess fehl.
- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Serverdatenumlagerung. Werden Daten gleichzeitig geschrieben und tritt für einen Kopierspeicherpool oder Pool für aktive Daten ein Schreibfehler auf, wird der fehlerhafte Speicherpool entfernt und der Datenumlagerungsprozess wird fortgesetzt. Bei Schreibfehlern für den primären Speicherpool schlägt der Umlagerungsprozess fehl.

#### ACTIVEDATApools

Gibt die Namen der Pools für aktive Daten an, in die der Server während einer Clientsicherungsoperation gleichzeitig Daten schreibt. Der Parameter ACTIVEATAPOOLS ist optional. Leerzeichen zwischen den Namen der Pools für aktive Daten sind nicht zulässig.

Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSGTPOOLS und ACTIVEATAPOOLS angegeben sind, darf drei nicht überschreiten.

Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Pools für aktive Daten aus dem Zielspeicherpool, der in der Kopiengruppe angegeben ist. Der primäre Speicherpool wird durch die Kopiengruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

Der Server kann nur während Sicherungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder durch Anwendungsclients, die die IBM Spectrum Protect-API verwenden, Daten gleichzeitig in Pools für aktive Daten schreiben.  
Einschränkungen:

1. Dieser Parameter ist nur für primäre Speicherpools verfügbar, die das Datenformat NATIVE oder NONBLOCK verwenden. Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP
2. Das simultane Schreiben in Pools für aktive Daten wird nicht unterstützt, wenn die Operation die LAN-unabhängige Datenversetzung verwendet. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch akzeptiert.
3. Die Funktion für simultanes Schreiben wird nicht unterstützt, wenn eine NAS-Sicherungsoperation eine Inhaltsverzeichnisdatei schreibt. Sind für den primären Speicherpool, der in TOCDESTINATION in der Kopiengruppe der Verwaltungsklasse angegeben ist, Pools für aktive Daten definiert, werden die Pools für aktive Daten ignoriert und die Daten werden nur im primären Speicherpool gespeichert.
4. Die Funktion für simultanes Schreiben kann mit CENTERA-Speichereinheiten nicht verwendet werden.
5. Daten, die importiert werden, können nicht in Pools für aktive Daten gespeichert werden. Verwenden Sie nach einer Importoperation den Befehl COPY ACTIVEATA, um die importierten Daten in einem Pool für aktive Daten zu speichern.

Achtung: Die mit dem Parameter ACTIVEATAPOOLS zur Verfügung gestellte Funktion soll nicht den Befehl COPY ACTIVEATA ersetzen. Wird der Parameter ACTIVEATAPOOLS verwendet, verwenden Sie den Befehl COPY ACTIVEATA, um sicherzustellen, dass die Pools für aktive Daten alle aktiven Daten des primären Speicherpools enthalten.

#### DEDuplicate

Gibt an, ob die in diesem Speicherpool gespeicherten Daten dedupliziert werden. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.

#### IDENTIFYProcess

Gibt die Anzahl paralleler Prozesse an, die für die serverseitige Datendeduplizierung verwendet werden sollen. Dieser Parameter ist wahlfrei und nur für Speicherpools mit einer Einheitenklasse gültig, der der Einheitentyp FILE zugeordnet ist. Geben Sie einen Wert von 1 bis 50 ein.

Hinweis: Datendeduplizierungsprozesse können entweder aktiv oder inaktiv sein. Prozesse, die gegenwärtig Dateien bearbeiten, sind aktiv. Prozesse, die auf Dateien warten, die bearbeitet werden sollen, sind inaktiv. Prozesse bleiben inaktiv, bis Datenträger mit Daten, die dedupliziert werden sollen, verfügbar werden. Die Ausgabe des Befehls QUERY PROCESS für einen Datendeduplizierungsprozess umfasst die Gesamtzahl Byte und Dateien, die seit dem ersten Start des Prozesses verarbeitet wurden. Wenn beispielsweise ein Datendeduplizierungsprozess vier Dateien verarbeitet, dann inaktiv wird und anschließend fünf weitere Dateien verarbeitet, beträgt die Gesamtzahl der verarbeiteten Dateien neun. Prozesse werden nur beendet, wenn sie

abgebrochen werden oder wenn die Anzahl Datenduplizierungsprozesse für den Speicherpool in einen Wert geändert wird, der kleiner als die gegenwärtig angegebene Anzahl ist.

## Beispiel: Die mountfähigen Arbeitsdatenträger des primären Speicherpools mit sequenziellem Zugriff aktualisieren

Den primären Speicherpool mit sequenziellem Zugriff mit dem Namen TAPEPOOL1 aktualisieren, um das Laden von maximal 10 Arbeitsdatenträgern zu erlauben.

```
update stgpool tapepool1 maxscratch=10
```

## UPDATE STGPOOL (Kopienspeicherpool mit sequenziellem Zugriff aktualisieren)

Mit diesem Befehl kann ein Kopienspeicherpool mit sequenziellem Zugriff aktualisiert werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool, der aktualisiert werden soll, erforderlich.

### Syntax

```
>>-UPDate STGpool--Poolname--+-----+-----+-----+----->
                                     '-DESCRiption---Beschreibung-'
>--+-----+-----+-----+----->
   '-ACCess-----+READWrite---+'
                                     +-READOnly-----+
                                     '-UNAVailable-'
>--+-----+-----+-----+----->
   '-COLlocate-----+No-----+'   '-RECLaim-----Prozent-'
                                     +-GRoup-----+
                                     +-NODE-----+
                                     '-Filespace-'
>--+-----+-----+-----+----->
   '-RECLAIMProcess-----Anzahl-'
>--+-----+-----+-----+----->
   '-OFFSITERECLAIMLimit-----+NOLimit--+'
                                     '-Anzahl--'
>--+-----+-----+-----+----->
   '-MAXSCRatch-----Anzahl-'   '-REUsedelay-----Tage-'
>--+-----+-----+-----+----->
   '-OVFLORation-----Standort-'   '-CRCDData-----+Yes--+'
                                     '-No--'
>--+-----+-----+-----+----->
   '-DEDUPlicate-----+No-----+'
                                     |         (1) |
                                     '-Yes-----'
>--+-----+-----+-----+-----><
   |         (2) |
   '-IDENTIFYProcess-----Anzahl-----'
```

Anmerkungen:

1. Dieser Parameter ist nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.
2. Dieser Parameter ist nur verfügbar, wenn der Parameter DEDUPLICATE den Wert YES hat.

### Parameter

Poolname (Erforderlich)



Gibt den Namen des Kopierspeicherpools an, der aktualisiert werden soll.

#### DESCription

Gibt eine Beschreibung des Kopierspeicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge ("" ) angeben.

#### ACCess

Gibt an, wie Clientknoten und Serverprozesse (wie Wiederherstellung) auf Dateien im Kopierspeicherpool zugreifen können. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

##### READWrite

Gibt an, dass Dateien auf die Datenträger im Kopierspeicherpool geschrieben und daraus gelesen werden können.

##### READOnly

Gibt an, dass Clientknoten Dateien, die auf den Datenträgern im Kopierspeicherpool gespeichert sind, nur lesen können.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Kopierspeicherpool verwenden, um Dateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Kopierspeicherpool sind jedoch keine neuen Schreiboperationen durch Datenträger außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht im Kopierspeicherpool gesichert werden.

##### UNAVailable

Gibt an, dass Clientknoten nicht auf Dateien zugreifen können, die auf Datenträgern im Kopierspeicherpool gespeichert sind.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Kopierspeicherpool verwenden, um Dateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Kopierspeicherpool sind jedoch keine neuen Schreiboperationen durch Datenträger außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht im Kopierspeicherpool gesichert werden.

#### COLlocate

Gibt an, ob der Server versucht, Daten, die zu den folgenden Kandidaten gehören, auf möglichst wenig Datenträgern zu speichern:

- Ein einzelner Clientknoten
- Eine Gruppe von Dateibereichen
- Eine Gruppe von Clientknoten
- Ein Clientdateibereich

Dieser Parameter ist wahlfrei.

Die Kollokation reduziert die Anzahl der Ladevorgänge für Datenträger mit sequenziellem Zugriff für Zurückschreibungs-, Abruf- und Rückrufoperationen. Die Kollokation erfordert jedoch mehr Serverzeit, um Dateien zum Speichern zusammenzufassen, sowie eine größere Anzahl Datenträger.

Sie können eine der folgenden Optionen angeben:

##### No

Gibt an, dass die Kollokation inaktiviert ist.

##### GRoup

Gibt an, dass die Kollokation auf Gruppenebene für Clientknoten oder Dateibereiche aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten für Knoten oder Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf so wenig Datenträgern wie möglich zu speichern.

Wenn Sie COLLOCATE=GROUP angeben, aber keine Kollokationsgruppen definieren, oder wenn Sie keine Knoten oder Dateibereiche zu einer Kollokationsgruppe hinzufügen, werden Daten nach Knoten durch Kollokation zusammengefasst. Ziehen Sie die Verwendung von Bändern in Betracht, wenn Sie Clientknoten oder Dateibereiche in Kollokationsgruppen zusammenfassen.

Besteht beispielsweise ein bandbasierter Speicherpool aus Daten von Knoten, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst die Daten für gruppierte Knoten nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Knoten gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten für nicht gruppierte Knoten nach Knoten zusammen. Wenn möglich, speichert der Server die Daten für einen einzelnen Knoten auf einem einzelnen Band. Alle verfügbaren Bänder, die bereits Daten für den Knoten enthalten, werden verwendet, bevor verfügbarer Speicherbereich auf einem anderen Band verwendet wird.

Besteht ein bandbasierter Speicherpool aus Daten aus gruppierten Dateibereichen, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst nur die Daten für gruppierte Dateibereiche nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Dateibereichen gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Dateibereich können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten nach Knoten zusammen (für Dateibereiche, die nicht explizit für eine Dateibereichskollokationsgruppe definiert sind). Beispiel: Knoten1 hat die Dateibereiche A, B, C, D und E. Die Dateibereiche A und B gehören zu einer Dateibereichskollokationsgruppe, die Dateibereiche C, D und E dagegen nicht. Die Dateibereiche A und B werden nach Dateibereichskollokationsgruppe zusammengefasst, während die Dateibereiche C, D und E nach Knoten zusammengefasst werden.

Daten werden auf so wenig Datenträger mit sequenziellem Zugriff wie möglich zusammengefasst.

#### NODE

Gibt an, dass die Kollokation auf Clientknotenebene aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten eines Knotens auf so wenig Datenträgern wie möglich zu speichern. Verfügt der Knoten über mehrere Dateibereiche, versucht der Server nicht, diese Dateibereiche durch Kollokation zusammenzufassen. Für die Kompatibilität mit früheren Versionen wird COLLOCATE=YES noch vom Server akzeptiert, um die Kollokation auf der Clientknotenebene anzugeben.

Enthält ein Speicherpool Daten für einen Knoten, der Teil einer Kollokationsgruppe ist, und geben Sie COLLOCATE=NODE an, werden die Daten nach Knoten durch Kollokation zusammengefasst.

#### Filespace

Gibt an, dass die Kollokation auf der Dateibereichsebene für Clientknoten aktiviert ist. Der Server versucht, Daten eines Knotens und eines Dateibereichs auf so wenig Datenträgern wie möglich zu speichern. Verfügt ein Knoten über mehrere Dateibereiche, versucht der Server, Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern zu speichern.

#### REclaim

Gibt an, wann der Server einen Datenträger auf der Basis des Prozentsatzes wiederherstellbaren Speicherbereichs auf einem Datenträger zurückfordert. Der wiederherstellbare Speicherbereich ist der Speicherbereich, der durch Dateien belegt ist, die verfallen sind oder aus der IBM Spectrum Protect-Datenbank gelöscht wurden.

Bei der Wiederherstellung wird der zerstückelte Speicherbereich auf Datenträgern durch Versetzen der restlichen aktiven Dateien von einem Datenträger auf einen anderen wieder verwendbar, wodurch der ursprüngliche Datenträger wiederverwendet werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 100 angeben. Der Wert 100 bedeutet, dass Datenträger nicht zurückgefordert werden.

Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

Wird der Standardwert 100 geändert, einen Wert von 50 Prozent oder höher angeben, so dass Dateien, die auf zwei Datenträgern gespeichert sind, auf einem einzigen Ausgabedatenträger gespeichert werden können.

Wenn ein ausgelagerter Kopierspeicherpool datenträger für die Wiederherstellung ausgewählt werden kann, versucht der Wiederherstellungsprozess, die aktiven Dateien auf einem zurückforderbaren Datenträger aus einem primären Speicherpool oder einem Kopierspeicherpool vor Ort abzurufen. Der Prozess schreibt dann diese Dateien auf einen verfügbaren Datenträger in dem ursprünglichen Kopierspeicherpool. Tatsächlich werden diese Dateien wieder an den Standort vor Ort versetzt. Die Dateien können jedoch nach einem Katastrophenfall auch vom ausgelagerten Datenträger abgerufen werden, wenn eine Datenbanksicherung verwendet wird, die auf die Dateien auf dem ausgelagerten Datenträger verweist. Wegen der Art, mit der ausgelagerte Datenträger bei der Wiederherstellung bearbeitet werden, sollte die Wiederherstellung bei Kopierspeicherpools mit Vorsicht verwendet werden.

#### RECLAIMProcess

Gibt die Anzahl paralleler Prozesse für das Wiederherstellen der Datenträger in diesem Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein.

Berücksichtigen Sie bei der Berechnung des Werts für diesen Parameter die folgenden Ressourcen, die für die Wiederherstellungsverarbeitung erforderlich sind:

- Die Anzahl sequenzieller Speicherpools
- Die Anzahl logischer und physischer Laufwerke, die der Operation zugeordnet werden kann

Für den Zugriff auf Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk.

Beispiel: Angenommen, Sie möchten die Datenträger aus zwei Speicherpools mit sequenziellem Zugriff gleichzeitig wiederherstellen und Sie möchten vier Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Jeder Prozess benötigt zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um acht

Wiederherstellungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 16 Mountpunkte und 16 Laufwerke. Die Einheitenklasse für jeden Speicherpool muss einen Grenzwert für Ladeanforderungen von mindestens 8 haben.

Sie können einen oder mehrere Wiederherstellungsprozesse für jeden Kopierspeicherpool angeben. Sie können mehrere gleichzeitig ablaufende Wiederherstellungsprozesse für einen einzelnen Kopierspeicherpool angeben. Damit wird eine bessere Nutzung Ihrer verfügbaren Bandlaufwerke oder FILE-Datenträger erreicht. Wenn die gleichzeitig ablaufende Verarbeitung mehrerer Prozesse nicht erforderlich ist, geben Sie den Wert 1 für den Parameter RECLAIMPROCESS an.

#### OFFSITERECLAIMLimit

Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich während der Wiederherstellung für diesen Speicherpool zurückgefordert wird. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

##### NOLimit

Gibt an, dass der Speicherbereich auf allen ausgelagerten Datenträgern wiederhergestellt werden soll.

##### Anzahl

Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich wiederhergestellt werden soll. Sie können eine ganze Zahl von 0 bis 99999 angeben. Der Wert 0 bedeutet, dass für keine ausgelagerten Datenträger der Speicherbereich wiederhergestellt wird.

Tipp:

Um den Wert für OFFSITERECLAIMLIMIT zu bestimmen, verwenden Sie die statistischen Informationen in der Nachricht, die am Ende der Wiederherstellungsoperation für den ausgelagerten Datenträger ausgegeben wird. Die statistischen Informationen umfassen die folgenden Elemente:

- Die Anzahl der ausgelagerten Datenträger, die verarbeitet wurden
- Die Anzahl der parallelen Prozesse, die verwendet wurden
- Die Gesamtzeit, die für die Verarbeitung benötigt wurde

Die Reihenfolge, in der ausgelagerte Datenträger wiederhergestellt werden, basiert auf dem Umfang des freien Speicherplatzes auf einem Datenträger. (Freier Speicherplatz umfasst den Speicherbereich, der auf dem Datenträger nie verwendet wurde, und den Speicherbereich, der aufgrund des Löschs von Dateien frei geworden ist.) Datenträger mit dem größten freien Speicherplatz werden zuerst wiederhergestellt.

Beispiel: Angenommen, ein Kopierspeicherpool enthält drei Datenträger: VOL1, VOL2 und VOL3. VOL1 hat den größten freien Speicherplatz, und VOL3 hat den kleinsten freien Speicherplatz. Weiter wird angenommen, dass der Prozentsatz des freien Speicherplatzes auf jedem der drei Datenträger größer als der Wert des Parameters RECLAIM ist. Wird kein Wert für den Parameter OFFSITERECLAIMLIMIT angegeben, werden alle drei Datenträger wiederhergestellt, wenn die Wiederherstellung ausgeführt wird. Wird der Wert 2 angegeben, werden nur VOL1 und VOL2 bei der Wiederherstellung wiederhergestellt. Wird der Wert 1 angegeben, wird nur VOL1 wiederhergestellt.

#### MAXSCRatch

Gibt die maximale Anzahl der Arbeitsdatenträger an, die der Server für diesen Speicherpool anfordern kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 100000000 angeben. Wird dem Server das Anfordern von Arbeitsdatenträgern nach Bedarf erlaubt, muss der Benutzer nicht jeden zu verwendenden Datenträger definieren.

Mit dem für diesen Parameter angegebenen Wert wird die Gesamtzahl der im Kopierspeicherpool verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Kopierspeicherpools geschätzt.

Arbeitsdatenträger werden automatisch aus dem Speicherpool gelöscht, sobald sie leer sind. Lautet jedoch der Zugriffsmodus für einen Arbeitsdatenträger OFFSITE, wird der Datenträger erst dann aus dem Kopierspeicherpool gelöscht, wenn der Zugriffsmodus geändert wird. Ein Administrator kann den Server nach leeren ausgelagerten Arbeitsdatenträgern abfragen und diese an den Standort vor Ort zurückgeben.

Wenn Arbeitsdatenträger mit dem Einheitentyp FILE leer werden und gelöscht werden, wird der von den Datenträgern belegte Speicherbereich von dem Server freigegeben und an das Dateisystem zurückgegeben.

Tipp: Für serverübergreifende Operationen, die virtuelle Datenträger verwenden und ein kleines Datenvolumen speichern, sollte ein Wert für den Parameter MAXSCRATCH angegeben werden, der höher als der Wert ist, der normalerweise für Schreiboperationen für andere Datenträgertypen angegeben wird. Nach einer Schreiboperation auf einem virtuellen Datenträger markiert IBM Spectrum Protect den Datenträger als FULL, auch wenn der Wert des Parameters MAXCAPACITY in der Einheitenklassendefinition noch nicht erreicht wurde. Der IBM Spectrum Protect-Server behält virtuelle Datenträger nicht im Status FILLING und hängt keine Daten an. Ist der Wert des Parameters MAXSCRATCH zu niedrig, können serverübergreifende Operationen fehlschlagen.

#### REUsedelay

Gibt die Anzahl Tage an, die nach dem Löschen aller Dateien von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerpool zurückgestellt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Wert 0 bedeutet, dass ein Datenträger wieder beschrieben bzw. als Arbeitsdatenträger zurückgegeben werden kann, sobald alle Dateien auf dem Datenträger gelöscht wurden.

Tipp: Mit diesem Parameter kann sichergestellt werden, dass Datenbankverweise auf Dateien im Kopierspeicherpool noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird. Dieser Parameter muss auf einen Wert gesetzt werden, der größer als die Anzahl der Tage ist, die die älteste Datenbanksicherung aufbewahrt werden soll. Die für diesen Parameter angegebene Anzahl Tage muss der im Befehl SET DRMDBBACKUPEXPIREDDAYS angegebenen Anzahl entsprechen.

#### OVFLocation

Gibt den Überlaufstandort für den Speicherpool an. Der Server ordnet diesen Standortnamen einem Datenträger zu, der durch den Befehl MOVE MEDIA aus dem Kassettenarchiv ausgegeben wird. Dieser Parameter ist wahlfrei. Der Standortname darf maximal 255 Zeichen lang sein. Den Standortnamen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

Soll ein vorhandener Wert entfernt werden, eine Nullzeichenfolge ("" ) angeben.

#### CRCData

Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist nur für Speicherpools mit dem Datenformat NATIVE gültig. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCDATA auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

##### Yes

Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da eine zusätzliche Verarbeitung erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

##### No

Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

#### Tipp:

Für Speicherpools, die dem Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet sind, bietet der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust als die CRC-Überprüfung für einen Speicherpool. Wenn Sie die CRC-Überprüfung für einen Speicherpool angeben, werden Daten nur während der Ausführung von Datenträgerprüfungsoperationen überprüft. Fehler werden identifiziert, nachdem Daten auf Band geschrieben wurden.

Um den Schutz logischer Blöcke zu aktivieren, geben Sie den Wert READWRITE für den Parameter LBPROTECT in den Befehlen DEFINE DEVCLASS und UPDATE DEVCLASS für den Einheitentyp 3592, LTO oder ECARTRIDGE an. Der Schutz logischer Blöcke wird nur für die folgenden Typen von Laufwerken und Datenträgern unterstützt:

- IBM® LTO5 und höher
- IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
- Oracle StorageTek T10000C- und T10000D-Laufwerke

#### DEDuplicate

Gibt an, ob die in diesem Speicherpool gespeicherten Daten dedupliziert werden. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.

#### IDENTIFYProcess

Gibt die Anzahl paralleler Prozesse an, die für die serverseitige Datendeduplizierung verwendet werden sollen. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Geben Sie einen Wert von 1 bis 50 ein.

Hinweis: Datendeduplizierungsprozesse können entweder aktiv oder inaktiv sein. Prozesse, die gegenwärtig Dateien bearbeiten, sind aktiv. Prozesse, die auf Dateien warten, die bearbeitet werden sollen, sind inaktiv. Prozesse bleiben inaktiv, bis Datenträger mit Daten, die dedupliziert werden sollen, verfügbar werden. Die Ausgabe des Befehls QUERY PROCESS für einen Datendeduplizierungsprozess umfasst die Gesamtzahl Byte und Dateien, die seit dem ersten Start des Prozesses verarbeitet wurden. Wenn beispielsweise ein Datendeduplizierungsprozess vier Dateien verarbeitet, dann inaktiv wird und anschließend fünf weitere Dateien verarbeitet, beträgt die Gesamtzahl der verarbeiteten Dateien neun. Prozesse werden nur beendet, wenn sie abgebrochen werden oder wenn die Anzahl Datendeduplizierungsprozesse für den Speicherpool in einen Wert geändert wird, der kleiner als die gegenwärtig angegebene Anzahl ist.

## Beispiel: Einen Kopierspeicherpool aktualisieren, um die Verzögerungszeit für die Datenträgerwiederverwendung in 30 Tage zu ändern und Dateien nach Clientknoten zusammenzufassen

Den Kopierspeicherpool TAPEPOOL2 aktualisieren, um die Verzögerungszeit für die Datenträgerwiederverwendung in 30 Tage zu ändern und Dateien nach Clientknoten zusammenzufassen.

```
update stgpool tapepool2 reusedelay=30 collocate=node
```

#### Zugehörige Verweise:

SET DRMDBBACKUPEXPIREDDAYS (Verfall für DB-Sicherungsreihe angeben)

# UPDATE STGPOOL (Pool für aktive Daten mit sequenziellem Zugriff aktualisieren)

Mit diesem Befehl kann ein Pool für aktive Daten aktualisiert werden.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool, der aktualisiert werden soll, erforderlich.

## Syntax

```
>>-UPDate STGpool--Poolname--+-----+----->
                                '-DESCRiption---Beschreibung-'
>--+-----+----->
  '-ACCess---+READWrite---+'
    +-READOnly----+
    '-UNAVailable-'
>--+-----+-----+----->
  '-COLlocate---+No-----+' '-RECLaim---Prozent-'
    +-GRoup-----+
    +-NODE-----+
    '-Filespace-'
>--+-----+----->
  '-RECLAIMPRocess---Anzahl-'
>--+-----+----->
  '-OFFSITERECLAIMLimit---+NOLimit+-'
    '-Anzahl--'
>--+-----+-----+----->
  '-MAXSCRatch---Anzahl-' '-REUsedelay---Tage-'
>--+-----+-----+----->
  '-OVFLORation---Standort-' '-CRCDData---+Yes+-'
    '-No--'
>--+-----+-----+----->
  '-DEDUPlicate---+No-----+
    | (1) |
    '-Yes-----'
>--+-----+-----+-----><
  | (2) |
  '-IDENTIFYPRocess---Anzahl-----'
```

Anmerkungen:

1. Dieser Parameter ist nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.
2. Dieser Parameter ist nur verfügbar, wenn der Parameter DEDUPLICATE den Wert YES hat.

## Parameter

Poolname (Erforderlich)

Gibt den Namen des Pools für aktive Daten an, der aktualisiert werden soll.

DESCRiption

Gibt eine Beschreibung des Pools für aktive Daten an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge (") angeben.

ACCess

Gibt an, wie Clientknoten und Serverprozesse (wie Wiederherstellung) auf Dateien im Pool für aktive Daten zugreifen können. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

READWrite

Gibt an, dass Dateien auf die Datenträger im Pool für aktive Daten geschrieben und daraus gelesen werden können.

#### READOnly

Gibt an, dass Clientknoten Dateien, die auf den Datenträgern im Pool für aktive Daten gespeichert sind, nur lesen können.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Pool für aktive Daten verwenden, um aktive Versionen von Sicherungsdateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Pool für aktive Daten sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht in den Pool für aktive Daten kopiert werden.

#### UNAVailable

Gibt an, dass Clientknoten nicht auf Dateien zugreifen können, die auf Datenträgern im Pool für aktive Daten gespeichert sind.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Pool für aktive Daten verwenden, um aktive Versionen von Sicherungsdateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Pool für aktive Daten sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht in den Pool für aktive Daten kopiert werden.

#### COLlocate

Gibt an, ob der Server versucht, Daten, die zu den folgenden Kandidaten gehören, auf möglichst wenig Datenträgern zu speichern:

- Ein einzelner Clientknoten
- Eine Gruppe von Dateibereichen
- Eine Gruppe von Clientknoten
- Ein Clientdateibereich

Dieser Parameter ist wahlfrei.

Die Kollokation reduziert die Anzahl der Ladevorgänge für Datenträger mit sequenziellem Zugriff für Zurückschreibungs-, Abruf- und Rückrufoperationen. Die Kollokation erfordert jedoch mehr Serverzeit, um Dateien zum Speichern zusammenzufassen, sowie eine größere Anzahl Datenträger.

Sie können eine der folgenden Optionen angeben:

#### No

Gibt an, dass die Kollokation inaktiviert ist.

#### GRoup

Gibt an, dass die Kollokation auf Gruppenebene für Clientknoten oder Dateibereiche aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten für Knoten oder Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf so wenig Datenträgern wie möglich zu speichern.

Wenn Sie COLLOCATE=GROUP angeben, aber keine Kollokationsgruppen definieren, oder wenn Sie keine Knoten oder Dateibereiche zu einer Kollokationsgruppe hinzufügen, werden Daten nach Knoten durch Kollokation zusammengefasst. Ziehen Sie die Verwendung von Bändern in Betracht, wenn Sie Clientknoten oder Dateibereiche in Kollokationsgruppen zusammenfassen.

Besteht beispielsweise ein bandbasierter Speicherpool aus Daten von Knoten, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst die Daten für gruppierte Knoten nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Knoten gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten für nicht gruppierte Knoten nach Knoten zusammen. Wenn möglich, speichert der Server die Daten für einen einzelnen Knoten auf einem einzelnen Band. Alle verfügbaren Bänder, die bereits Daten für den Knoten enthalten, werden verwendet, bevor verfügbarer Speicherbereich auf einem anderen Band verwendet wird.

Besteht ein bandbasierter Speicherpool aus Daten aus gruppierten Dateibereichen, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst nur die Daten für gruppierte Dateibereiche nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Dateibereichen gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Dateibereich können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten nach Knoten zusammen (für Dateibereiche, die nicht explizit für eine Dateibereichskollokationsgruppe definiert sind). Beispiel: Knoten1 hat die Dateibereiche A, B, C, D und E. Die Dateibereiche A und B gehören zu einer Dateibereichskollokationsgruppe, die Dateibereiche C, D und E dagegen nicht. Die Dateibereiche A und B werden nach Dateibereichskollokationsgruppe zusammengefasst, während die Dateibereiche C, D und E nach Knoten zusammengefasst werden.

Daten werden auf so wenig Datenträger mit sequenziellem Zugriff wie möglich zusammengefasst.

## NODE

Gibt an, dass die Kollokation auf Clientknotenebene aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten eines Knotens auf so wenig Datenträgern wie möglich zu speichern. Verfügt der Knoten über mehrere Dateibereiche, versucht der Server nicht, diese Dateibereiche durch Kollokation zusammenzufassen. Für die Kompatibilität mit früheren Versionen wird COLLOCATE=YES noch vom Server akzeptiert, um die Kollokation auf der Clientknotenebene anzugeben.

Enthält ein Speicherpool Daten für einen Knoten, der Teil einer Kollokationsgruppe ist, und geben Sie COLLOCATE=NODE an, werden die Daten nach Knoten durch Kollokation zusammengefasst.

## FILESpace

Gibt an, dass die Kollokation auf der Dateibereichsebene für Clientknoten aktiviert ist. Der Server versucht, Daten eines Knotens und eines Dateibereichs auf so wenig Datenträgern wie möglich zu speichern. Verfügt ein Knoten über mehrere Dateibereiche, versucht der Server, Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern zu speichern.

## RECLAIM

Gibt an, wann der Server einen Datenträger auf der Basis des Prozentsatzes wiederherstellbaren Speicherbereichs auf einem Datenträger zurückfordert. Der wiederherstellbare Speicherbereich ist der Speicherbereich, der durch Dateien belegt ist, die verfallen sind oder aus der IBM Spectrum Protect-Datenbank gelöscht wurden.

Bei der Wiederherstellung werden der fragmentierte Speicherbereich und der durch inaktive Sicherungsdateien belegte Speicherbereich auf Datenträgern durch Versetzen der restlichen nicht verfallenen Dateien und der aktiven Sicherungsdateien von einem Datenträger auf einen anderen Datenträger wieder verwendbar. Mit dieser Aktion kann der ursprüngliche Datenträger wiederverwendet werden. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 100 angeben. Der Wert 100 bedeutet, dass Datenträger nicht zurückgefordert werden.

Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

Wird der Standardwert 60 geändert, einen Wert von 50 Prozent oder höher angeben, so dass Dateien, die auf zwei Datenträgern gespeichert sind, auf einem einzigen Ausgabedatenträger gespeichert werden können.

Wenn ein ausgelagerter Datenträger des Pools für aktive Daten für die Wiederherstellung ausgewählt werden kann, versucht der Wiederherstellungsprozess, die aktiven Dateien auf einem zurückforderbaren Datenträger aus einem primären Speicherpool oder einem Pool für aktive Daten vor Ort abzurufen. Der Prozess schreibt dann diese Dateien auf einen verfügbaren Datenträger in dem ursprünglichen Pool für aktive Daten. Tatsächlich werden diese Dateien wieder an den Standort vor Ort versetzt. Die Dateien können jedoch nach einem Katastrophenfall auch vom ausgelagerten Datenträger abgerufen werden, wenn eine Datenbanksicherung verwendet wird, die auf die Dateien auf dem ausgelagerten Datenträger verweist. Wegen der Art, mit der ausgelagerte Datenträger bei der Wiederherstellung bearbeitet werden, sollte die Wiederherstellung bei Pools mit aktiven Daten mit Vorsicht verwendet werden.

## RECLAIMPROCESS

Gibt die Anzahl paralleler Prozesse für das Wiederherstellen der Datenträger in diesem Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein.

Berücksichtigen Sie bei der Berechnung des Werts für diesen Parameter die folgenden Ressourcen, die für die Wiederherstellungsverarbeitung erforderlich sind:

- Die Anzahl sequenzieller Speicherpools
- Die Anzahl logischer und physischer Laufwerke, die der Operation zugeordnet werden kann

Für den Zugriff auf Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk.

Beispiel: Angenommen, Sie möchten die Datenträger aus zwei Speicherpools mit sequenziellem Zugriff gleichzeitig wiederherstellen und Sie möchten vier Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Jeder Prozess benötigt zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um acht Wiederherstellungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 16 Mountpunkte und 16 Laufwerke. Die Einheitenklasse für jeden Speicherpool muss einen Grenzwert für Ladeanforderungen von mindestens 8 haben.

Sie können einen oder mehrere Wiederherstellungsprozesse für jeden Pool für aktive Daten angeben. Sie können mehrere gleichzeitig ablaufende Wiederherstellungsprozesse für einen einzelnen Pool für aktive Daten angeben. Damit wird eine bessere Nutzung Ihrer verfügbaren Bandlaufwerke oder FILE-Datenträger erreicht. Wenn die gleichzeitig ablaufende Verarbeitung mehrerer Prozesse nicht erforderlich ist, geben Sie den Wert 1 für den Parameter RECLAIMPROCESS an.

## OFFSITERECLAIMLimit

Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich während der Wiederherstellung für diesen Speicherpool zurückgefordert wird. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

#### NOLimit

Gibt an, dass der Speicherbereich auf allen ausgelagerten Datenträgern wiederhergestellt werden soll.

#### Anzahl

Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich wiederhergestellt werden soll. Sie können eine ganze Zahl von 0 bis 99999 angeben. Der Wert 0 bedeutet, dass für keine ausgelagerten Datenträger der Speicherbereich wiederhergestellt wird.

Tipp:

Um den Wert für OFFSITERECLAIMLIMIT zu bestimmen, verwenden Sie die statistischen Informationen in der Nachricht, die am Ende der Wiederherstellungsoperation für den ausgelagerten Datenträger ausgegeben wird. Die statistischen Informationen umfassen die folgenden Elemente:

- Die Anzahl der ausgelagerten Datenträger, die verarbeitet wurden
- Die Anzahl der parallelen Prozesse, die verwendet wurden
- Die Gesamtzeit, die für die Verarbeitung benötigt wurde

Die Reihenfolge, in der ausgelagerte Datenträger wiederhergestellt werden, basiert auf dem Umfang des freien Speicherplatzes auf einem Datenträger. (Freier Speicherplatz umfasst den Speicherbereich, der auf dem Datenträger nie verwendet wurde, und den Speicherbereich, der aufgrund des Löschs von Dateien frei geworden ist.) Datenträger mit dem größten freien Speicherplatz werden zuerst wiederhergestellt.

Beispiel: Angenommen, ein Pool für aktive Daten enthält drei Datenträger: VOL1, VOL2 und VOL3. VOL1 hat den größten freien Speicherplatz, und VOL3 hat den kleinsten freien Speicherplatz. Weiter wird angenommen, dass der Prozentsatz des freien Speicherplatzes auf jedem der drei Datenträger größer als der Wert des Parameters RECLAIM ist. Wird kein Wert für den Parameter OFFSITERECLAIMLIMIT angegeben, werden alle drei Datenträger wiederhergestellt, wenn die Wiederherstellung ausgeführt wird. Wird der Wert 2 angegeben, werden nur VOL1 und VOL2 bei der Wiederherstellung wiederhergestellt. Wird der Wert 1 angegeben, wird nur VOL1 wiederhergestellt.

#### MAXSCRatch

Gibt die maximale Anzahl der Arbeitsdatenträger an, die der Server für diesen Speicherpool anfordern kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 100000000 angeben. Wird dem Server das Anfordern von Arbeitsdatenträgern nach Bedarf erlaubt, muss der Benutzer nicht jeden zu verwendenden Datenträger definieren.

Mit dem für diesen Parameter angegebenen Wert wird die Gesamtzahl der im Pool für aktive Daten verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Pools für aktive Daten geschätzt.

Arbeitsdatenträger werden automatisch aus dem Speicherpool gelöscht, sobald sie leer sind. Lautet jedoch der Zugriffsmodus für einen Arbeitsdatenträger OFFSITE, wird der Datenträger erst dann aus dem Pool für aktive Daten gelöscht, wenn der Zugriffsmodus geändert wird. Ein Administrator kann den Server nach leeren ausgelagerten Arbeitsdatenträgern abfragen und diese an den Standort vor Ort zurückgeben.

Wenn Arbeitsdatenträger mit dem Einheitentyp FILE leer werden und gelöscht werden, wird der von den Datenträgern belegte Speicherbereich von dem Server freigegeben und an das Dateisystem zurückgegeben.

Tipp: Für serverübergreifende Operationen, die virtuelle Datenträger verwenden und ein kleines Datenvolumen speichern, sollte ein Wert für den Parameter MAXSCRATCH angegeben werden, der höher als der Wert ist, der normalerweise für Schreiboperationen für andere Datenträgertypen angegeben wird. Nach einer Schreiboperation auf einem virtuellen Datenträger markiert IBM Spectrum Protect den Datenträger als FULL, auch wenn der Wert des Parameters MAXCAPACITY in der Einheitenklassendefinition noch nicht erreicht wurde. Der IBM Spectrum Protect-Server behält virtuelle Datenträger nicht im Status FILLING und hängt keine Daten an. Ist der Wert des Parameters MAXSCRATCH zu niedrig, können serverübergreifende Operationen fehlschlagen.

#### REUsedelay

Gibt die Anzahl Tage an, die nach dem Löschen aller Dateien von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerpool zurückgestellt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Wert 0 bedeutet, dass ein Datenträger wieder beschrieben bzw. als Arbeitsdatenträger zurückgegeben werden kann, sobald alle Dateien auf dem Datenträger gelöscht wurden.

Tipp: Mit diesem Parameter kann sichergestellt werden, dass Datenbankverweise auf Dateien im Pool für aktive Daten noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird. Dieser Parameter muss auf einen Wert gesetzt werden, der größer als die Anzahl der Tage ist, die die älteste Datenbanksicherung aufbewahrt werden soll. Die für diesen Parameter angegebene Anzahl Tage muss der im Befehl SET DRMDBBACKUPEXPIREDAYS angegebenen Anzahl entsprechen.

#### OVFLOcation

Gibt den Überlaufstandort für den Speicherpool an. Der Server ordnet diesen Standortnamen einem Datenträger zu, der durch den Befehl MOVE MEDIA aus dem Kassettenarchiv ausgegeben wird. Dieser Parameter ist wahlfrei. Der Standortname darf maximal 255 Zeichen lang sein. Den Standortnamen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

Soll ein vorhandener Wert entfernt werden, eine Nullzeichenfolge ("" ) angeben.

#### CRCDData



Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist nur für Speicherpools mit dem Datenformat NATIVE gültig. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCDATA auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

Yes

Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da eine zusätzliche Verarbeitung erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

No

Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

Tipp:

Für Speicherpools, die dem Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet sind, bietet der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust als die CRC-Überprüfung für einen Speicherpool. Wenn Sie die CRC-Überprüfung für einen Speicherpool angeben, werden Daten nur während der Ausführung von Datenträgerprüfungsoperationen überprüft. Fehler werden identifiziert, nachdem Daten auf Band geschrieben wurden.

Um den Schutz logischer Blöcke zu aktivieren, geben Sie den Wert READWRITE für den Parameter LBPROTECT in den Befehlen DEFINE DEVCLASS und UPDATE DEVCLASS für den Einheitentyp 3592, LTO oder ECARTRIDGE an. Der Schutz logischer Blöcke wird nur für die folgenden Typen von Laufwerken und Datenträgern unterstützt:

- IBM® LTO5 und höher
- IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
- Oracle StorageTek T10000C- und T10000D-Laufwerke

DEDuplicate

Gibt an, ob die in diesem Speicherpool gespeicherten Daten dedupliziert werden. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.

IDENTIFYProcess

Gibt die Anzahl paralleler Prozesse an, die für die serverseitige Dateneduplizierung verwendet werden sollen. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Geben Sie einen Wert von 1 bis 50 ein.

Hinweis: Dateneduplizierungsprozesse können entweder aktiv oder inaktiv sein. Prozesse, die gegenwärtig Dateien bearbeiten, sind aktiv. Prozesse, die auf Dateien warten, die bearbeitet werden sollen, sind inaktiv. Prozesse bleiben inaktiv, bis Datenträger mit Daten, die dedupliziert werden sollen, verfügbar werden. Die Ausgabe des Befehls QUERY PROCESS für einen Dateneduplizierungsprozess umfasst die Gesamtzahl Byte und Dateien, die seit dem ersten Start des Prozesses verarbeitet wurden. Wenn beispielsweise ein Dateneduplizierungsprozess vier Dateien verarbeitet, dann inaktiv wird und anschließend fünf weitere Dateien verarbeitet, beträgt die Gesamtzahl der verarbeiteten Dateien neun. Prozesse werden nur beendet, wenn sie abgebrochen werden oder wenn die Anzahl Dateneduplizierungsprozesse für den Speicherpool in einen Wert geändert wird, der kleiner als die gegenwärtig angegebene Anzahl ist.


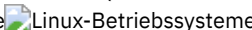

## Beispiel: Einen Pool für aktive Daten aktualisieren

Den Pool für aktive Daten TAPEPOOL2 aktualisieren, um die Verzögerungszeit für die Datenträgerwiederverwendung in 30 Tage zu ändern und Dateien nach Clientknoten zusammenzufassen.

```
update stgpool tapepool3 reusedelay=30 collocate=node
```

### Zugehörige Verweise:

SET DRMDBBACKUPEXPIREDAYS (Verfall für DB-Sicherungsreihe angeben)

## UPDATE STGPOOLDIRECTORY (Speicherpoolverzeichnis aktualisieren)

Mit diesem Befehl kann ein Speicherpoolverzeichnis aktualisiert werden.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung erforderlich.

### Syntax

```

>>-UPDate STGPOOLDIrectory--Poolname--Verzeichnis----->
                                     .-MAXPRocess---4-----.
>---ACcEss-----+READWrite---+-----+-----+----->
      +-READOnly-----+   '-MAXProcess---Anzahl-'
      +-DEStroyed---+
      '-UNAVailable-'

      .-Wait---No-----.
>---+-----+-----+----->
      '-Wait---No---+'
      '-Yes-'

```

## Parameter

### Poolname (Erforderlich)

Gibt den Speicherpool an, der das zu aktualisierende Verzeichnis enthält. Dieser Parameter ist erforderlich.

### Verzeichnis (Erforderlich)

Gibt ein Dateisystemverzeichnis des Speicherpools an. Dieser Parameter ist erforderlich.

### ACcEss (Erforderlich)

Gibt an, wie Clientknoten und Serverprozesse auf Dateien in dem Speicherpoolverzeichnis zugreifen können. Dieser Parameter ist erforderlich. Die folgenden Werte sind gültig:

#### READWrite

Gibt an, dass Dateien aus dem Speicherpoolverzeichnis gelesen und in das Speicherpoolverzeichnis geschrieben werden können.

#### READOnly

Gibt an, dass Dateien aus dem Speicherpoolverzeichnis gelesen werden können.

#### DEStroyed

Gibt an, dass Dateien dauerhaft beschädigt sind und aus dem Speicherpoolverzeichnis gelöscht werden müssen. Verwenden Sie diesen Zugriffsmodus, um anzugeben, dass ein gesamtes Speicherpoolverzeichnis wiederhergestellt werden muss.

Tipps:

- Markieren Sie Speicherpoolverzeichnisse als `DESTROYED`, bevor Sie die Datenwiederherstellung ausführen. Wenn das Speicherpoolverzeichnis als `DESTROYED` markiert ist, können Sie Datenbereiche auf dem Zielreplikationsserver wiederherstellen.
- Verwenden Sie den Parameter `MAXPROCESS`, um die Anzahl paralleler Prozesse anzugeben, die Sie zur Aktualisierung eines Speicherpoolverzeichnisses verwenden können.

#### UNAVailable

Gibt an, dass auf Dateien in dem Speicherpoolverzeichnis im Speicherpool nicht zugegriffen werden kann.

### MAXPRocess

Gibt die maximale Anzahl paralleler Prozesse für die Aktualisierung eines Speicherpoolverzeichnisses an. Dieser Parameter ist wahlfrei. Sie können einen Wert im Bereich von 1 bis 99 angeben. Der Standardwert ist 4.

Einschränkung: Dieser Parameter kann nur bei Angabe des Parameters `ACCESS=DESTROYED` verwendet werden.

Wenn Sie den Parameter `ACCESS=DESTROYED` angeben, wird jeder Container im Speicherpoolverzeichnis durch einen einzelnen Prozess aktualisiert. Falls die maximale Anzahl paralleler Prozesse größer oder gleich der Anzahl der Container ist, die aktualisiert werden müssen, wird für jeden Container nur ein einzelner Prozess erstellt. Überschreitet die Anzahl der Container den Wert des Parameters `MAXPROCESS`, wartet der Befehl die Beendigung von untergeordneten Prozessen ab, bevor neue Prozesse beginnen können.

### Wait

Dieser optionale Parameter gibt an, ob darauf gewartet werden soll, dass der IBM Spectrum Protect-Server die Verarbeitung dieses Befehls im Vordergrund beendet. Der Standardwert ist `NO`. Sie können die folgenden Werte angeben:

#### No

Der Server verarbeitet diesen Befehl im Hintergrund und Sie können mit anderen Tasks fortfahren, während der Befehl verarbeitet wird. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden entweder in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, je nachdem, wo die Nachrichten protokolliert werden.

#### Yes

Der Server verarbeitet diesen Befehl im Vordergrund. Die Verarbeitung der Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.

Einschränkung: Sie können nicht `WAIT=YES` an der Serverkonsole angeben.

## Beispiel: Ein Speicherpoolverzeichnis aktualisieren, um es zu löschen

Aktualisieren Sie ein Speicherpoolverzeichnis mit dem Namen DIR1 im Speicherpool POOL1, um es als dauerhaft beschädigt zu markieren.

```
update stgpooldirectory pool1 dir1 access=destroyed
```

## Beispiel: Ein Speicherpoolverzeichnis aktualisieren, um es in einem Cloud-Containerspeicherpool zu löschen

Aktualisieren Sie ein Speicherpoolverzeichnis mit dem Namen DIR3 im Cloud-Containerspeicherpool CLOUDLOCALDISK1, um es als gelöscht zu markieren.

```
update stgpooldirectory cloudlocaldisk1 dir3 access=destroyed
```

## Beispiel: Ein Speicherpoolverzeichnis aktualisieren, um es als nicht verfügbar zu markieren

Wenn das Speicherpoolverzeichnis nicht verfügbar ist, werden vom Server keine Daten aus dem Verzeichnis gelesen und keine Daten in das Verzeichnis geschrieben. Um den Zugriffsmodus für das Speicherpoolverzeichnis dir1 in dem Speicherpool pool1 in 'nicht verfügbar' zu aktualisieren, geben Sie den folgenden Befehl aus:

```
update stgpooldirectory pool1 dir1 access=unavailable
```

Tabelle 1. Zugehörige Befehle für UPDATE STGPOOLDIRECTORY

| Befehl                  | Beschreibung  |
|-------------------------|---|
| DEFINE STGPOOL          | Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.                      |
| DEFINE STGPOOLDIRECTORY | Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool. |
| DELETE STGPOOLDIRECTORY | Löscht ein Speicherpoolverzeichnis aus einem Verzeichniscontainer- oder Cloud-Containerspeicherpool.    |
| QUERY STGPOOLDIRECTORY  | Zeigt Informationen zu Speicherpoolverzeichnissen an.   |

## UPDATE STGRULE (Speicherregel für einen oder mehrere Speicherpools aktualisieren)

Verwenden Sie diesen Befehl, um eine Speicherregel für einen oder mehrere Speicherpools zu aktualisieren. Die Speicherregel plant das Tiering zwischen Containerspeicherpools. Sie können eine oder mehrere Speicherregeln für einen Containerspeicherpool aktualisieren.

### Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung erforderlich.

### Syntax

```
>>-UPDate STGRULE--Regelname----->
>+-----+
| .-,-----, |
| v          | |
|'---SRCpools---Quellenpool+--'|
>+-----+-----+----->
|'-TIERDelay---Verzögerung-' |'-MAXPRocess---Anzahl-'
>+-----+-----+----->
|'-DURation---+Minuten+-' |'-STARTTime---Uhrzeit-'
|'-NOLimit-'
>+-----+-----+-----<
|'-ACTIVE---+No---' |'-DESCRiption---Beschreibung-'
```

## Parameter

### Regelname (Erforderlich)

Gibt den Namen der Speicherregel an. Die maximale Länge des Namens beträgt 30 Zeichen.

### SRCPools

Gibt den Namen eines oder mehrerer Verzeichniscontainerspeicherpools an, aus denen Objekte mit Tiering in den Zielspeicherpool versetzt werden. Um mehrere Speicherpools anzugeben, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen.

### TIERDelay

Gibt die Anzahl Tage an, die gewartet werden soll, bevor die Speicherregel Objekte mit Tiering in den nächsten Speicherpool versetzt. Sie können eine ganze Zahl im Bereich von 0 bis 9999 angeben. Der Parameterwert gilt für alle Dateien in dem Speicherpool.

### MAXProcess

Gibt die maximale Anzahl paralleler Prozesse für die Ausführung der Speicherregel für jeden angegebenen Quellenspeicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert im Bereich von 1 bis 99 ein. Wenn Sie beispielsweise 4 Quellenspeicherpools haben und den Standardwert 8 für diesen Parameter angeben, werden 32 Prozesse gestartet.

### DURATION

Gibt die maximale Anzahl Minuten an, die die Speicherregel ausgeführt wird, bevor sie automatisch abgebrochen wird. Sie können eine Zahl im Bereich von 60 bis 1440 angeben. Wenn Sie den Wert NOLimit angeben, wird die Speicherregel bis zur Beendigung ausgeführt. Dieser Parameter ist wahlfrei.

### STARTTime

Gibt die Uhrzeit für den Anfang des Fensters an, in dem die Speicherregel zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Die Speicherregel wird täglich innerhalb von 5 Minuten nach der angegebenen Uhrzeit ausgeführt. Geben Sie einen der folgenden Werte an:

| Wert                  | Beschreibung  | Beispiel              |
|-----------------------|---|-----------------------|
| HH:MM:SS              | Eine bestimmte Uhrzeit.   | 23:30:08              |
| NOW                   | Die aktuelle Uhrzeit.   | NOW                   |
| NOW+HH:MM oder +HH:MM | Die aktuelle Uhrzeit plus die angegebene Anzahl Stunden und Minuten.  | NOW+02:00 oder +02:00 |
| NOW-HH:MM oder -HH:MM | Die aktuelle Uhrzeit minus die angegebene Anzahl Stunden und Minuten. | NOW-02:00 oder -02:00 |

### ACTIVE

Gibt an, ob die Speicherregelverarbeitung stattfindet. Dieser Parameter ist wahlfrei. Die folgenden Werte sind gültig:

No

Gibt an, dass die definierte Speicherregel inaktiv ist. Die Speicherregel wird nicht zum geplanten Zeitpunkt verarbeitet.

Yes

Gibt an, dass die definierte Speicherregel aktiv ist. Die Speicherregel wird zum geplanten Zeitpunkt verarbeitet.

### DESCRiption

Gibt eine Beschreibung der Speicherregel an. Dieser Parameter ist wahlfrei.

## Speicherregel aktualisieren

Eine Speicherregel mit dem Namen tieraction aktualisieren, um Daten aus den Verzeichniscontainerspeicherpools dirpool1 und dirpool2 in den Cloud-Containerspeicherpool cloudpool1 zu versetzen. Eine Startzeit von 23:30:08 Uhr und ein Maximum von 16 Prozessen angeben:

```
update stgrule tieraction srcpools=dirpool1,dirpool2
maxprocess=16 starttime=23:30:08
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE STGRULE

| Befehl         | Beschreibung                                    |
|----------------|---|
| DEFINE STGRULE | Definiert eine Speicherregel für Speicherpools. |
| DELETE STGRULE | Löscht Speicherregeln für Speicherpools.        |
| QUERY STGRULE  | Zeigt Informationen zu Speicherregeln an.       |

# UPDATE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs aktualisieren)

Verwenden Sie diesen Befehl, um eine Definition für die Zuordnung des virtuellen Dateibereichs zu aktualisieren.

Einschränkung: Sie können den Befehl UPDATE VIRTUALFSMAPPING nicht verwenden, um eine Zuordnung des virtuellen Dateibereichs für eine EMC Celerra- oder EMC VNX-NAS-Einheit zu aktualisieren. Sie müssen den Befehl DEFINE VIRTUALFSMAPPING verwenden.

Der NAS-Einheit muss eine Definition für eine Einheit zum Versetzen von Daten zugeordnet sein, da bei der Aktualisierung der Zuordnung eines virtuellen Dateibereichs durch den Server der Server die NAS-Einheit anspricht, um das virtuelle Dateisystem und den Dateisystemnamen zu prüfen.

## Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Systemberechtigung
- Uneingeschränkte Maßnahmenberechtigung
- Eingeschränkte Maßnahmenberechtigung für die Domäne, der der NAS-Knoten zugeordnet ist

## Syntax

```
>>-UPDate VIRTUALFSMapping--Knotenname--Name_des_virtuellen_Dateibereichs-->
>--+-----+----->
  '-FILESystem---neuer_Dateisystemname-'
>--+-----+-----+<<
  |                                     .-NAMEType---SERVER-----.|
  '-PATH---neuer_Pfadname--+-----+-'
                                     '-NAMEType---+SERVER-----+'
                                     '-HEXadecimal-'
```

## Parameter

Knotenname (Erforderlich)

Gibt den NAS-Knoten an, auf dem sich das Dateisystem und der Pfad befinden. Sie können keine Platzhalterzeichen verwenden und keine Liste mit Namen angeben.

Name\_des\_virtuellen\_Dateibereichs (Erforderlich)

Gibt die zu aktualisierende Zuordnung des virtuellen Dateibereichs an. Sie können keine Platzhalterzeichen verwenden und keine Liste mit Namen angeben.

FILESystem

Gibt den neuen Namen des Dateisystems an, in dem sich der Pfad befindet. Der Dateisystemname muss auf dem angegebenen NAS-Knoten vorhanden sein. Der Dateisystemname darf keine Platzhalterzeichen enthalten. Der Dateisystemname sollte nur geändert werden, wenn der Dateisystemname auf der NAS-Einheit geändert wird oder wenn beispielsweise das Verzeichnis in ein anderes Dateisystem versetzt wird. Dieser Parameter ist wahlfrei.

PATH

Gibt den neuen Pfad vom Stamm des Dateisystems zum Verzeichnis an. Der Pfad kann nur auf ein Verzeichnis verweisen. Der Pfad sollte nur geändert werden, wenn der Pfad auf der NAS-Einheit geändert wurde; beispielsweise, wenn das Verzeichnis in einen anderen Pfad versetzt wird. Die maximale Länge des Pfads beträgt 1024 Zeichen. Bei dem Pfadnamen muss die Groß-/Kleinschreibung beachtet werden. Dieser Parameter ist wahlfrei.

NAMEType

Gibt an, wie der Server den angegebenen Pfadnamen interpretieren soll. Geben Sie diesen Parameter nur an, wenn Sie einen Pfad angeben. Dieser Parameter ist nützlich, wenn ein Pfad Zeichen enthält, die nicht Teil der Codepage sind, in der der Server ausgeführt wird. Der Standardwert lautet SERVER.

Gültige Werte:

## SERVER

Die Codepage, in der der Server ausgeführt wird, wird zum Interpretieren des Pfads verwendet.

## HEXadecimal

Der Server interpretiert den eingegebenen Pfad als hexadezimale Darstellung des Pfads. Diese Option sollte verwendet werden, wenn ein Pfad Zeichen enthält, die nicht eingegeben werden können. Diese Situation kann beispielsweise auftreten, wenn für das NAS-Dateisystem eine Sprache definiert ist, die von der Sprache abweicht, in der der Server ausgeführt wird.

## Beispiel: Den Pfad für die Zuordnung des virtuellen Dateibereichs ändern

Die Zuordnung des virtuellen Dateibereichs mit dem Namen /mikeshomedir für den NAS-Knoten NAS1 aktualisieren, indem der Pfad geändert wird.

```
update virtualfsmapping nas1 /mikeshomedir path=/new/home/mike
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE VIRTUALFSMAPPING

| Befehl                  | Beschreibung   |
|-------------------------|--|
| DEFINE VIRTUALFSMAPPING | Zuordnung eines virtuellen Dateibereichs definieren. |
| DELETE VIRTUALFSMAPPING | Zuordnung eines virtuellen Dateibereichs löschen.    |
| QUERY VIRTUALFSMAPPING  | Zuordnung eines virtuellen Dateibereichs abfragen.   |

## UPDATE VOLHISTORY (History-Daten für sequentielle Datenträger aktualisieren)

Mit diesem Befehl können Datenträgerhistorydaten für einen Datenträger aktualisiert werden, der durch eine Datenbanksicherungs- oder Exportoperation erstellt wurde. Dieser Befehl gilt nicht für Speicherpooldatenträger.

Verwenden Sie den Befehl UPDATE BACKUPSET, um angegebene Datenträgerinformationen für Sicherungsgruppen in der Protokolldatei für Datenträger zu aktualisieren. Sie dürfen nicht diesen Befehl UPDATE VOLHISTORY verwenden, um Datenträgerinformationen für Sicherungsgruppen in der Protokolldatei für Datenträger zu aktualisieren.

## Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

## Syntax

```
>>-UPDate VOLHistory--Datenträgername----->
>--DEVclass-----Einheitenklassenname----->
>-----+----->
  '-LLocation-----Standort-'
>-----+-----<
  '-ORMState-----+Mountable-----+-'
    +-NOTMountable----+
    +-COURier-----+
    +-VAult-----+
    '-COURIERRetrieve-'
```

## Parameter

Datenträgername (Erforderlich)

Gibt den Datenträgernamen an. Der Datenträger muss für eine Datenbanksicherung oder eine Exportoperation verwendet worden sein.

DEVclass (Erforderlich)

Gibt den Namen der Einheitenklasse für den Datenträger an.

LOcation

Gibt den Standort des Datenträgers an. Dieser Parameter ist erforderlich, wenn der Parameter ORMSTATE nicht angegeben wird. Die maximale Textlänge beträgt 255 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält. Tipp: Der Befehl UPDATE VOLHISTORY unterstützt Aktualisierungen von Standortinformationen und ORMSTATE für Datenträger für Datenbankmomentaufnahmesicherungen.

**ORMState**

Gibt eine Änderung im Status eines Datenbanksicherungsdatenträgers an. Dieser Parameter ist erforderlich, wenn der Parameter LOCATION nicht angegeben wird. Dieser Parameter wird nur für Systeme unterstützt, die mit Disaster Recovery Manager lizenziert sind. Gültige Statusangaben sind:

**MOnstable**

Der Datenträger enthält gültige Daten und kann für die Verarbeitung vor Ort verwendet werden.

**NOTMOnstable**

Der Datenträger ist vor Ort, enthält gültige Daten und kann nicht für die Verarbeitung vor Ort verwendet werden.

**COUrier**

Der Datenträger wird ausgelagert.

**VAult**

Der Datenträger ist ausgelagert, enthält gültige Daten und kann nicht für die Verarbeitung vor Ort verwendet werden.

**COURIERretrieve**

Der Datenträger wird versetzt, so dass er wieder vor Ort ist.

## Beispiel: Den Standort eines Datenträgers aktualisieren, der für die Datenbanksicherung verwendet wird

In die Standortinformationen des Datenträgers BACKUP1, der für eine Datenbanksicherung verwendet wurde, soll die Angabe aufgenommen werden, dass der Datenträger ausgelagert wurde.

```
update volhistory backup1 devclass=tapebkup
location="700 w. magee rd."
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE VOLHISTORY

| Befehl            | Beschreibung  |
|-------------------|---|
| BACKUP VOLHISTORY | Zeichnet Datenträger-History-Daten in externen Dateien auf.                                   |
| DELETE VOLHISTORY | Löscht History-Daten sequenzieller Datenträger aus der Datenträger-History-Datei.             |
| MOVE DRMEDIA      | Versetzt DRM-Datenträger vor Ort und lagert sie aus.  |
| PREPARE           | Erstellt eine Wiederherstellungsplandatei.  |
| QUERY DRMEDIA     | Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an. |
| QUERY VOLHISTORY  | Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.            |

## UPDATE VOLUME (Speicherpooldatenträger ändern)

Mit diesem Befehl kann der Zugriffsmodus für einen oder mehrere Datenträger in Speicherpools geändert werden.

Eine Fehlerbedingung, die sich auf einen Datenträger bezieht, kann korrigiert werden, indem dem Datenträger der Zugriffsmodus READWRITE zugeordnet wird. Mit diesem Befehl lassen sich außerdem die Standortinformationen für einen oder mehrere Datenträger in Speicherpools mit sequentiellem Zugriff ändern.

## Berechtigungsklasse

Für diesen Befehl ist die System- oder die Bedienerberechtigung erforderlich.

## Syntax

```
(1)
>>-UPDate Volume-----Datenträgername----->
```

```

>-----+----->
  '-ACCess-----+READWrite-----+'
      +-READOnly-----+
      +-UNAVailable---+
      |           (2) |
      +-DEStroyed-----+
      |           (3) |
      '-OFFsite-----+'

>-----+----->
  |           (4) |
  '-LOcation-----Standort-'

  .-WHERESTGpool---*-----
>-----+----->
  '-WHERESTGpool---Poolname-'

  .-WHEREDEVclass---*-----
>-----+----->
  '-WHEREDEVclass---Einheitenklassenname-'

>-----+----->
  |           .-,----- . |
  |           V           | |
  '-WHEREACcEss-----+READWrite-----+'
      +-READOnly-----+
      +-UNAVailable-+
      +-OFFsite-----+
      '-DEStroyed---+'

>-----+----->
  |           .-,----- . |
  |           V           | |
  '-WHEREStatus-----+ONline-----+'
      +-OFFline-+
      +-EMPTy---+
      +-PENding-+
      +-FILLing-+
      '-FULl-----+'

  .-Preview---No-----
>-----+-----<
  '-Preview---+No--+-'
      '-Yes-'

```

Anmerkungen:

1. Mindestens ein Attribut (ACCESS oder LOCATION) muß aktualisiert werden.
2. Dieser Wert ist nur für Datenträger in primären Speicherpools gültig.
3. Dieser Wert ist nur für Datenträger in Kopierspeicherpools gültig.
4. Dieser Parameter ist nur für Datenträger in Speicherpools mit sequentiellm Zugriff gültig.

## Parameter

Datenträgername (Erforderlich)

Gibt den Speicherpooldatenträger an, der aktualisiert werden soll. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

ACCess

Gibt an, wie Clientknoten und Serverprozesse (wie Umlagerung) auf Dateien auf dem Speicherpooldatenträger zugreifen können. Dieser Parameter ist wahlfrei. Gültige Werte:

READWrite

Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff auf Dateien des Datenträgers haben.

Handelt es sich bei dem zu aktualisierenden Datenträger um einen leeren Arbeitsdatenträger, der den Zugriffsmodus OFFSITE (ausgelagert) hatte, löscht der Server den Datenträger aus der Datenbank.

READOnly

Gibt an, daß Client-Knoten und Server-Prozesse nur Lesezugriff auf Dateien des Datenträgers haben.

Handelt es sich bei dem zu aktualisierenden Datenträger um einen leeren Arbeitsdatenträger, der den Zugriffsmodus OFFSITE (ausgelagert) hatte, löscht der Server den Datenträger aus der Datenbank.



#### UNAVailable

Gibt an, dass weder Clientknoten noch Serverprozesse Zugriff auf Dateien haben, die auf dem Datenträger gespeichert sind.

Bevor ein Datenträger mit wahlfreiem Zugriff als nicht verfügbar gekennzeichnet wird, muß der Datenträger abgehängt werden. Nachdem ein Datenträger mit wahlfreiem Zugriff als nicht verfügbar gekennzeichnet wurde, kann der Datenträger nicht angehängt werden.

Wird ein Datenträger mit sequentiellm Zugriff als nicht verfügbar gekennzeichnet, versucht der Server nicht, den Datenträger zu laden.

Handelt es sich bei dem zu aktualisierenden Datenträger um einen leeren Arbeitsdatenträger, der den Zugriffsmodus OFFSITE (ausgelagert) hatte, löscht der Server den Datenträger aus der Datenbank.

#### DESTroyed

Gibt an, daß ein Datenträger für einen primären Speicherpool auf Dauer zerstört ist. Weder Client-Knoten noch Server-Prozesse können auf Dateien zugreifen, die auf dem Datenträger gespeichert sind. Mit diesem Zugriffsmodus kann angezeigt werden, dass ein gesamter Datenträger mit Hilfe des Befehls RESTORE STGPOOL zurückgeschrieben werden muss. Nachdem alle Dateien auf einem zerstörten Datenträger auf andere Datenträger zurückgeschrieben wurden, löscht der Server automatisch den zerstörten Datenträger aus der Datenbank.

Nur Datenträger in primären Speicherpools können in DESTROYED aktualisiert werden.

Bevor ein Datenträger mit wahlfreiem Zugriff in DESTROYED aktualisiert wird, muß der Datenträger abgehängt werden. Nachdem ein Datenträger mit wahlfreiem Zugriff in DESTROYED aktualisiert wurde, kann der Datenträger nicht angehängt werden.

Wird ein Datenträger mit sequentiellm Zugriff in DESTROYED aktualisiert, versucht der Server nicht, den Datenträger zu laden.

Enthält ein Datenträger keine Dateien und wird der Zugriffsmodus in DESTROYED geändert, löscht der Server den Datenträger aus der Datenbank.

#### Offsite

Gibt an, dass sich ein Datenträger eines Kopierspeicherpools oder Speicherpools für aktive Daten an einem ausgelagerten Standort befindet, an dem er nicht geladen werden kann. Nur Datenträger in Kopierspeicherpools oder Speicherpools für aktive Daten können den Zugriffsmodus OFFSITE haben.

Werden für beide Parameter (ACCESS und LOCATION) Werte angegeben, kann jedoch der Zugriffsmodus für einen bestimmten Datenträger nicht geändert werden, dann wird auch das Attribut für den Datenträgerstandort nicht geändert. Wird beispielsweise ACCESS=OFFSITE und ein Wert für LOCATION für einen Datenträger aus dem primären Speicherpool angegeben, wird weder der Wert für den Zugriff noch der Standort aktualisiert, da einem Datenträger aus dem primären Speicherpool nicht der Zugriffsmodus OFFSITE zugeordnet werden kann.

#### Location

Gibt den Standort des Datenträgers an. Dieser Parameter ist wahlfrei. Er kann nur für Datenträger in Speicherpools mit sequenziellm Zugriff angegeben werden. Die maximale Länge des Standorts beträgt 255 Zeichen. Wenn die Beschreibung des Standorts Leerzeichen enthält, muß sie in Anführungszeichen stehen. Soll ein zuvor definierter Standort entfernt werden, eine Nullzeichenfolge ("" ) angeben.

#### WHERESTGpool

Gibt den Namen des Speicherpools an, dessen Dateien aktualisiert werden sollen. Mit diesem Parameter kann die Aktualisierung auf den gewünschten Speicherpool beschränkt werden. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Speicherpoolname angegeben, werden die Datenträger aller Speicherpools aktualisiert.

#### WHEREDEVclass

Gibt den Namen der Einheitenklasse für die zu aktualisierenden Datenträger an. Mit diesem Parameter kann die Aktualisierung auf die gewünschte Einheitenklasse beschränkt werden. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Einheitenklassenname angegeben, werden Datenträger mit beliebiger Einheitenklasse aktualisiert.

#### WHEREACCess

Gibt den aktuellen Zugriffsmodus der zu aktualisierenden Datenträger an. Mit diesem Parameter kann die Aktualisierung auf Datenträger beschränkt werden, die gegenwärtig den angegebenen Zugriffsmodus haben. Dieser Parameter ist wahlfrei. Es können mehrere Zugriffsmodi angegeben werden, indem die Modi ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird kein Wert für diesen Parameter angegeben, wird die Aktualisierung nicht auf den aktuellen Zugriffsmodus eines Datenträgers beschränkt. Gültige Werte:

#### READWrite

Datenträger mit dem Zugriffsmodus READWRITE aktualisieren.

- READOnly  
Datenträger mit dem Zugriffsmodus READONLY aktualisieren.
- UNAVailable  
Datenträger mit dem Zugriffsmodus UNAVAILABLE aktualisieren.
- Offsite  
Datenträger mit dem Zugriffsmodus OFFSITE aktualisieren.
- DESTroyed  
Datenträger mit dem Zugriffsmodus DESTROYED aktualisieren.

#### WHEREStatus

Gibt den Status der zu aktualisierenden Datenträger an. Mit diesem Parameter kann die Aktualisierung auf Datenträger beschränkt werden, die einen angegebenen Status haben. Dieser Parameter ist wahlfrei. Es können mehrere Statuswerte angegeben werden, indem die Werte ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird kein Wert für diesen Parameter angegeben, wird die Aktualisierung nicht auf einen Datenträgerstatus beschränkt. Gültige Werte:

- ONline  
Datenträger mit dem Status ONLINE aktualisieren.
- Offline  
Datenträger mit dem Status OFFLINE aktualisieren.
- EMPTy  
Datenträger mit dem Status EMPTY aktualisieren.
- PENding  
Datenträger mit dem Status PENDING aktualisieren. Dabei handelt es sich um Datenträger, deren sämtliche Dateien gelöscht wurden, bei denen die für den Parameter REUSEDELAY angegebene Zeitspanne jedoch noch nicht abgelaufen ist.
- FILLing  
Datenträger mit dem Status FILLING aktualisieren.
- FULL  
Datenträger mit dem Status FULL aktualisieren.

#### Preview

Gibt an, ob die Aktualisierungsoperation vorab angezeigt werden soll, ohne Datenträger tatsächlich zu aktualisieren. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

- No  
Gibt an, daß die Datenträger tatsächlich aktualisiert werden sollen.
- Yes  
Gibt an, daß die Aktualisierungsoperation nur vorab angezeigt werden soll. Bei dieser Option werden die Datenträger, die aktualisiert werden sollen, zum Zeitpunkt der Operationsausführung angezeigt.

## Beispiel: Einen Banddatenträger nicht verfügbar machen

Den Banddatenträger DSMT20 aktualisieren, um ihn für Client-Knoten und Server-Prozesse als nicht verfügbar zu kennzeichnen.

```
update volume dsmt20 access=unavailable
```

## Beispiel: Den Zugriffsmodus aller ausgelagerten Datenträger in einem bestimmten Speicherpool aktualisieren

Alle leeren, ausgelagerten Datenträger im Speicherpool TAPEPOOL2 aktualisieren. Der Zugriffsmodus soll auf READWRITE gesetzt werden; außerdem sollen die Standortinformationen für die aktualisierten Datenträger gelöscht werden.

```
update volume * access=readwrite location="" wherestgpool=tapepool2
  whereaccess=offsite wherestatus=empty
```

## Zugehörige Befehle





Tabelle 1. Zugehörige Befehle für UPDATE VOLUME


| Befehl        | Beschreibung   |
|---------------|--|
| DEFINE VOLUME | Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll. |
| DELETE VOLUME | Löscht einen Datenträger aus einem Speicherpool.   |
| QUERY VOLUME  | Zeigt Informationen über Speicherpooldatenträger an.   |

| Befehl | Beschreibung  |
|--------|---|
| VARY   | Gibt an, ob ein Plattendatenträger für die Verwendung durch den Server verfügbar ist. |

## VALIDATE-Befehle

Mit dem Befehl VALIDATE kann überprüft werden, ob ein Objekt für IBM Spectrum Protect vollständig oder gültig ist.

-  Linux-Betriebssysteme VALIDATE ASPERA (Aspera FASP-Konfiguration validieren)
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme VALIDATE CLOUD (Cloudberechtigungs-nachweise prüfen)
- VALIDATE LANFREE (LAN-unabhängige Pfade prüfen)
- VALIDATE POLICYSET (Maßnahmengruppe prüfen)
- VALIDATE REPLICATION (Replikation für einen Clientknoten überprüfen)
- VALIDATE REPLPOLICY (Die Maßnahmen auf dem Zielreplikationsserver prüfen)

 Linux-Betriebssysteme

## VALIDATE ASPERA (Aspera FASP-Konfiguration validieren)

Mit diesem Befehl können Sie ermitteln, ob die Aspera FASP-Technologie (FASP = Fast Adaptive Secure Protocol) verwendet werden kann, um die Datenübertragung in Ihrer Systemumgebung zu optimieren. Sie können insbesondere feststellen, ob die Aspera FASP-Technologie einen besseren Netzdurchsatz als die TCP/IP-Technologie erzielen würde.

Dieser Befehl prüft außerdem die folgenden Aspekte:

- Ordnungsgemäße Konfiguration der Systemumgebung für die Verwendung der Aspera FASP-Technologie
- Installation der erforderlichen Lizenzen für die Aktivierung der Aspera FASP-Technologie

Mit der Aspera FASP-Technologie wird die Datenübertragung für die Knotenreplikation oder den Speicherpoolschutz in einem Weitverkehrsnetz (WAN) optimiert. Ihr System muss jedoch nicht zwingend für die Knotenreplikation oder den Speicherpoolschutz konfiguriert sein, damit der Befehl VALIDATE ASPERA ausgeführt werden kann. Falls Ihr System für die Knotenreplikation oder den Speicherpoolschutz in einer lokalen Umgebung konfiguriert ist, können Sie durch Ausgabe des Befehls bewerten, ob die Daten auf einem fernen Server erfolgreich repliziert werden können.

Dieser Befehl ist nur bei Linux x86\_64-Betriebssystemen verfügbar.

Führen Sie die folgenden Tasks aus, bevor Sie den Befehl ausgeben:

1. Stellen Sie sicher, dass in Ihrer Systemumgebung mindestens ein Server definiert ist. Geben Sie den Befehl PING SERVER aus, um sicherzustellen, dass Konnektivität zum definierten Server besteht. Geben Sie beispielsweise für einen Server namens VMRH6T den folgenden Befehl aus:

```
ping server vmrh6t
```

2. Um den Befehl VALIDATE ASPERA zur Ermittlung der Netzdurchsatzgeschwindigkeit einzusetzen, installieren Sie auf dem Quellen- und dem Zielsystem Testlizenzen mit einer Gültigkeit von 30 Tagen oder uneingeschränkte Volllizenzen. Installieren Sie beispielsweise Lizenzen auf dem Quellensystem und dem Zielsystem VMRH6 bzw. VMRH6T. Im Abschnitt Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann ist beschrieben, wie Sie Lizenzen beziehen und installieren können.

Um eine Umgebung zu simulieren, die mehrere Sitzungen verwendet, können Sie mehrere Instanzen des Befehls VALIDATE ASPERA gleichzeitig ausführen. Falls Sie die Ausführung mehrerer Sitzungen planen, kann es sinnvoll sein, die Bandbreite jeder Netzverbindung zu begrenzen, um sicherzustellen, dass für alle Netzverbindungen ausreichend Bandbreite verfügbar ist. Zum Begrenzen der Bandbreite geben Sie die Serveroption FASPTARGETRATE wie im Abschnitt FASPTARGETRATE beschrieben an.

Sie können das aktuelle Übertragungsvolumen abfragen, indem Sie den Befehl QUERY PROCESS ausgeben:

```
query process
```

Die Prozessnummer können Sie der Ausgabe des Befehls QUERY PROCESS entnehmen. Sie können den Prozess abbrechen, indem Sie den Befehl CANCEL PROCESS ausgeben und hierbei die Prozessnummer angeben. Beispiel:

```
cancel process 3
```

## Berechtigungs-klasse

Jeder Administrator kann diesen Befehl ausgeben.

## Syntax

---

```
>>-VALidate ASPera---+-----+-----+----->
                        '---Zielservername---'
                                .-Wait-----No-----
>+-----+-----+-----+-----<
'-DURation-----Sekunden-' '-Wait-----+No--+'
                                '-Yes-'
```

## Parameter

---

### Zielservername

Gibt einen zuvor definierten Server an. Dieser Parameter ist wahlfrei. Für die Angabe dieses Parameters gelten die folgenden Richtlinien:

- Um festzustellen, ob Aspera FASP einen Knotenreplikationsprozess optimieren kann, geben Sie einen Zielservers an, der für die Knotenreplikation konfiguriert ist.
- Um festzustellen, ob Aspera FASP einen Speicherpoolschutzprozess optimieren kann, geben Sie einen Zielservers an, der für den Speicherpoolschutz konfiguriert ist.
- Um festzustellen, ob Aspera FASP die Datenübertragung an einen fernen Server optimieren kann, der definiert, aber nicht für den Speicherpoolschutz oder die Knotenreplikation konfiguriert ist, geben Sie diesen Zielservers an.
- Falls Sie keinen Zielservers angeben, besagt die Befehlsausgabe, ob der Quellenservers ordnungsgemäß für die Datenübertragung mit Aspera FASP konfiguriert ist. In der Ausgabe ist außerdem angegeben, ob auf dem Quellenservers eine gültige Lizenz für Aspera FASP installiert ist.

### DURation

Gibt in Sekunden die zur Auswertung des Durchsatzes zugeordnete Zeit für die Übertragung von Daten im Netz an. Dieser Parameter ist wahlfrei. Der Standardwert ist 120 Sekunden. Sie können einen Wert im Bereich von 120 bis 3600000 Sekunden angeben. Die zugeordnete Zeit wird zwischen Aspera FASP- und TCP/IP-Datenübertragungen aufgeteilt.

### Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Befehlsverarbeitung beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

#### No

Gibt an, dass der Server den Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Bei Angabe von NO werden die Ausgabenachrichten im Aktivitätenprotokoll angezeigt.

#### Yes

Gibt an, dass der Server den Befehl im Vordergrund verarbeitet. Die Verarbeitung der Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Bei Angabe von YES werden die Ausgabenachrichten im Verwaltungsbefehlszeilenclient angezeigt.

Einschränkung: Sie können nicht WAIT=YES an der Serverkonsole angeben.

## Beispiel: Informationen zum Status einer Aspera FASP-Konfiguration anzeigen

---

Führen Sie auf dem Quellenservers den Befehl `VALIDATE ASPERA` aus. Um sicherzustellen, dass Nachrichten im Verwaltungsbefehlszeilenclient angezeigt werden, geben Sie `WAIT=YES` an. Für Felddesreibungen siehe Felddesreibungen.

```
validate aspera wait=yes
```

```
ANR3836I Überprüfung der Aspera FASP-Verbindung von VMRH6 zu localhost.
Mit FASP übertragenes Volumen: 0 MB pro Sekunde. Mit TCP/IP übertragenes
Volumen: 0 MB pro Sekunde. Latenzzeit: 0 Mikrosekunden. Status: OK. Tage bis
zum Ablauf der Lizenz: Never.
```

## Beispiel: Installation der erforderlichen Lizenzen überprüfen

---

Führen Sie auf dem Quellenservers den Befehl `VALIDATE ASPERA` aus und geben Sie den Zielreplikationsservers an. Um sicherzustellen, dass Nachrichten im Verwaltungsbefehlszeilenclient angezeigt werden, geben Sie `WAIT=YES` an. Für Felddesreibungen siehe Felddesreibungen.

```
validate aspera vmrh6t wait=yes
```

ANR0984I Prozess 8 für VALIDATE ASPERA im FOREGROUND um 09:35:21 AM gestartet.  
 ANR3672E Die Lizenzdatei, die zum Aktivieren der Aspera FASP-Technologie (FASP = Fast Adaptive Secure Protocol) erforderlich ist, wurde auf dem Server VMRH6 nicht gefunden.  
 ANR3836I Überprüfung der Aspera FASP-Verbindung von VMRH6 zu localhost. Mit FASP übertragenes Volumen: 0 MB pro Sekunde. Mit TCP/IP übertragenes Volumen: 0 MB pro Sekunde. Latenzzeit: 0 Mikrosekunden. Status: Ungültige Konfiguration. Tage bis zum Ablauf der Lizenz: Abgelaufen.  
 ANR0985I Prozess 8 für VALIDATE ASPERA, der im FOREGROUND ausgeführt wird, mit Beendigungsstatus FAILURE um 09:35:21 AM beendet.  
 ANR1893E Prozess 8 für VALIDATE ASPERA wurde mit dem Beendigungsstatus FAILURE beendet.

## Feldbeschreibungen

### Status

Der Status der Konfiguration. Die folgenden Werte sind gültig:

- **OK** gibt an, dass keine Probleme erkannt wurden.
- **Ungültige Konfiguration** gibt an, dass eine Konfigurationsdatei, eine Lizenzdatei oder eine Aspera FASP-Bibliotheksdatei fehlt.
- **Lizenzproblem** gibt an, dass eine Lizenz fehlt, ungültig ist oder abgelaufen ist.
- **Serverfehler** gibt an, dass alle Ports belegt sind, dass ein Fehler beim Schreib-/Lesezugriff im Netz aufgetreten ist oder dass keine Daten in die Aspera FASP-Protokolldatei geschrieben werden können.
- **Ungültige Zielkonfiguration** gibt an, dass eine Konfigurationsdatei, Lizenzdatei oder Aspera FASP-Bibliotheksdatei auf dem Zielsever fehlt.
- **Fehler auf Zielsever** gibt an, dass alle Ports belegt sind, dass ein Fehler beim Schreib-/Lesezugriff im Netz aufgetreten ist oder dass keine Daten in die Aspera FASP-Protokolldatei geschrieben werden können.
- **Lizenzproblem auf Zielsever** gibt an, dass eine Lizenz auf dem Zielsever ungültig oder abgelaufen ist.
- **Nicht unterstütztes Betriebssystem** gibt an, dass auf einem oder beiden Servern ein anderes Betriebssystem als Linux x86\_64 installiert ist.
- **Unbekannt** gibt an, dass ein unerwarteter Fehler aufgetreten ist. Prüfen Sie die Protokollnachrichten, um den Fehler zu ermitteln.

### Tage bis zum Ablauf der Lizenz

Die folgenden Werte sind gültig:

- **Never** gibt an, dass eine uneingeschränkte Volllizenz installiert ist.
- **Heute** gibt an, dass eine Testlizenz mit einer Gültigkeit von 30 Tagen installiert ist, die heute abläuft.
- **Abgelaufen** gibt an, dass eine Testlizenz mit einer Gültigkeit von 30 Tagen installiert, jedoch abgelaufen ist.
- **Eine Anzahl** gibt an, dass eine Testlizenz mit einer Gültigkeit von 30 Tagen installiert ist, die in der angegebenen Anzahl von Tagen abläuft.
- **Lizenz nicht gefunden** gibt an, dass keine Lizenz gefunden wurde.

### Übertragenes Volumen mit TCP/IP

Die Geschwindigkeit der Datenübertragung mit TCP/IP-Technologie in Megabyte pro Sekunde.

### Übertragenes Volumen mit FASP







Die Geschwindigkeit der Datenübertragung mit Aspera FASP-Technologie in Megabyte pro Sekunde.

### Latenzzeit

Die Latenzzeit der Datenübertragung in Mikrosekunden.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für VALIDATE ASPERA

| Befehl   | Beschreibung   |
|--|--|
| CANCEL SESSION   | Bricht aktive Sitzungen mit dem Server ab.   |
| DEFINE SERVER  | Definiert einen Server für die Übertragung zwischen Servern.   |
| PING SERVER  | Testet die Verbindungen zwischen Servern.  |
|  AIX-Betriebssysteme  Linux-Betriebssysteme<br> Windows-Betriebssysteme PROTECT STGPOOL |  AIX-Betriebssysteme  Linux-Betriebssysteme<br> Windows-Betriebssysteme Schützt einen Verzeichniscontainerspeicherpool. |

| Befehl         | Beschreibung   |
|----------------|--|
| REPLICATE NODE | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören. |

## VALIDATE CLOUD (Cloudberechtigungsachweise prüfen)

Bevor Sie einen Speicherpool definieren, verwenden Sie diesen Befehl, um sicherzustellen, dass die Berechtigungsachweise für einen Cloud-Containerspeicherpool gültig sind und dem Benutzer die erforderlichen Berechtigungen erteilt wurden.

### Berechtigungsachweise

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```

      .-CLOUDType-----Swift-----
>>-VALidate CLOud-+-----+----->
      '-CLOUDType-----+AZure-----+'
                    +-S3-----+
                    +-SOftlayer-+
                    +-SWift-----+
                    '-V1Swift----'

                                (1)
>--CLOUDUrl-----Cloud-URL--IDentity-----Cloud-ID----->
>--PAssword-----Kennwort-----+-----<
                    |                               (2) |
                    '-BUCKETName-----Bucketname-----'

```

Anmerkungen:

1. Wenn Sie CLOUDTYPE=AZURE angeben, geben Sie nicht den Parameter IDENTITY an.
2. Der Parameter BUCKETNAME ist nur gültig, wenn Sie CLOUDTYPE=S3 angeben.

### Parameter

#### CLOUDType

Gibt den Typ der Cloudumgebung an, in der der Speicherpool konfiguriert wird. Sie können einen der folgenden Werte angeben:

#### AZure

Gibt an, dass der Speicherpool ein Cloud-Computing-System 'Microsoft Azure' verwendet.

#### S3

Gibt an, dass der Speicherpool ein Cloud-Computing-System mit dem Protokoll 'Simple Storage Service' (S3) verwendet, wie z. B. IBM® Cloud Object Storage oder Amazon Web Services (AWS) S3.

#### SOftlayer

Gibt an, dass der Speicherpool ein Cloud-Computing-System 'IBM SoftLayer' (IBM Bluemix) mit einem Cloud-Computing-System 'OpenStack Swift' verwendet.

#### SWift

Gibt an, dass der Speicherpool ein Cloud-Computing-System 'OpenStack Swift' verwendet. Dieser Wert gibt auch an, dass der Speicherpool Version 2 des Protokolls für die Authentifizierung bei der Cloud verwendet. Die URL der Cloud enthält normalerweise die Versionsnummer des verwendeten Protokolls.

#### V1Swift

Gibt an, dass der Speicherpool ein Cloud-Computing-System 'OpenStack Swift' verwendet. Dieser Wert gibt auch an, dass der Speicherpool Version 1 des Protokolls für die Authentifizierung bei der Cloud verwendet. Die URL der Cloud enthält normalerweise die Versionsnummer des verwendeten Protokolls.

Dieser Parameter ist wahlfrei. Wird der Parameter nicht angegeben, wird der Standardwert SWIFT verwendet.

#### CLOUDUrl (Erforderlich)

Gibt die URL der Cloudumgebung an, in der Sie den Speicherpool konfigurieren. Auf der Basis Ihres Cloud-Providers können Sie einen BLOB-Dienstendpunkt, eine Regionsendpunkt-URL, eine Accesser-IP-Adresse, einen Endpunkt für öffentliche Authentifizierung (Public Authentication Endpoint) oder einen ähnlichen Wert für diesen Parameter verwenden. Stellen Sie sicher,

dass das Protokoll wie z. B. `https://` oder `http://` am Anfang der URL eingefügt wird. Die maximale Länge der Webadresse beträgt 870 Zeichen. Der Parameter CLOUDURL wird geprüft, wenn die erste Sicherung beginnt.

#### Identity (Erforderlich)

Gibt die Benutzer-ID für die Cloud an. Dieser Parameter ist für alle unterstützten Cloud-Computing-Systeme außer Azure erforderlich. Wenn Sie CLOUDTYPE=AZURE angeben, geben Sie nicht den Parameter IDENTITY an. Auf der Basis Ihres Cloud-Providers können Sie eine Zugriffsschlüssel-ID, einen Benutzernamen, einen Tenantenamen und Benutzernamen oder einen ähnlichen Wert für diesen Parameter verwenden. Die maximale Länge der Benutzer-ID beträgt 255 Zeichen.

#### PAssword (Erforderlich)

Gibt das Kennwort für die Cloud an. Auf der Basis Ihres Cloud-Providers können Sie ein SAS-Token (SAS = Shared Access Signature), einen geheimen Zugriffsschlüssel, einen API-Schlüssel, ein Kennwort oder einen ähnlichen Wert für diesen Parameter verwenden. Dieser Parameter ist erforderlich. Die maximale Länge des Kennworts beträgt 255 Zeichen.

#### BUCKETName

Gibt den Namen für ein AWS S3-Bucket oder eine IBM Cloud Object Storage-Vault an, das bzw. die anstelle des Standardbuckets oder der Standardvault mit diesem Speicherpool verwendet werden soll. Dieser Parameter ist optional und ist nur gültig, wenn Sie CLOUDTYPE=S3 angeben. Wenn ein Bucket oder eine Vault mit dem angegebenen Namen vorhanden ist, wird dieses Bucket oder diese Vault getestet, um sicherzustellen, dass die korrekten Berechtigungen definiert sind. Ist das Bucket oder die Vault nicht vorhanden, wird mit dem Parameter nur verifiziert, dass kein Bucket oder keine Vault mit diesem Namen vorhanden ist. Beachten Sie die Einschränkungen bei der Benennung für Ihren Cloud-Provider, wenn Sie diesen Parameter angeben. Überprüfen Sie die Berechtigungen für das Bucket oder die Vault und stellen Sie sicher, dass die Berechtigungsnachweise über die Berechtigung zum Lesen, Schreiben, Auflisten und Löschen von Objekten in diesem Bucket oder dieser Vault haben.

Tipp: Wird der Parameter BUCKETNAME nicht angegeben, wird die global eindeutige Replikations-ID als Standardbucketname verwendet. Der Standardwert ist

```
ibmsp GUID
```

. Dabei ist GUID der Wert für REPLICATION GLOBALLY UNIQUE ID, minus der Punkte, in der Ausgabe des Befehls QUERY REPLSERVER. Lautet die global eindeutige Replikations-ID beispielsweise 52.82.39.20.64.d0.11.e6.9d.77.0a.00.27.00.00.00, ist der Standardbucketname `ibmsp.5282392064d011e69d770a0027000000`.

## Beispiel: Berechtigungsnachweise eines S3-Cloud-Containerspeicherpools prüfen

Die Berechtigungsnachweise des Cloud-Containerspeicherpools prüfen.

```
validate cloud
cloudtype=s3 cloudurl=http://123.234.123.234:5000/v2.0
password=protect8991 bucketname=ibmsp.5282392064d011e69d770a0027000000
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für VALIDATE CLOUD

| Befehl                           | Beschreibung                                    |
|----------------------------------|---|
| DEFINE STGPOOL (Cloud-Container) | Definiert einen Cloud-Containerspeicherpool.    |
| QUERY REPLSERVER                 | Zeigt Informationen zu Replikationsservern an.  |
| UPDATE STGPOOL (Cloud-Container) | Aktualisiert einen Cloud-Containerspeicherpool. |

## VALIDATE LANFREE (LAN-unabhängige Pfade prüfen)

Verwenden Sie diesen Befehl, um zu bestimmen, welche Ziele für einen bestimmten Knoten, der einen spezifischen Speicheragenten verwendet, für die LAN-unabhängige Datenversetzung verwendet werden können.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
>>-VALidate LANfree--Knotenname--Speicheragentenname-----<<
```

## Parameter

Knotenname (Erforderlich)

Der Name des Knotens, der ausgewertet werden soll.  
 Speicheragentenname (Erforderlich)  
 Der Name des Speicheragenten, der ausgewertet werden soll.

## Beispiel: Eine aktuelle LAN-unabhängige Konfiguration prüfen

Die aktuellen Serverdefinitionen und die Konfiguration des Knotens TIGER für die Verwendung des Speicheragenten AIX\_STA1 für LAN-unabhängige Datenoperationen prüfen.

```
validate lanfree tiger aix_stal
```

| Knoten-<br>name | Speicher-<br>agent | Operation | Verw.-<br>Klasse | Ziel-<br>name | LAN-<br>unabhängig? | Erläuterung   |
|-----------------|--------------------|-----------|------------------|---------------|---------------------|---|
| TIGER           | AIX_STA1           | BACKUP    | STANDARD         | OUTPOOL       | NO                  | Keine verfügbaren<br>Onlinepfade.<br>Zielspeicher-<br>pool ist für<br>simultanes<br>Schreiben<br>konfiguriert.                        |
| TIGER           | AIX_STA1           | BACKUP    | STANDARD         | PRIMARY       | NO                  |   |
| TIGER           | AIX_STA1           | BACKUP    | STANDARD         | SHRPOOL       | YES                 | Speicherpool<br>enthält von Clients<br>deduplizierte Daten<br>und ist für<br>Speicheragenten<br>V6.1 oder früher<br>nicht zugänglich. |
| TIGER           | AIX_STA1           | BACKUP    | NOARCH           | LFFILE        | NO                  |   |
| TIGER           | AIX_STA1           | ARCHIVE   | STANDARD         | OUTPOOL       | NO                  | Keine verfügbaren<br>Onlinepfade.   |
| TIGER           | AIX_STA1           | ARCHIVE   | STANDARD         | PRIMARY       | NO                  | Zielspeicher-<br>pool ist für<br>simultanes<br>Schreiben<br>konfiguriert.   |
| TIGER           | AIX_STA1           | ARCHIVE   | STANDARD         | SHRPOOL       | YES                 |   |

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für VALIDATE LANFREE

| Befehl          | Beschreibung  |
|-----------------|---|
| QUERY COPYGROUP | Zeigt die Attribute einer Kopiengruppe an.  |
| QUERY DEVCLASS  | Zeigt Informationen zu Einheitenklassen an.   |
| QUERY DOMAIN    | Zeigt Informationen über Maßnahmendomänen an.   |
| QUERY DRIVE     | Zeigt Informationen zu Laufwerken an.   |
| QUERY LIBRARY   | Zeigt Informationen zu einem oder zu mehreren<br>Kassettenarchiven an.  |
| QUERY MGMTCLASS | Zeigt Informationen zu Verwaltungsklassen an.   |
| QUERY NODE      | Zeigt Informationen zu einem oder mehreren Clients teilweise<br>oder vollständig an.                                    |
| QUERY PATH      | Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.   |
| QUERY POLICYSET | Zeigt Informationen über Maßnahmengruppen an.   |
| QUERY SERVER    | Zeigt Informationen über Server an.   |
| QUERY STATUS    | Zeigt die Einstellungen von Serverparametern an, beispielsweise<br>die mit den SET-Befehlen ausgewählten Einstellungen. |
| QUERY STGPOOL   | Zeigt Informationen zu Speicherpools an.  |

## VALIDATE POLICYSET (Maßnahmengruppe prüfen)

Mit diesem Befehl kann geprüft werden, ob eine Maßnahmengruppe vollständig und gültig ist, bevor sie aktiviert wird. Der Befehl untersucht die Verwaltungsklassen- und Kopiengruppendefinitionen in der Maßnahmengruppe und meldet Bedingungen, die vor der



Aktivierung der Maßnahmengruppe berücksichtigt werden müssen.

Der Befehl VALIDATE POLICYSET schlägt fehl, wenn eine der folgenden Bedingungen vorhanden ist:

- Die Maßnahmengruppe hat keine Standardverwaltungs-klasse.
- Eine Kopiergruppe in der Maßnahmengruppe gibt einen Kopierspeicherpool als Zielort an.
- Eine Verwaltungs-klasse gibt einen Kopierspeicherpool als Zielort für Dateien an, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.
- Ein Parameter TOCDESTINATION ist angegeben, und der Speicherpool ist entweder ein Kopienpool oder der Speicherpool hat ein anderes Format als NATIVE oder NONBLOCK.

Der Server gibt für folgende Bedingungen Warnungen aus:

- Eine Kopiergruppe gibt einen Speicherpool an, der als Zielort für gesicherte oder archivierte Dateien nicht vorhanden ist.

Wird eine Maßnahmengruppe mit Kopiergruppen aktiviert, die nicht vorhandene Speicher-pools angeben, schlagen die Sicherungs- oder Archivierungsoperationen des Clients fehl.

- Eine Verwaltungs-klasse gibt einen Speicherpool an, der als Zielort für Dateien, die von IBM Spectrum Protect for Space Management-Clients umgelagert werden, nicht vorhanden ist.
- Die Maßnahmengruppe verfügt nicht über eine oder mehrere Verwaltungs-klassen, die in der aktuellen aktiven (ACTIVE) Maßnahmengruppe vorhanden sind.

Wird die Maßnahmengruppe aktiviert, werden Sicherungsdateien, die an die gelöschten Verwaltungs-klassen gebunden sind, erneut an die Standardverwaltungs-klasse in der neuen aktiven Maßnahmengruppe gebunden.

- Die Maßnahmengruppe verfügt nicht über eine oder mehrere Kopiergruppen, die in der aktuellen aktiven (ACTIVE) Maßnahmengruppe vorhanden sind.

Wird die Maßnahmengruppe aktiviert, werden Dateien, die an die Verwaltungs-klassen mit den gelöschten Kopiergruppen gebunden sind, nicht mehr archiviert bzw. gesichert.

- Die Standardverwaltungs-klasse für die Maßnahmengruppe enthält keine Sicherungs- oder Archivierungskopiergruppe.

Wird die Maßnahmengruppe mit dieser Standardverwaltungs-klasse aktiviert, können Clients, die den Standardwert verwenden, keine Dateien sichern bzw. archivieren.

- Eine Verwaltungs-klasse gibt an, daß eine Sicherungs-version vorhanden sein muß, bevor eine Datei aus einem Client-Knoten umgelagert werden kann (MIGREQUIRESBKUP=YES), aber die Verwaltungs-klasse enthält keine Sicherungskopiergruppe.

Ist für den Server der Aufbewahrungsschutz für Daten aktiviert, müssen die folgenden Bedingungen zutreffen:

- Alle Verwaltungs-klassen in der Maßnahmengruppe, die geprüft werden soll, müssen eine Archivierungskopiergruppe enthalten.
- Ist eine Verwaltungs-klasse in der aktiven Maßnahmengruppe vorhanden, muss eine Verwaltungs-klasse mit demselben Namen in der Maßnahmengruppe vorhanden sein, die geprüft werden soll.
- Ist eine Archivierungskopiergruppe in der aktiven Maßnahmengruppe vorhanden, muss die entsprechende Kopiergruppe in der zu prüfenden Maßnahmengruppe über einen Wert für RETVER verfügen, der mindestens so groß wie die entsprechenden Werte in der aktiven Kopiergruppe ist.

## Berechtigungsklasse

---

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Maßnahmengruppe gehört.

## Syntax

---

```
>>-VALidate Policyset--Domänenname--Name_der_Maßnahmengruppe---><
```

## Parameter

---

Domänenname (Erforderlich)

Gibt den Namen der Maßnahmendomäne an, der die Maßnahmengruppe zugeordnet wird.

Name\_der\_Maßnahmengruppe (Erforderlich)

Gibt den Namen der Maßnahmengruppe an, die geprüft werden soll.

## Beispiel: Eine bestimmte Maßnahmengruppe prüfen

---

Die Maßnahmengruppe VACATION, die sich in der Maßnahmendomäne EMPLOYEE\_RECORDS befindet, soll ausgewertet werden.

```
validate policyset employee_records vacation
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für VALIDATE POLICYSET

| Befehl             | Beschreibung  |
|--------------------|---|
| ACTIVATE POLICYSET | Wertet eine Maßnahmengruppe aus und aktiviert sie.  |
| COPY POLICYSET     | Erstellt eine Kopie einer Maßnahmengruppe.  |
| DEFINE COPYGROUP   | Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse. |
| DEFINE MGMTCLASS   | Definiert eine Verwaltungsklasse.   |
| DELETE POLICYSET   | Löscht eine Maßnahmengruppe einschließlich ihrer Verwaltungsklassen und Kopiengruppen aus einer Maßnahmendomäne.              |
| QUERY POLICYSET    | Zeigt Informationen über Maßnahmengruppen an.   |
| UPDATE COPYGROUP   | Ändert ein oder mehrere Attribute einer Kopiengruppe.   |
| UPDATE POLICYSET   | Ändert die Beschreibung einer Maßnahmengruppe.  |

## VALIDATE REPLICATION (Replikation für einen Clientknoten überprüfen)

Verwenden Sie diesen Befehl, um die Replikationsregeln zu identifizieren, die für Dateibereiche in Clientknoten gelten, die für die Replikation konfiguriert sind. Sie können mit diesem Befehl auch überprüfen, ob der Quellenreplikationsserver mit dem Zielreplikationsserver kommunizieren kann.

Bevor Sie mit der Replikationsverarbeitung beginnen, verwenden Sie den Befehl VALIDATE REPLICATION, um zu bestimmen, ob Ihre Replikationskonfiguration korrekt ist.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

## Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

## Syntax

```
      .-+-----+
      v          |
>>-VALidate REPLication-----Knotenname----->
      .-VERIFYconnection-----No-----
>-+-----+-----+-----><
  '-VERIFYconnection-----+No--+
      '-Yes-'
```

## Parameter

Knotenname (Erforderlich)

Gibt den Namen des Clientknotens an, dessen Dateibereiche angezeigt werden sollen. Werden mehrere Clientknotenamen angegeben, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

Informationen werden nur zu den Clientknoten angezeigt, die für die Replikation aktiviert oder inaktiviert sind. Der Replikationsmodus muss SEND lauten. Um zu bestimmen, ob ein Clientknoten für die Replikation und ihren Modus aktiviert oder inaktiviert ist, geben Sie den Befehl QUERY NODE aus. Überprüfen Sie die Werte in den Feldern 'Replikationsstatus' und 'Replikationsmodus'.

VERIFYconnection

Gibt an, ob die Verbindung zu einem Zielreplikationsserver überprüft werden soll. Die Version des Zielreplikationsservers wird ebenfalls überprüft, um sicherzustellen, dass es sich um Version 6.3 oder eine höhere Version handelt. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No

Die Verbindung und Version des Zielreplikationsservers werden nicht überprüft.

Yes

Die Verbindung und Version des Zielreplikationsservers werden überprüft.

## Beispiel: Die Replikation für einen Clientknoten überprüfen

---

Der Name des Clientknotens ist NODE1. Den Verbindungsstatus zwischen dem Quellen- und dem Zielreplikationsserver überprüfen.

```
validate replication nodel verifyconnection=yes

        Knotenname: NODE1
        Dateibereichsname: \\nodel\c$
        FSID: 1
        Typ: Bkup
        Steuernde Replikationsregel: ACTIVE_DATA
        Replikationsregelebene: Systemebene
        Servername: DRSRV
        Verbindungsstatus: Gültige Verbindung

        Knotenname: NODE1
        Dateibereichsname: \\nodel\c$
        FSID: 1
        Typ: Arch
        Steuernde Replikationsregel: ALL_DATA_HIGH_PRIORITY
        Replikationsregelebene: Knotenebene
        Servername: DRSRV
        Verbindungsstatus: Gültige Verbindung

        Knotenname: NODE1
        Dateibereichsname: \\nodel\c$
        FSID: 1
        Typ: SpMg
        Steuernde Replikationsregel: ALL_DATA
        Replikationsregelebene: Systemebene
        Servername: DRSRV
        Verbindungsstatus: Gültige Verbindung
```

Die Ausgabe wird für alle Datentypen angezeigt, unabhängig davon, ob ein Dateibereich die Datentypen enthält. Beispiel: Enthält ein Dateibereich nur Sicherungs- und Archivierungsdaten, enthält die Ausgabe des Befehls VALIDATE REPLICATION auch Informationen zu speicher verwalteten Daten.

## Feldbeschreibungen

---

**Knotenname**

Der Knoten, der der Eigner der replizierten Daten ist.

**Dateibereichsname**

Der Name des Dateibereichs, der zu dem Knoten gehört.

Dateibereichsnamen können eine andere Zeichenumsetzungstabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetzungstabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetzungstabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetzungstabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

**FSID**

Die Dateibereichs-ID des Dateibereichs. Der Server ordnet eine eindeutige FSID zu, wenn ein Dateibereich zum ersten Mal auf dem Server gespeichert wird.

**Typ**

Der Datentyp. Die folgenden Werte sind gültig:

Arch

Archivierungsdaten

Bkup

Sicherungsdaten

SpMg

Daten, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

#### Steuernde Replikationsregel

Der Name der Replikationsregel, die die Replikation für einen Datentyp in einem Dateibereich steuert. Um zu bestimmen, ob die Steuerungsregel eine Dateibereichsregel, eine Clientregel oder eine Serverregel ist, überprüfen Sie das Feld 'Replikationsregelebene'.

#### Replikationsregelebene

Die Ebene der Steuerungsregel in der Replikationsregelhierarchie. Die folgenden Werte sind gültig:

##### Dateibereich

Die Steuerungsregel ist einem Datentyp in dem Dateibereich zugeordnet.

##### Knoten

Die Steuerungsregel ist einem Datentyp für einen Clientknoten zugeordnet.

##### Server

Die Steuerungsregel ist einem Datentyp für alle Dateibereiche in allen Clientknoten zugeordnet, die für die Replikation konfiguriert sind.

#### Servername

Der Name des Zielreplikationsservers, der abgefragt werden soll.

#### Verbindungsstatus

Der Verbindungsstatus zwischen dem Quellen- und dem Zielreplikationsserver. Die folgenden Werte sind gültig:

##### Gültige Verbindung

Die Kommunikation mit dem Zielreplikationsserver war erfolgreich und der Zielreplikationsserver ist ein Server mit Version 6.3.

##### Zielserver nicht definiert

Der Zielreplikationsserver ist nicht definiert. Um den Zielreplikationsserver zu definieren, geben Sie den Befehl SET REPLSERVER aus.

##### Übertragungsfehler

Der Quellenreplikationsserver konnte den Zielreplikationsserver nicht ansprechen. Überprüfen Sie das Aktivitätenprotokoll auf Fehlernachrichten zur fehlgeschlagenen Übertragung. Ziehen Sie die folgenden möglichen Ursachen in Betracht:

- Die Replikationskonfiguration auf dem Quellenreplikationsserver ist nicht gültig. Einer oder mehrere der folgenden Fehler können vorhanden sein:
  - Die Serverdefinition für den Zielreplikationsserver ist nicht korrekt.
  - Wurde die Definition des Zielreplikationsservers gelöscht und erneut definiert, geben Sie den Befehl PING SERVER aus, um die Verbindung zwischen dem Quellen- und Zielreplikationsserver zu testen. Ist der Befehl PING SERVER erfolgreich, geben Sie den Befehl UPDATE SERVER aus und geben Sie FORCESYNC=YES an, um die Serverprüfchlüssel zurückzusetzen.
  - Der Servername, die Serveradresse der unteren Ebene, die Serveradresse der höheren Ebene und das Serverkennwort stimmen nicht mit den Werten überein, die in der Serverdefinition auf dem Zielreplikationsserver angegeben sind.
- Die Replikationskonfiguration auf dem Zielreplikationsserver ist nicht gültig. Einer oder mehrere der folgenden Fehler können vorhanden sein:
  - Die Version des Zielreplikationsservers ist eine Version vor Version 6.3.
  - Die Serverdefinition für den Quellenreplikationsserver ist nicht korrekt.
  - Der Servername, die Serveradresse der unteren Ebene, die Serveradresse der höheren Ebene und das Serverkennwort stimmen nicht mit den Werten überein, die in der Serverdefinition auf dem Quellenreplikationsserver angegeben sind.
- Die Netzkommunikation ist nicht verfügbar. Um die Verbindung zwischen dem Quellen- und Zielservers zu testen, geben Sie den Befehl PING SERVER aus.
- Der Zielreplikationsserver ist nicht verfügbar.
- Sitzungen zwischen dem Quellen- und Zielreplikationsserver sind inaktiviert. Um den Status der Sitzungen zu überprüfen, geben Sie den Befehl QUERY STATUS aus.

#### Replikation ausgesetzt

Die Replikationsverarbeitung wird ausgesetzt, wenn Sie die Datenbank auf dem Quellenreplikationsserver zurückschreiben oder die Replikationsverarbeitung auf diesem Server mit dem Befehl DISABLE REPLICATION inaktivieren.

## Zugehörige Befehle

---

Tabelle 1. Zugehörige Befehle für VALIDATE REPLICATION

| Befehl                | Beschreibung   |
|-----------------------|--|
| DISABLE REPLICATION   | Verhindert die Verarbeitung abgehender Replikation auf einem Server.   |
| ENABLE REPLICATION    | Ermöglicht die Verarbeitung abgehender Replikation auf einem Server.   |
| ENABLE SESSIONS       | Nimmt die Serveraktivität nach einem Befehl DISABLE oder ACCEPT DATE wieder auf.                                     |
| QUERY FILESPACE       | Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.                                      |
| QUERY NODE            | Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.                                    |
| QUERY REPLRULE        | Zeigt Informationen zu Knotenreplikationsregeln an.  |
| QUERY SERVER          | Zeigt Informationen über Server an.  |
| QUERY STATUS          | Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen. |
| REPLICATE NODE        | Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.   |
| SET ARREPLRULEDEFAULT | Gibt die Serverknotenreplikationsregel für Archivierungsdaten an.  |
| SET BKREPLRULEDEFAULT | Gibt die Serverknotenreplikationsregel für Sicherungsdaten an.   |
| SET REPLSERVER        | Gibt einen Zielreplikationsserver an.  |
| SET SPREPLRULEDEFAULT | Gibt die Serverknotenreplikationsregel für speicher verwaltete Daten an.   |
| UPDATE FILESPACE      | Ändert Knotenreplikationsregeln für Dateibereiche.   |
| UPDATE NODE           | Ändert die Attribute, die einem Clientknoten zugeordnet sind.  |
| UPDATE REPLRULE       | Aktiviert oder inaktiviert Replikationsregeln.   |
| UPDATE SERVER         | Aktualisiert Informationen über einen Server.  |

## VALIDATE REPLPOLICY (Die Maßnahmen auf dem Zielreplikationsserver prüfen)

Verwenden Sie diesen Befehl, um die Maßnahmen für Clientknoten auf dem Quellenreplikationsserver mit denselben Maßnahmen auf dem Zielreplikationsserver zu vergleichen, auf dem die Clientknotendaten repliziert werden.

Der Befehl zeigt die Unterschiede zwischen diesen Maßnahmen an. Sie können prüfen, ob die Unterschiede zwischen den Maßnahmen auf dem Quellen- und dem Zielreplikationsserver beabsichtigt sind, oder die Maßnahmen auf dem Zielreplikationsserver ändern.

Stellen Sie sicher, dass IBM Spectrum Protect Version 7.1.1 oder höher auf dem Quellen- und Zielreplikationsserver installiert ist, bevor Sie diesen Befehl ausgeben. Geben Sie diesen Befehl auf dem Quellenreplikationsserver aus.

### Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

### Syntax

```
>>-VALidate REPLPolicy--+-+-----+-----<<
                        '-Servername-'
```

### Parameter

Servername

Gibt den Namen des Zielreplikationsservers an, der über Maßnahmen verfügt, die geprüft werden sollen. Dieser Parameter ist wahlfrei. Wenn Sie diesen Parameter nicht angeben, definiert der Befehl den Standardreplikationsserver als Zielreplikationsserver.

## Beispiel: Die Unterschiede zwischen den Replikationsmaßnahmen auf einem Quellen- und Zielreplikationsserver anzeigen

Um die Unterschiede zwischen den Maßnahmen auf dem Quellenreplikationsserver und den Maßnahmen auf dem Zielreplikationsserver CVTCVS\_LXS\_SRV2 anzuzeigen, auf dem die Clientdaten repliziert werden, geben Sie den folgenden Befehl auf dem Quellenreplikationsserver aus:

```
VALIDATE REPLPOLICY CVTCVS_LXS_SRV2
```

| Name der Maßnahmendomäne auf diesem Server | Name der Maßnahmendomäne auf dem Zielserver | Name des Zielserver |
|--|---|---------------------|
| STANDARD                                   | STANDARD                                    | CVTCVS_LXS_SRV2     |
| Unterschiede in Maßnahmengruppe:           |   |                     |
| Änderung erkannt                           | Wert für Quellenserver                      | Wert für Zielserver |
| Verwaltungsklasse nur auf Ziel             | Nicht zutreffend                            | STANDARD2           |
| Verwaltungsklasse nur auf Quelle           | STANDARD1                                   | Nicht zutreffend    |
| Unterschiede in Sicherungskopiengruppe:    |   |                     |
| Änderung erkannt                           | STANDARD in Verwaltungsklasse               | STANDARD            |
|  | Wert für Quellenserver                      | Wert für Zielserver |
| Versionen bestehender Daten                | 2   | 20                  |
| Betroffene Knoten                          |   |                     |
| NODE1,NODE2,NODE3,NODE4,NODE5              |   |                     |

## Feldbeschreibungen

Name der Maßnahmendomäne auf diesem Server

Gibt den Namen der Maßnahmendomäne auf dem Quellenreplikationsserver an, auf dem der Befehl ausgegeben wird.

Name der Maßnahmendomäne auf dem Zielserver

Gibt den Namen der Maßnahmendomäne auf dem Zielreplikationsserver an.

Name des Zielserver

Gibt den Namen des Zielreplikationsservers an.

Unterschiede in Maßnahmengruppe:

Gibt die Unterschiede zwischen den Maßnahmen an, die auf dem Quellen- und dem Zielreplikationsserver definiert sind. Die Unterschiede zwischen den Maßnahmen werden unter den folgenden Feldern aufgelistet:

Änderung erkannt

Gibt die Liste der Maßnahmenelemente an, die auf dem Quellen- und dem Zielreplikationsserver unterschiedlich sind.

Wert für Quellenserver

Gibt den Wert für das Maßnahmenelement auf dem Quellenreplikationsserver an.

Wert für Zielserver

Gibt den Wert für das Maßnahmenelement auf dem Zielreplikationsserver an.

Unterschiede in Sicherungskopiengruppe <Name der Sicherungskopiengruppe> in Standardverwaltungsklasse ODER Unterschiede in Archivierungskopiengruppe <Name der Archivierungskopiengruppe> in Standardverwaltungsklasse

Gibt die Unterschiede zwischen den Sicherungskopiengruppen oder den Archivierungskopiengruppen in der Verwaltungsklasse an. Die Unterschiede werden unter den folgenden Feldern aufgelistet:

Änderung erkannt

Gibt die Liste der Kopiengruppenfelder an, die unterschiedlich sind.

Wert für Quellenserver

Gibt den Wert im Kopiengruppenfeld auf dem Quellenreplikationsserver an.

Wert für Zielserver

Gibt den Wert im Kopiengruppenfeld auf dem Zielreplikationsserver an.

Betroffene Knoten

Gibt die Namen aller Clientknoten an, die von den in dieser Ausgabe angezeigten Änderungen betroffen sind.

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für VALIDATE REPLPOLICY

| Befehl                 | Beschreibung  |
|------------------------|---|
| VALIDATE REPLICATION   | Überprüft die Replikation für Dateibereiche und Datentypen.                                   |
| QUERY REPLSERVER       | Zeigt Informationen zu Replikationsservern an.  |
| SET DISSIMILARPOLICIES | Aktiviert die Maßnahmen auf dem Zielreplikationsserver für die Verwaltung replizierter Daten. |
| QUERY DOMAIN           | Zeigt Informationen über Maßnahmendomänen an.   |
| QUERY POLICYSET        | Zeigt Informationen über Maßnahmengruppen an.   |
| QUERY COPYGROUP        | Zeigt die Attribute einer Kopiengruppe an.  |
| QUERY MGMTCLASS        | Zeigt Informationen zu Verwaltungsklassen an.   |

## VARY (Datenträger mit wahlfreiem Zugriff an-/abhängen)

Mit diesem Befehl kann ein Speicherpooldatenträger mit wahlfreiem Zugriff für den Server angehängt oder abgehängt werden.

### Berechtigungsklasse

Dieser Befehl ist nur für Datenträger in Einheiten mit wahlfreiem Zugriff gültig. Dieser Befehl kann beispielsweise während der Wartung eines Datenträgers mit wahlfreiem Zugriff oder bei der Fehlerberichtigung verwendet werden. Ein Datenträger mit wahlfreiem Zugriff, der als Unavailable (nicht verfügbar) definiert ist, kann nicht angehängt werden.

Für diesen Befehl ist die System- oder die Bedienerberechtigung erforderlich.

### Syntax

```
>>-VARY--+-ONline--+-Datenträgername--+-----+-----<<
      '-Offline-'          '-Wait-----+No--+'
                          '-Yes-'
```

### Parameter

#### ONline

Gibt an, daß der Server den Datenträger mit wahlfreiem Zugriff verwenden kann.

#### OFFline

Gibt an, daß der Server den Datenträger nicht verwenden kann.

#### Datenträgername (Erforderlich)

Gibt die Datenträger-ID an. Datenträgernamen dürfen keine eingebetteten Leerzeichen oder Gleichheitszeichen enthalten.

#### Wait




Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

#### No



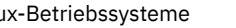

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet, während andere Tasks ausgeführt werden. Bei dem Hintergrundprozess erstellte Nachrichten werden vom Server entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

#### Yes

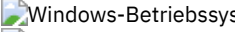

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Erst nachdem der Befehl vollständig ausgeführt wurde, kann mit anderen Aufgaben fortgefahren werden. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungs-Client an, wenn der Befehl beendet ist.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

## Beispiel: Einen Datenträger anhängen

  Den Datenträger /adsm/stgvol/1 für den Server als Speicherpool datenträger zur Verfügung stellen.  

```
vary online /adsm/stgvol/1
```

 Den Datenträger j:\storage\pool001 für den Server als Speicherpool datenträger zur Verfügung stellen. 

```
vary online j:\storage\pool001
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für VARY

| Befehl         | Beschreibung   |
|----------------|--|
| CANCEL PROCESS | Bricht einen Serverhintergrundprozess ab.  |
| DEFINE VOLUME  | Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll. |
| DELETE VOLUME  | Löscht einen Datenträger aus einem Speicherpool.   |
| QUERY PROCESS  | Zeigt Informationen über Hintergrundprozesse an.   |
| QUERY VOLUME   | Zeigt Informationen über Speicherpool datenträger an.  |

## Serveroptionen

Bei der Installation stellt IBM Spectrum Protect eine Serveroptionsdatei zur Verfügung, die eine Reihe von Standardoptionen zum Starten des Servers enthält.

Die Datei ist:

- dmserv.opt im Serverinstanzverzeichnis

Mit Serveroptionen kann Folgendes angepasst werden:

- Übertragung
- Serverspeicher
- Client/Server
- Datum, Nummer, Uhrzeit und Sprache
- Datenbank- und Wiederherstellungsprotokoll
- Datenübertragung
- Nachricht
- Ereignisprotokollierung
- Sicherheit und Lizenzierung


Einige andere Optionen sind für sonstige Zwecke verfügbar. Diese nicht dokumentierten Optionen sind nur für die Verwendung durch den IBM® Support bestimmt.

Sollen die aktuellen Optionseinstellungen angezeigt werden, Folgendes eingeben:

```
query option
```






- Serveroptionen ändern  
Bei der Serverinitialisierung liest der Server die Serveroptionsdatei. Wird eine Serveroption durch Editieren der Datei aktualisiert, muss der Server gestoppt und anschließend wieder gestartet werden, um die aktualisierte Serveroptionsdatei zu aktivieren.
- Arten von Serveroptionen  
Mit Serveroptionen können Sie die Arbeitsweise von einigen Funktionen und Prozessen anpassen.
- 3494SHARED  
Die Option 3494SHARED gibt an, ob ein Kassettenarchiv IBM 3494 andere Anwendungen als IBM Spectrum Protect gemeinsam benutzen kann.
- ACSACCESSID  
Die Option ACSACCESSID gibt die ID für die ACS-Zugriffssteuerung eines ACSLS-Kassettenarchivs an.
- ACSLOCKDRIVE  
Die Option ACSLOCKDRIVE gibt an, ob die Laufwerke in den ACSLS-Kassettenarchiven gesperrt sind. Durch das Sperren von Laufwerken wird die exklusive Benutzung der Laufwerke in dem ACSLS-Kassettenarchiv in einer gemeinsamen Umgebung sichergestellt. Die Leistung ist jedoch etwas besser, wenn Kassettenarchive nicht gesperrt werden. Wenn andere Anwendungen die IBM Spectrum Protect-Laufwerke nicht verwenden, ist das Sperren der Laufwerke nicht erforderlich.





















- **ACSQUICKINIT**  
Die Option ACSQUICKINIT gibt an, ob die Initialisierung des ACSLS-Kassettenarchivs beim Serverstart eine schnelle oder vollständige Initialisierung ist. Der Standardwert ist 'Yes'. Eine schnelle Initialisierung vermeidet den Aufwand, der mit der Synchronisation des Datenträgerbestands des IBM Spectrum Protect-Servers mit dem Datenträgerbestand des ACSLS-Kassettenarchivs verbunden ist (durch eine Prüfung des Kassettenarchivs).
- **ACSTIMEOUTX**  
Die Option ACSTIMEOUTX gibt das Vielfache des integrierten Zeitlimitwerts für ACSLS-APIs an. Der integrierte Zeitlimitwert für die ENTER-, EJECT- und AUDIT-ACS-API beträgt 1800 Sekunden; für alle anderen ACSLS-APIs beträgt der Wert 600 Sekunden. Lautet das angegebene Vielfache beispielsweise 5, beträgt der Zeitlimitwert für die Prüf-API 9000 Sekunden und für alle anderen APIs 3000 Sekunden.
- **ACTIVELOGDIRECTORY**  
Die Option ACTIVELOGDIRECTORY gibt den Namen des Verzeichnisses an, in dem alle aktiven Protokolldateien gespeichert werden.
- **ACTIVELOGSIZE**  
Die Option ACTIVELOGSIZE definiert die Gesamtgröße der Protokolldatei.
- **ADMINCOMMTIMEOUT**  
Die Option ADMINCOMMTIMEOUT gibt an, wie lange der Server während einer Operation, die eine Datenbankaktualisierung zur Folge hat, auf eine erwartete Verwaltungsclientnachricht wartet.
- **ADMINIDLETIMEOUT**  
Die Option ADMINIDLETIMEOUT gibt die Zeit in Minuten an, die eine Verwaltungsclientsitzung inaktiv sein kann, bevor der Server die Sitzung abbricht.
- **ADMINONCLIENTPORT**  
Die Option ADMINONCLIENTPORT gibt an, ob TCPPOINT von Verwaltungssitzungen verwendet werden kann. Der Standardwert ist YES.
-  **Windows-BetriebssystemeADSMGROUPNAME**  
Die Option ADSMGROUPNAME gibt den Namen einer Windows-Gruppe an. Ein Clientknoten muss Teil dieser Gruppe sein, um mit dem IBM Spectrum Protect-Server über NT Unified Logon arbeiten zu können. Der Clientknoten muss außerdem als IBM Spectrum Protect-Clientknoten registriert sein.
- **ALIASHALT**  
Die Option ALIASHALT ermöglicht es Administratoren, dem IBM Spectrum Protect-Befehl **HALT** einen anderen Namen zuzuordnen.
- **ALLOWDESAUTH**  
Die Option ALLOWDESAUTH gibt an, ob die Verwendung von Data Encryption Standard (DES) für die Authentifizierung zwischen einem Server und einem Client für Sichern/Archivieren zulässig ist.
- **ALLOWREORGINDEX**  
Die Option ALLOWREORGINDEX gibt an, ob die vom Server eingeleitete Indexreorganisation aktiviert oder inaktiviert ist.
- **ALLOWREORGTABLE**  
Die Option ALLOWREORGTABLE gibt an, ob die vom Server eingeleitete Tabellenreorganisation aktiviert oder inaktiviert ist.
- **ARCHFAILOVERLOGDIRECTORY**  
Die Option ARCHFAILOVERLOGDIRECTORY gibt das Verzeichnis an, das der Server zum Speichern der Archivprotokolldateien verwendet, die nicht im Verzeichnis für Archivprotokolle gespeichert werden können.
- **ARCHLOGCOMPRESS**  
Sie können die Komprimierung von Archivprotokollen auf dem IBM Spectrum Protect-Server aktivieren oder inaktivieren. Durch die Komprimierung der Archivprotokolle wird der Speicherbedarf reduziert, der für die Speicherung erforderlich ist.
- **ARCHLOGDIRECTORY**  
Die Option ARCHLOGDIRECTORY gibt ein Verzeichnis an, in dem der Datenbankmanager eine Protokolldatei archivieren kann, nachdem alle in dieser Protokolldatei angegebenen Transaktionen abgeschlossen wurden.
- **ARCHLOGUSEDTHRESHOLD**  
Die Option ARCHLOGUSEDTHRESHOLD gibt an, wann eine automatische Datenbanksicherung in Relation zum Prozentsatz des belegten Speicherbereichs für die Archivprotokolldatei gestartet werden soll. Der Standardwert ist 80 Prozent.
- **ASSISTVCRRECOVERY**  
Die Option ASSISTVCRRECOVERY gibt an, ob IBM Spectrum Protect ein Laufwerk IBM 3590 bei der Wiederherstellung nach verloren gegangenen oder beschädigten VCR (Vital Cartridge Records) unterstützt. Wird YES (Standardwert) angegeben und erkennt IBM Spectrum Protect während der Ladeverarbeitung einen Fehler, geht TSM während der Entladeverarbeitung an das Datenende, um den Laufwerken die Wiederherstellung der VCR zu ermöglichen. Während der Bandoperation kann dies geringe Auswirkungen auf die Leistung haben, da das Laufwerk keine schnelle Suche mit einem verloren gegangenen oder beschädigten VCR ausführen kann. Es tritt jedoch kein Datenverlust auf.
- **AUDITSTORAGE**  
Als Teil einer Lizenzprüfung berechnet der Server nach Knoten den Umfang des Serverspeichers, der für Sicherungsdateien, Archivierungsdateien und speicher verwaltete Dateien verwendet wird. Bei Servern, die umfangreiche Datenmengen verwalten, kann diese Berechnung sehr viel CPU-Zeit beanspruchen und andere Serveraktivitäten blockieren. Mit der Option AUDITSTORAGE kann angegeben werden, dass bei der Lizenzprüfung der Speicher nicht berechnet werden soll.
- **BACKUPINITIATIONROOT**  
Die Option BACKUPINITIATIONROOT gibt an, ob der Server Knotenparameterwerte für Benutzer überschreibt, die keine berechtigten IBM Spectrum Protect-Benutzer sind.


- CHECKTAPEPOS  
Die Option CHECKTAPEPOS gibt an, ob der IBM Spectrum Protect-Server die Position von Datenblöcken auf Band überprüft.
- CLIENTDEDUPTXNLIMIT  
Die Option CLIENTDEDUPTXNLIMIT gibt die maximale Größe einer Transaktion an, wenn vom Client deduplizierte Daten gesichert oder archiviert werden.
- CLIENTDEPLOYCATALOGURL  
Die Option CLIENTDEPLOYCATALOGURL gibt die Position der Katalogdatei an, die für automatische Clientimplementierungsoperationen verwendet wird.
- CLIENTDEPLOYUSELOCALCATALOG  
Die Option CLIENTDEPLOYCATALOGURL gibt an, ob die lokale Version der Katalogdatei für automatische Clientimplementierungsoperationen verwendet wird.
- COMMMETHOD  
Die Option COMMMETHOD gibt eine Übertragungsmethode an, die vom Server verwendet werden soll.
- COMMTIMEOUT  
Die Option COMMTIMEOUT gibt an, wie lange der Server während einer Operation, die eine Datenbankaktualisierung zur Folge hat, auf eine erwartete Clientnachricht wartet. Wenn die Zeitlänge dieses Zeitlimit überschreitet, beendet der Server die Sitzung mit dem Client. Sie können den Wert für das Zeitlimit erhöhen, damit keine Zeitlimitüberschreitung bei den Clients auftritt. Eine Zeitlimitüberschreitung kann bei Clients auftreten, wenn eine hohe Netzauslastung in Ihrer Umgebung vorhanden ist, oder wenn die Clients große Dateien sichern.
- CONTAINERRESOURCESTIMEOUT  
Die Option CONTAINERRESOURCESTIMEOUT gibt an, wie lange der Server auf die Ausführung einer Datenspeicheroperation für einen Containerspeicherpool wartet.
-  Windows-BetriebssystemeDATEFORMAT  
Die Option DATEFORMAT gibt das Format an, in dem Datumsangaben vom Server angezeigt werden.
- DBDIAGLOGSIZE  
Mit dieser Option können Sie die Größe des Speicherbereichs steuern, der von Diagnoseprotokolldateien verwendet wird.
- DBDIAGPATHFSTHRESHOLD  
Die Option DBDIAGPATHFSTHRESHOLD gibt den Schwellenwert für freien Speicherbereich in dem Dateisystem oder auf der Platte an, das bzw. die die Datei db2diag.log enthält.
- DBMEMPERCENT  
Verwenden Sie diese Option, um den Prozentsatz des virtuellen Adressraums anzugeben, der den Datenbankmanagerprozessen zugeordnet ist.
- DBMTCPPORT  
Die Option DBMTCPPORT gibt die Nummer des Anschlusses an, an dem der TCP/IP-DFV-Treiber für den Datenbankmanager auf Anforderungen für Clientsitzungen.
- DEDUPREQUIRESBACKUP  
Die Option DEDUPREQUIRESBACKUP gibt an, ob Datenträger in primären Speicherpools mit sequenziellem Zugriff, die für die Deduplizierung von Daten definiert sind, wiederhergestellt und doppelte Daten gelöscht werden können, bevor die Speicherpools gesichert werden.
- DEDUPTIER2FILESIZE  
Die Option DEDUPTIER2FILESIZE gibt an, bei welcher Dateigröße IBM Spectrum Protect beginnt, die Schicht 2 der Dateneduplizierung zu verwenden.
- DEDUPTIER3FILESIZE  
Die Option DEDUPTIER3FILESIZE gibt an, bei welcher Dateigröße IBM Spectrum Protect beginnt, die Schicht 3 der Dateneduplizierung zu verwenden.
- DEVCONFIG  
Die Option DEVCONFIG gibt den Namen einer Datei an, in der IBM Spectrum Protect eine Sicherungskopie der Einheitenkonfigurationsinformationen speichern soll.
- DISABLEREORGTABLE  
Die Option DISABLEREORGTABLE gibt an, ob die Onlinetabellenreorganisation für Tabellennamen inaktiviert wird, die in der Tabellenliste angegeben sind.
- DISABLESCHEDS  
Die Option DISABLESCHEDS gibt an, ob Verwaltungszeitpläne und Clientzeitpläne während der Wiederherstellung des IBM Spectrum Protect-Servers inaktiviert sind.
- DISPLAYLFINFO  
Die Option DISPLAYLFINFO gibt an, wie die Abrechnungssätze und Einträge in der Übersichtstabelle den Knotennamen angeben.
- DNSLOOKUP  
Die Option DNSLOOKUP gibt an, ob der Server System-API-Aufrufe verwendet, um die DNS-Namen (DNS = Domain Name Server) von Systemen zu bestimmen, die den Server ansprechen.
- DRIVEACQUIRERETRY  
Mit der Option DRIVEACQUIRERETRY kann angegeben werden, wie oft der Server versuchen soll, ein Laufwerk in einem Kassettenarchiv IBM 349x anzufordern. Wird das Kassettenarchiv von mehreren Anwendungen gemeinsam benutzt, scheinen seine Laufwerke für den Server verfügbar zu sein (durch die Verwendung eines Sendeaufrufprozesses im Hintergrund), obwohl sie es nicht sind.

- **ENABLENASDEDUP**  
Die Serveroption ENABLENASDEDUP gibt an, ob der Server Daten dedupliziert, die von einem NAS-Dateiserver gespeichert werden. Diese Option gilt nur für NetApp-Dateiserver.
- **EVENTSERVER**  
Die Option EVENTSERVER gibt an, ob der Server beim Systemstart eine Verbindung zum Ereignisserver herstellen soll.
- **EXPINTERVAL**  
Die Option EXPINTERVAL gibt das Intervall (in Stunden) an, in dem automatische Bestandsverfallsprozesse in IBM Spectrum Protect stattfinden. Beim Datenträgerbestandsverfall werden Clientsicherungs- und Archivierungsdateikopien aus dem Server gelöscht, und zwar wie von den Verwaltungsklassen angegeben, denen die Clientdateien zugeordnet sind. Findet nicht regelmäßig ein Datenträgerverfall statt, wird kein Speicherpoolbereich von abgelaufenen Clientdateien zurückgefordert, so dass für den Server mehr Speicherbereich benötigt wird, als für die Maßnahme eigentlich nötig wäre.
- **EXPQUIET**  
Die Option EXPQUIET gibt an, ob IBM Spectrum Protect detaillierte Nachrichten während der Verfallsverarbeitung sendet.
-   **FASPBEGPORT**  
Die Option FASPBEGPORT gibt die Anfangsnummer des Bereichs von Anschlussnummern an, die für die Netzkommunikation mit der Aspera FASP-Technologie (Fast Adaptive Secure Protocol) verwendet werden.
-   **FASPENDPORT**  
Die Option FASPENDPORT gibt die Endnummer des Bereichs von Anschlussnummern an, die für die Netzkommunikation mit der Aspera FASP-Technologie (Fast Adaptive Secure Protocol) verwendet werden.
-   **FASPTARGETRATE**  
Die Option FASPTARGETRATE gibt die Zielgeschwindigkeit für die Datenübertragung mit der Aspera FASP-Technologie (Fast Adaptive Secure Protocol) an. Mit der Angabe der Zielgeschwindigkeit begrenzen Sie die Bandbreite jeder Netzverbindung, die die Aspera FASP-Technologie verwendet. Auf diese Weise können Sie sicherstellen, dass genügend Bandbreite für alle Netzverbindungen verfügbar ist.
- **FFDCLOGLEVEL**  
Die Option FFDCLOGLEVEL gibt den Typ von allgemeinen Servernachrichten an, die im FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) angezeigt werden.
- **FFDCLOGNAME**  
Die Option FFDCLOGNAME gibt einen Namen für das FFDC-Protokoll (FFDC = First-Failure Data Capture) an.
- **FFDCMAXLOGSIZE**  
Die Option FFDCMAXLOGSIZE gibt die Größe für die FFDC-Protokolldatei (FFDC = First-Failure Data Capture) an.
- **FFDCNUMLOGS**  
Die Option FFDCNUMLOGS gibt die Anzahl der Protokolldateien an, die für die Umlaufprotokollierung verwendet werden können. Der Standardwert ist 10.
- **FILEEXIT**  
Die Option FILEEXIT gibt eine Datei an, an die aktivierte Ereignisse weitergeleitet werden. Jedes protokollierte Ereignis ist ein Satz in der Datei.
- **FILETEXTEXIT**  
Die Option FILETEXTEXIT gibt eine Datei an, an die aktivierte Ereignisse weitergeleitet werden. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.
- **FSUSEDTHRESHOLD**  
Die Option FSUSEDTHRESHOLD gibt den Prozentsatz des Dateisystems an, der von der Datenbank ausgefüllt werden kann, bevor eine Alertnachricht ausgegeben wird.
- **IDLETIMEOUT**  
Die Option IDLETIMEOUT gibt die Zeit in Minuten an, die eine Clientsitzung inaktiv sein kann, bevor der Server die Sitzung abbricht. Sie können den Wert für das Zeitlimit erhöhen, damit bei hoher Netzauslastung in Ihrer Umgebung keine Zeitlimitüberschreitung bei den Clients auftritt. Beachten Sie jedoch, dass bei einer großen Anzahl von inaktiven Sitzungen andere Benutzer möglicherweise keine Verbindung zu dem Server herstellen können.
- **KEEPALIVE**  
Die Option KEEPALIVE gibt an, ob die TCP-Keepalive-Funktion (TCP = Transmission Control Protocol) für abgehende TCP-Sockets aktiviert ist. Die TCP-Keepalive-Funktion sendet eine Übertragung von einer Einheit zu einer anderen Einheit, um zu überprüfen, ob die Verbindung zwischen den beiden Einheiten betriebsbereit ist.
- **KEEPALIVETIME**  
Die Option KEEPALIVETIME gibt an, wie oft TCP eine Keepalive-Übertragung sendet, wenn eine Antwort empfangen wird. Diese Option gilt nur, wenn die Option KEEPALIVE auf YES gesetzt wurde.
- **KEEPALIVEINTERVAL**  
Die Option KEEPALIVEINTERVAL gibt an, wie oft eine Keepalive-Übertragung gesendet wird, wenn keine Antwort empfangen wird. Diese Option gilt nur, wenn die Option KEEPALIVE auf YES gesetzt wurde.
- **LANGUAGE**  
Die Option LANGUAGE steuert die Initialisierung von länderspezifischen Angaben. Die länderspezifischen Angaben enthalten unter anderem die Landessprache sowie die Datums-, Uhrzeit- und Zahlenformate, die für die Konsole und den Server verwendet werden sollen.
- **LDAPCACHEDURATION**  
Die Option LDAPCACHEDURATION bestimmt die Zeit, die der IBM Spectrum Protect-Server Informationen zur LDAP-Kennwortauthentifizierung zwischenspeichert.

- LDAPURL  
Die Option LDAPURL gibt die Position Ihres Lightweight Directory Access Protocol-Servers (LDAP-Servers) an. Definieren Sie die Option LDAPURL nach der Konfiguration des LDAP-Servers.
- MAXSESSIONS  
Die Option MAXSESSIONS gibt die maximal zulässige Anzahl gleichzeitig stattfindender Clientsitzungen für den Server an.
- MESSAGEFORMAT  
Die Option MESSAGEFORMAT gibt an, ob eine Nachrichtennummer in allen Zeilen angezeigt wird, wenn sich die Nachricht über mehrere Zeilen erstreckt.
- MIRRORLOGDIRECTORY  
Die Option MIRRORLOGDIRECTORY gibt das Verzeichnis zum Spiegeln des Pfads für aktive Protokolldateien an.
- MOVEBATCHSIZE  
Die Option MOVEBATCHSIZE gibt die Anzahl Clientdateien an, die innerhalb derselben Servertransaktion als Stapel gruppiert und versetzt werden sollen. Dieses Versetzen von Daten resultiert aus Speicherpoolsicherungen und -zurückschreibungen, Umlagerungsoperationen, Wiederherstellungsoperationen und MOVE DATA-Operationen. Diese Option arbeitet zusammen mit der Option MOVESIZETHRESH.
- MOVESIZETHRESH  
Die Option MOVESIZETHRESH gibt den Grenzwert für die Datenmenge an (in Megabyte), die innerhalb derselben Servertransaktion als Stapel versetzt werden soll. Wenn diese Schwelle erreicht ist, werden dem aktuellen Stapel keine weiteren Dateien hinzugefügt. Nachdem der aktuelle Stapel versetzt wurde, wird eine neue Transaktion gestartet.
- MSGINTERVAL  
Die Option MSGINTERVAL gibt die Zeit in Minuten zwischen Nachrichten an, in denen ein Bediener zum Einlegen eines Bands für den Server aufgefordert wird.
-  Windows-Betriebssysteme NAMEDPIPENAME  
Die Option NAMEDPIPENAME gibt eine Übertragungsmethode an, mit der Prozesse miteinander kommunizieren können, ohne wissen zu müssen, wo sich die Sende- und Empfangsprozesse befinden. Der Name fungiert als Aliasname und verbindet die beiden Prozesse unabhängig davon, ob sie sich auf demselben Rechner oder in verbundenen Domänen befinden.
- NDMPCONNECTIONTIMEOUT  
Die Serveroption NDMPCONNECTIONTIMEOUT gibt die Zeit in Stunden an, die der IBM Spectrum Protect-Server auf den Empfang von Statusaktualisierungen während der Ausführung von NDMP-Zurückschreibungsoperationen über das LAN wartet. NDMP-Zurückschreibungsoperationen mit großen NAS-Dateisystemen können einen langen Inaktivitätszeitraum aufweisen. Der Standardwert ist 6 Stunden.
- NDMPCONTROLPORT  
Die Option NDMPCONTROLPORT gibt die Anschlussnummer an, die für interne Übertragungen für bestimmte NDMP-Operationen (NDMP = Network Data Management Protocol) verwendet werden soll. Der IBM Spectrum Protect-Server arbeitet nicht als allgemeiner NDMP-Bandserver.
- NDMPENABLEKEEPALIVE  
Die Serveroption NDMPENABLEKEEPALIVE gibt an, ob der IBM Spectrum Protect-Server TCP-Keepalive (TCP = Transmission Control Protocol) für NDMP-Steuerverbindungen (NDMP = Network Data Management Protocol) zu NAS-Einheiten (NAS = Network-attached Storage) aktiviert. Der Standardwert ist NO.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme NDMPKEEPIDLEMINUTES  
Die Serveroption NDMPKEEPIDLEMINUTES gibt die Zeit in Minuten an, bevor das Betriebssystem das erste TCP-Keepalive-Paket (TCP = Transmission Control Protocol) für eine NDMP-Steuerverbindung (NDMP = Network Data Management Protocol) überträgt. Der Standardwert ist 120 Minuten.
- NDMPPORTRANGE  
Die Option NDMPPORTRANGE gibt den Bereich der Anschlussnummern an, in dem IBM Spectrum Protect navigiert, um eine Anschlussnummer zum Akzeptieren einer Sitzung von einer NAS-Einheit für die Datenübertragung zu erhalten. Der Standardwert 0,0 bedeutet, dass IBM Spectrum Protect einen Anschluss vom Betriebssystem zur Verfügung stellen lässt (ephemerer Anschluss).
- NDMPREFDATAINTERFACE  
Diese Option gibt die IP-Adresse an, die der Schnittstelle zugeordnet ist, in der der Server alle NDMP-Sicherungsdaten (NDMP = Network Data Management Protocol) empfangen soll.
- NOPREEMPT  
Der Server ermöglicht bestimmten Operationen das Zugriffsvorrecht für Datenträger und Einheiten. Durch Angabe von NOPREEMPT kann das Zugriffsvorrecht inaktiviert werden. In diesem Fall hat dann keine Operation das Zugriffsvorrecht auf einen Datenträger und lediglich einer Datenbanksicherungsoperation kann das Zugriffsvorrecht für eine Einheit vor einer anderen Operation eingeräumt werden.
- NORETRIEVEDATE  
Die Option NORETRIEVEDATE gibt an, dass der Server das Abrufdatum einer Datei in einem Plattenspeicherpool nicht aktualisiert, wenn ein Client die Datei zurückschreibt oder abrufft. Diese Option und der Speicherpoolparameter MIGDELAY steuern, wann der Server Dateien umgelagert.
-  Windows-Betriebssysteme NPAUDITFAILURE  
Die Option NPAUDITFAILURE gibt an, ob ein Ereignis an das Ereignisprotokoll gesendet wird, wenn ein Knoten sich bei dem Server anmeldet und dabei einen Namen verwendet, der sich zwar in der Windows-Gruppe befindet, aber nicht mit dem Windows-Kontoanmeldenamen übereinstimmt. Um sicherzustellen, dass ein Knoten nur auf seine eigenen Daten zugreifen kann, müssen der Knotenname und der Windows-Kontoanmeldenamen übereinstimmen.

-  Windows-BetriebssystemeNPAUDITSUCCESS  
Die Option NPAUDITSUCCESS gibt an, dass ein Ereignis an das Ereignisprotokoll gesendet wird, wenn für einen Clientknotenbenutzer über SECUREPIPE eine Identifikationsprüfung durchgeführt wird, bevor er auf den Server zugreifen kann.
-  Windows-BetriebssystemeNPBUFFERSIZE  
Die Option NPBUFFERSIZE gibt die Größe des Kommunikationspuffers für benannte Pipes an.
-  Windows-BetriebssystemeNUMBERFORMAT  
Die Option NUMBERFORMAT gibt das Format an, in dem der Server Zahlen anzeigt.
- NUMOPENVOLSALLOWED  
Die Option NUMOPENVOLSALLOWED gibt die Anzahl der FILE-Eingabedatenträger in einem deduplizierten Speicherpool an, die gleichzeitig geöffnet sein können.
- PUSHSTATUS  
Die Option PUSHSTATUS wird auf Peripherieservern verwendet, um sicherzustellen, dass Statusinformationen an den Hub-Server gesendet werden. Aktualisieren Sie diese Option nur, wenn Sie die Konfiguration des Operations Center im vorkonfigurierten Zustand zurückschreiben müssen, in dem die IBM Spectrum Protect-Server nicht als Hub-Server oder Peripherieserver definiert sind.
- QUERYAUTH  
Die Option QUERYAUTH gibt die Administratorberechtigungsstufe an, die für die Ausgabe des Befehls QUERY oder SQL SELECT erforderlich ist. Standardmäßig kann jeder Administrator die Befehle QUERY und SELECT ausgeben. Mit dieser Option kann die Verwendung dieser Befehle eingeschränkt werden.
- RECLAIMDELAY  
Mit dieser Option wird die Wiederherstellung eines SnapLock-Datenträgers verzögert. Damit wird es ermöglicht, dass verbleibende Daten verfallen können, so dass keine Notwendigkeit zur Wiederherstellung des Datenträgers besteht.
- RECLAIMPERIOD  
Mit dieser Option können Sie die Anzahl der Tage für den Wiederherstellungszeitraum eines SnapLock-Datenträgers definieren.
- REORGBEGINTIME  
Die Option REORGBEGINTIME gibt die früheste Zeit an, zu der der IBM Spectrum Protect-Server eine Tabellen- oder Indexreorganisation starten kann.
- REORGDURATION  
Die Option REORGDURATION gibt ein Intervall an, in dem die vom Server eingeleitete Tabellen- oder Indexreorganisation gestartet werden kann.
- REPORTRETRIEVE  
Die Option REPORTRETRIEVE erstellt Berichte zu Zurückschreibungs- oder Abrufoperationen, die von Clientknoten oder Administratoren ausgeführt werden. Der Standardwert ist NO.
- REPLBATCHSIZE  
Die Option REPLBATCHSIZE gibt die Anzahl Clientdateien an, die innerhalb derselben Servertransaktion als Stapel repliziert werden sollen. Diese Option betrifft nur die Knotenreplikationsprozesse und arbeitet mit der Option REPLSIZETHRESH, um die Knotenreplikationsverarbeitung zu verbessern.
- REPLSIZETHRESH  
Die Option REPLSIZETHRESH gibt einen Schwellenwert (in Megabyte) für das replizierte Datenvolumen innerhalb derselben Servertransaktion an.
- REQSYSAUTHOUTFILE  
Die Option REQSYSAUTHOUTFILE gibt an, ob die Systemberechtigung für Verwaltungsbefehle erforderlich ist, die IBM Spectrum Protect veranlassen, in eine externe Datei zu schreiben.
- RESOURCETIMEOUT  
Die Option RESOURCETIMEOUT gibt an, wie lange der Server auf eine Ressource wartet, bevor die anstehende Anforderung einer Ressource abgebrochen wird. Tritt eine Zeitlimitüberschreitung auf, wird die Anforderung der Ressource abgebrochen.
- RESTHTTPSPORT  
Die Option RESTHTTPSPORT gibt die Anschlussnummer an, die für die HTTPS-Kommunikation (HTTPS = Hypertext Transfer Protocol Secure) zwischen dem Operations Center und dem Hub-Server verwendet werden soll.
- RESTOREINTERVAL  
Die Option RESTOREINTERVAL gibt an, wie lange eine wiederanlauffähige Zurückschreibungssitzung in der Serverdatenbank gesichert werden kann. Solange die Zurückschreibungssitzung in der Datenbank gesichert ist, kann sie ab dem Punkt, an dem sie gestoppt wurde, erneut gestartet werden.
- RETENTIONEXTENSION  
Die Option RETENTIONEXTENSION gibt die Anzahl der Tage an, um die das Ende des Aufbewahrungszeitraums eines SnapLock-Datenträgers erweitert werden soll. Mit dieser Option kann der Server das Ende des Aufbewahrungszeitraums eines SnapLock-Datenträgers erweitern, um eine übermäßige Wiederherstellung zu vermeiden.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-BetriebssystemeSANDISCOVERY  
Die Option SANDISCOVERY gibt an, ob die SAN-Erkennungsfunktion von IBM Spectrum Protect aktiviert ist.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-BetriebssystemeSANDISCOVERYTIMEOUT  
Die Option SANDISCOVERYTIMEOUT gibt die Zeit an, die für die Antwort von Hostbusadaptern zulässig ist, wenn sie von dem SAN-Erkennungsprozess abgefragt werden. Sobald die für SANDISCOVERYTIMEOUT angegebene Zeit erreicht wird, tritt bei dem Prozess eine Zeitlimitüberschreitung auf.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-BetriebssystemeSANREFRESHTIME  
Die Option SANREFRESHTIME gibt die Zeit an, die vergeht, bevor die zwischengespeicherten SAN-Erkennungsinformationen

- aktualisiert werden. Die Option SANREFRESHTIME hat den Standardwert 0, der angibt, dass kein SAN-Erkennungscache vorhanden ist. Bei jeder Ausführung einer SAN-Erkennungsoperation durch den Server werden die Informationen direkt von dem Hostbusadapter abgerufen.
- SEARCHMPQUEUE  
Die Option SEARCHMPQUEUE gibt die Reihenfolge an, in der der Server Anforderungen in der Ladewarteschlange ausführt. Wird die Option angegeben, versucht der Server zuerst, Anforderungen für Datenträger auszuführen, die bereits geladen sind. Diese Anforderungen können vor anderen Anforderungen ausgeführt werden, auch wenn die anderen Anforderungen schon länger auf den Mountpunkt warten. Wird diese Option nicht angegeben, führt der Server Anforderungen in der Reihenfolge aus, in der sie empfangen werden.
  -  Windows-Betriebssysteme SECUREPIPES  
Bei Verwendung des Protokolls mit benannten Pipes führt das Aktivieren von SECUREPIPES dazu, dass der Server die über ADSMGROUPNAME angegebene Windows-Gruppe prüft, um einen Clientknoten/Benutzer zu authentifizieren.
  - SERVERDEDUPTXNLIMIT  
Die Option SERVERDEDUPTXNLIMIT gibt die maximale Größe von Objekten an, die auf dem Server dedupliziert werden können.
  - SHMPORT  
 AIX-Betriebssysteme  Linux-Betriebssysteme Die Option SHMPORT gibt die TCP/IP-Anschlussadresse eines Servers bei Verwendung von gemeinsam benutztem Speicher an. Jede Übertragung mit gemeinsam benutztem Speicher beginnt mit einer TCP/IP-Verbindung.  Windows-Betriebssysteme Die Option SHMPORT gibt den Anschluss an, an dem der Server für Verbindungen mit gemeinsam genutztem Speicher empfangsbereit ist.
  - SHREDDING  
Die Option SHREDDING gibt an, ob das Schreddern von gelöschten sensiblen Daten automatisch oder manuell ausgeführt wird. Das Schreddern gilt nur für Daten in Speicherpools, die explizit für die Unterstützung des Schredderns konfiguriert wurden.
  - SNMPHEARTBEATINTERVAL  
Die Option SNMPHEARTBEATINTERVAL gibt das Intervall zwischen den Abfragen des IBM Spectrum Protect-Servers in Minuten an.
  - SNMPPMESSAGECATEGORY  
Die Option SNMPPMESSAGECATEGORY gibt die Abfangarten an, die verwendet werden, wenn Nachrichten des Servers über den SNMP-Subagenten (SNMP = Simple Network Management Protocol) an den SNMP-Manager weitergeleitet werden.
  - SNMPSUBAGENT  
Die Option SNMPSUBAGENT gibt die Parameter an, die erforderlich sind, damit der IBM Spectrum Protect-Subagent mit dem SNMP-Dämon (SNMP = Simple Network Management Protocol) kommunizieren kann. Diese Option betrifft nur das Konfigurieren des SNMP-Subagenten, damit dieser mit dem SNMP-Agenten kommunizieren kann; die Option wird vom Server ignoriert.
  - SNMPSUBAGENTHOST  
Die Option SNMPSUBAGENTHOST gibt den Standort des IBM Spectrum Protect SNMP-Subagenten (SNMP = Simple Network Management Protocol) an. Der Standardwert für diese Option lautet 127.0.0.1.
  - SNMPSUBAGENTPORT  
Die Option SNMPSUBAGENTPORT gibt die Anschlussnummer des IBM Spectrum Protect SNMP-Subagenten (SNMP = Simple Network Management Protocol) an.
  - SSLFIPSMODE  
Die Option SSLFIPSMODE gibt an, ob der FIPS-Modus (Federal Information Processing Standards) für Secure Sockets Layer (SSL) aktiv ist. Der Standardwert ist NO.
  - SSLINITTIMEOUT  
Die Option SSLINITTIMEOUT gibt die Zeit in Minuten an, die der Server darauf wartet, dass eine SSL-Sitzung (SSL = Secure Sockets Layer) die Initialisierung beendet, bevor der Server die Sitzung abbricht.
  - SSLTCPADMINPORT  
Die Option SSLTCPADMINPORT gibt die Anschlussadresse an, an der der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen nur für SSL-aktivierte Sitzungen wartet. Die Sitzungen gelten für den Verwaltungsbefehlszeilenclient.
  - SSLTCPPOINT  
Die Option SSLTCPPOINT gibt die SSL-Anschlussnummer (SSL = Secure Sockets Layer) nur für SSL-fähige Sitzungen an. Der TCP/IP-Kommunikationstreiber des Servers wartet an diesem Anschluss auf Anforderungen für SSL-aktivierte Sitzungen vom Client.
  - TCPADMINPORT  
Die Option TCPADMINPORT gibt die Nummer des Anschlusses an, an dem der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen für andere TCP/IP-Sitzungen und SSL-fähige Sitzungen als Clientsitzungen wartet. Dazu gehören Verwaltungssitzungen, Sitzungen zwischen Servern, Speicheragentensitzungen, Speicherarchivclientsitzungen, Sitzungen verwalteter Server und Ereignisserversitzungen.
  -  AIX-Betriebssysteme  Linux-Betriebssysteme TCPBUFSIZE  
Die Option TCPBUFSIZE gibt die Größe des Puffers an, der für TCP/IP-Sendeanforderungen verwendet wird. Während einer Zurückschreibung werden Clientdaten aus der IBM Spectrum Protect-Sitzungskomponente in einen TCP-DFV-Treiber versetzt. Die Option TCPBUFSIZE bestimmt, ob der Server die Daten direkt aus dem Sitzungspuffer sendet oder die Daten in den TCP-Puffer kopiert. Eine Puffergröße von 32 KB zwingt den Server dazu, Daten in den Kommunikationspuffer zu kopieren und den Inhalt des Puffers zu löschen, wenn er gefüllt ist.
  - TCPNODELAY  
Die Option TCPNODELAY gibt an, ob der Server die Verzögerung beim Senden von aufeinanderfolgenden kleinen Paketen im Netz inaktiviert.

- **TCPPORT**  
Die Option TCPPORT gibt die Nummer des Anschlusses an, an dem der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen für Clientsitzungen wartet. Der TCP/IP-Kommunikationstreiber des Servers ist an diesem Anschluss sowohl für TCP/IP-Sitzungen als auch für SSL-fähige Sitzungen vom Client empfangsbereit.
- **TCPWINDOWSIZE**  
Die Option TCPWINDOWSIZE gibt den Umfang (in Kilobyte) der Empfangsdaten an, die bei einer TCP/IP-Verbindung gleichzeitig gepuffert werden können. Der sendende Host kann erst dann weitere Daten senden, wenn er eine Bestätigung und eine Aktualisierung des TCP-Empfangsfensters empfängt. Jedes TCP-Paket enthält das entsprechende TCP-Empfangsfenster in der Verbindung. Bei einem größeren Fenster kann der Sender mit dem Senden von Daten fortfahren. Außerdem wird möglicherweise die Übertragungsleistung verbessert, besonders in schnellen Netzen mit hoher Latenzzeit.
- **TECBEGINEVENTLOGGING**  
Die Option TECBEGINEVENTLOGGING gibt an, ob die Ereignisprotokollierung für den TIVOLI-Empfänger beim Serverstart beginnen soll. Wird die Option TECHOST angegeben, wird für TECBEGINEVENTLOGGING standardmäßig der Wert YES angenommen.
- **TECHOST**  
Die Option TECHOST gibt den Hostnamen oder die IP-Adresse für den Tivoli-Ereignisserver an.
- **TECPORT**  
Die Option TECPORT gibt die TCP/IP-Anschlussadresse an, an der der Tivoli-Ereignisserver empfangsbereit ist. Diese Option ist nur erforderlich, wenn sich der Tivoli-Ereignisserver auf einem System befindet, auf dem der Service 'Port Mapper' nicht ausgeführt wird.
- **TECUTF8EVENT**  
Die Option TECUTF8EVENT ermöglicht es dem IBM Spectrum Protect-Administrator, Informationen im UTF-8-Datenformat an den Tivoli Enterprise Console (TEC)-Server zu senden. Der Standardwert ist 'No'. Mit dem Befehl QUERY OPTION können Sie abfragen, ob diese Option aktiviert ist.
- **THROUGHPUTDATATHRESHOLD**  
Die Option THROUGHPUTDATATHRESHOLD gibt eine Durchsatzschwelle an, die eine Clientsitzung erreichen muss, damit sie nicht abgebrochen wird, wenn die Zeitschwelle erreicht wird.
- **THROUGHPUTTIMETHRESHOLD**  
Die Option THROUGHPUTTIMETHRESHOLD gibt die Zeitschwelle für eine Sitzung an, nach deren Ablauf die Sitzung aufgrund zu geringen Durchsatzes abgebrochen werden kann.
-  **Windows-BetriebssystemeTIMEFORMAT**  
Die Option TIMEFORMAT gibt das Format an, in dem Uhrzeitangaben vom Server angezeigt werden.
- **TXNGROUPMAX**  
Die Option TXNGROUPMAX gibt die Anzahl der Objekte an, die als Gruppe zwischen einem Client und dem Server zwischen Transaktions-COMMIT-Punkten übertragen werden. Der Mindestwert beträgt 4 Objekte und der Maximalwert beträgt 65000 Objekte. Der Standardwert ist 4096 Objekte. Bei den übertragenen Objekten handelt es sich um tatsächliche Dateien, Verzeichnisse oder beides. Der Server zählt jede Datei oder jedes Verzeichnis als ein Objekt.
- **UNIQUEDPTEEVENTS**  
Die Option UNIQUEDPTEEVENTS generiert eine eindeutige Tivoli Enterprise Console (TEC)-Ereignisklasse für jede einzelne IBM Spectrum Protect-Nachricht, einschließlich Client-, Server- und IBM Spectrum Protect Data Protection-Clientnachrichten. Der Standardwert ist 'No'.
- **UNIQUETEEVENTS**  
Die Option UNIQUETEEVENTS generiert eine eindeutige Tivoli Enterprise Console (TEC)-Ereignisklasse für jede einzelne IBM Spectrum Protect-Nachricht. Der Standardwert ist 'No'.
- **USEREXIT**  
Die Option USEREXIT gibt einen benutzerdefinierten Ausgang an, dem die Steuerung für die Verwaltung eines Ereignisses übergeben wird.
- **VERBCHECK**  
Die Option VERBCHECK gibt an, dass der Server eine zusätzliche Fehlerprüfung für die Struktur der Befehle durchführt, die vom Client gesendet werden. Diese Option sollte nur aktiviert werden, wenn der Client nicht ordnungsgemäß gebildete Anforderungen an den Server sendet, die zum Absturz des Servers führen. Ist diese Option aktiviert, hat dies einen Protokollfehler an Stelle eines Serverabsturzes zur Folge.
- **VOLUMEHISTORY**  
Die Option VOLUMEHISTORY gibt den Namen von Dateien an, die automatisch aktualisiert werden sollen, wenn History-Informationen von sequenziellen Datenträgern des Servers sich ändern. Für diese Option gibt es keinen Standardwert.

## Serveroptionen ändern



---

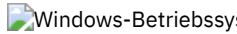
Bei der Serverinitialisierung liest der Server die Serveroptionsdatei. Wird eine Serveroption durch Editieren der Datei aktualisiert, muss der Server gestoppt und anschließend wieder gestartet werden, um die aktualisierte Serveroptionsdatei zu aktivieren.

## Informationen zu diesem Vorgang

---

Einige Optionen können dynamisch mit dem Befehl SETOPT geändert werden, ohne dass der Server gestoppt und gestartet werden muss. Für ausführliche Informationen siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

  Die Datei dmserv.opt.smp (wird ebenfalls bei der Installation zur Verfügung gestellt) enthält das Format der Optionsdatei und alle Standardeinstellungen. Alle Optionen in der Datei dmserv.opt.smp können geändert werden. Soll der Server die geänderten Optionen verwenden, müssen Sie die Datei in dmserv.opt umbenennen. Zum Aktivieren einer Option in der Serveroptionsdatei ist das der Option vorausgehende \*>>> zu entfernen. Der Server ignoriert alle Optionen, denen \*>>> vorausgeht.

 Sie können Serveroptionen ändern, indem Sie den Optionsdateieditor verwenden, der in der IBM Spectrum Protect-Konsole enthalten ist. Mit diesem Editor werden Kommunikationsparameter erkannt und Werte auf ihre Gültigkeit hin überprüft, und er bietet Hilfe für alle Optionen. Das Arbeiten mit dem Optionsdateieditor stellt die bevorzugte Methode für das Ändern von Serveroptionen dar, aber es kann auch mit einem Texteditor gearbeitet werden.

## Arten von Serveroptionen

Mit Serveroptionen können Sie die Arbeitsweise von einigen Funktionen und Prozessen anpassen.

- **Serverübertragungsoptionen**  
Sie können Serveroptionen verwenden, um Serverübertragungsmethoden und ihre Kenndaten anzugeben.
- **Optionen für den Serverspeicher**  
IBM Spectrum Protect stellt eine Reihe von Optionen bereit, mit denen Sie bestimmte Operationen für Einheiten und Serverspeicher konfigurieren können.
- **Client/Server-Optionen**  
Sie können Serveroptionen verwenden, um die Client/Server-Verarbeitung zu steuern.
- **Optionen für Datum, Zahlen, Uhrzeit und Sprache**  
Sie können Serveroptionen verwenden, um Anzeigeformate für Datums-, Uhrzeit- und Zahlenangaben sowie für die Landessprache anzugeben.
- **Datenbankoptionen**  
Mit Serveroptionen können Sie bestimmte Aspekte bei der Datenbankverarbeitung steuern.
- **Datenübertragungsoptionen**  
Mit Serveroptionen können Sie steuern, wie IBM Spectrum Protect Daten gruppiert und überträgt.
- **Nachrichtenoptionen**  
Mit Serveroptionen lässt sich die Nachrichtenausgabe in IBM Spectrum Protect flexibler gestalten.
- **Optionen für die Aufzeichnung des Ereignisprotokolls**  
Optionen können bei der Verwaltung von Ereignisprotokollempfängern helfen.
- **Optionen für Sicherheit und Lizenzierung**  
Sie können Serveroptionen verwenden, um Serversicherheits- und -lizenzprüfungen anzupassen.
- **Weitere Optionen**  
Sie können eine Vielzahl anderer Serveroptionen verwenden, um IBM Spectrum Protect anzupassen.





## Serverübertragungsoptionen


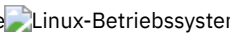


Sie können Serveroptionen verwenden, um Serverübertragungsmethoden und ihre Kenndaten anzugeben.

Tabelle 1. Übertragungsoptionen

| Option            | Beschreibung   |
|-------------------|--|
| ADMINCOMMTIMEOUT  | Die Zeit, die der Server während einer Operation, die eine Datenbankaktualisierung zur Folge hat, auf eine Verwaltungsclientnachricht wartet |
| ADMINIDLETIMEOUT  | Die Zeit, die eine Verwaltungsclientsitzung inaktiv sein kann  |
| ADMINONCLIENTPORT | Der Anschluss, der bestimmt, ob Verwaltungssitzungen den in der Option TCPPORT angegebenen Anschluss verwenden können                        |
| COMMMETHOD        | Übertragungsmethode des Servers  |



| Option   | Beschreibung  |
|--|---|
| DBMTCPPORT   | Die Nummer des Anschlusses, an dem der TCP/IP-DFV-Treiber für den Datenbankmanager auf Anforderungen für Clientsitzungen wartet   |
| DNSLOOKUP  | Steuerung der Verwendung von Domännennamenservices (Domain Name Services = DNS) zum Suchen der Namen der Systeme, die den Server ansprechen   |
| LDAPCACHEDURATION  | Bestimmt die Dauer, die Authentifizierungssitzungen für denselben Knoten oder Administrator übersprungen werden. Möglicherweise stellen Sie eine geringe Leistungsverbesserung fest, wenn Sitzungen übersprungen werden.  |
| LDAPURL  | Gibt den LDAP-Verzeichnisserver an. Jede Einstellung muss den Namen des LDAP-Verzeichnisseservers, eine Anschlussnummer und den Basis-DN des Namensbereichs (oder Suffix) enthalten, den der Server verwaltet.  |
|  Windows-Betriebssysteme NAMEDPIPENAME  |  Windows-Betriebssysteme Übertragungsmethode mit benannten Pipes   |
| NDMPCONTROLPORT  | Der interne Übertragungsanschluss, der für bestimmte NDMP-Operationen (NDMP = Network Data Management Protocol) verwendet wird  |
| NDMPENABLEKEEPALIVE  | Der TCP-Keepalive-Mechanismus   |
|  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme<br>NDMPKEEPIDLEMINUTES |  AIX-Betriebssysteme<br> Linux-Betriebssysteme<br> Windows-Betriebssysteme Die Leerlaufzeit, bevor das erste TCP-Keepalive-Paket gesendet wird   |
|  Windows-Betriebssysteme NPBUFFERSIZE   |  Windows-Betriebssysteme Die Größe des Kommunikationspuffers für benannte Pipes  |
| SHMPORT  |  AIX-Betriebssysteme<br> Linux-Betriebssysteme Die TCP/IP-Anschlussadresse eines Servers bei Verwendung von gemeinsam genutztem Speicher<br><br> Windows-Betriebssysteme Der Anschluss, an dem der Server für Verbindungen mit gemeinsam genutztem Speicher empfangsbereit ist |
| SNMPHEARTBEATINTERVAL  | Intervall in Minuten zwischen den Abfragen des IBM Spectrum Protect-Servers   |
| SNMPMESSAGECATEGORY  | Die beim Weiterleiten von Nachrichten von dem Server verwendeten Abfangarten  |
| SNMPSUBAGENT   | Die Parameter, die erforderlich sind, damit der IBM Spectrum Protect-Subagent mit dem SNMP-Dämon kommunizieren kann   |
| SNMPSUBAGENTHOST   | Der Standort des IBM Spectrum Protect SNMP-Subagenten   |
| SNMPSUBAGENTPORT   | Die Anschlussadresse des IBM Spectrum Protect SNMP-Subagenten   |



















| Option   | Beschreibung  |
|--|---|
| SSLFIPSMODE  | Gibt an, ob der FIPS-Modus (Federal Information Processing Standards) für Secure Sockets Layer (SSL) aktiv ist  |
| SSLTCPADMINPORT  | Die Anschlussadresse, an der der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen für SSL-aktivierte Sitzungen für den Verwaltungsbefehlszeilenclient wartet  |
| SSLTCPPOINT  | Die SSL-Anschlussnummer, an der der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen für SSL-aktivierte Sitzungen aus den folgenden Quellen wartet: <ul style="list-style-type: none"> <li>• Befehlszeilenclient für Sichern/Archivieren</li> <li>• GUI des Clients für Sichern/Archivieren</li> <li>• Verwaltungsclient</li> <li>• Anwendungsprogrammierschnittstelle (API)</li> </ul> |
| TCPADMINPORT   | Die TCP/IP-Anschlussnummer für Verwaltungssitzungen   |
|   TCPBUFSIZE |   Die Größe des Puffers, der für TCP/IP-Sendeanforderungen verwendet wird   |
| TCPPOINT   | Die TCP/IP-Anschlussnummer für Clientsitzungen  |
| TCPWINDOWSIZE  | Das TCP/IP-Schiebefenster des Clientknotens   |

## Optionen für den Serverspeicher

IBM Spectrum Protect stellt eine Reihe von Optionen bereit, mit denen Sie bestimmte Operationen für Einheiten und Serverspeicher konfigurieren können.

Tabelle 1. Optionen für den Serverspeicher

| Option              | Beschreibung  |
|---------------------|---|
| 3494SHARED          | Ermöglicht die gemeinsame Nutzung eines Speicherarchivs 3494 mit anderen Anwendungen als IBM Spectrum Protect.  |
| ACSACCESSID         | Die ID für die ACS-Zugriffssteuerung.   |
| ACSLOCKDRIVE        | Ermöglicht das Sperren der Laufwerke in den ACSLS-Speicherarchiven.   |
| ACSQUICKINIT        | Ermöglicht eine schnelle oder vollständige Initialisierung des ACSLS-Speicherarchivs.   |
| ACSTIMEOUTX         | Das Vielfache des integrierten Zeitlimitwerts für die ACSLS-API.  |
| ASSISTVCRRECOVERY   | Gibt an, ob der Server ein Laufwerk IBM 3590 bei der Wiederherstellung nach verloren gegangenen oder beschädigten VCR (Vital Cartridge Records) unterstützt.  |
| CHECKTAPEPOS        | Gibt an, ob der Server die Datenposition auf Band überprüft.  |
| CLIENTDEDUPTXNLIMIT | Gibt die maximale Größe einer Transaktion an, wenn clientseitig deduplizierte Daten gesichert oder archiviert werden.   |
| DEDUPREQUIRESBACKUP | Gibt an, ob Datenträger in primären Speicherpools mit sequenziellem Zugriff, die für die Dateneduplizierung definiert sind, wiederhergestellt werden können und ob doppelte Daten gelöscht werden können, bevor die Speicherpools gesichert werden. |

| Option  | Beschreibung   |
|---|--|
| DEDUPTIER2FILESIZE  | Dateigröße, bei der die Schicht 2-Verarbeitung für die Dateneduplizierung verwendet wird.  |
| DEDUPTIER3FILESIZE  | Dateigröße, bei der die Schicht 3-Verarbeitung für die Dateneduplizierung verwendet wird.  |
| DEVCONFIG   | Der Name der Datei, in der Sicherungskopien der Einheitenkonfigurationsinformationen gespeichert werden.   |
| DRIVEACQUIRERETRY   | Gibt an, wie oft der Server versucht, ein Laufwerk in einem Speicherarchiv IBM 349x anzufordern, das von mehreren Anwendungen gemeinsam genutzt wird.  |
| ENABLENASDEDUP  | Gibt an, ob der Server Daten dedupliziert, die von einem NetApp NAS-Dateiserver gespeichert werden   |
| NUMOPENVOLSALLOWED  | Die Anzahl der FILE-Eingabedatenträger in einem deduplizierten Speicherpool, die gleichzeitig geöffnet sein können.  |
| RECLAIMDELAY  | Die Anzahl der Tage, um die die Wiederherstellung eines SnapLock-Datenträgers verzögert wird.  |
| RECLAIMPERIOD   | Die Anzahl der Tage für den Wiederherstellungszeitraum eines SnapLock-Datenträgers   |
| RESOURCE TIMEOUT  | Angabe, wie lange der Server auf eine Ressource wartet, bevor die anstehende Anforderung der Ressource abgebrochen wird.   |
| RETENTIONEXTENSION  | Die Anzahl der Tage, um die das Ende des Aufbewahrungszeitraums eines SnapLock-Datenträgers verlängert werden soll.  |
|  AIX-Betriebssysteme<br> Linux-Betriebssysteme<br> Windows-Betriebssysteme<br>SANDISCOVERY             |  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme<br>Angabe, ob die IBM Spectrum Protect-SAN-Erkennungsfunktion aktiviert ist.                   |
|  AIX-Betriebssysteme<br> Linux-Betriebssysteme<br> Windows-Betriebssysteme<br>SANDISCOVERYTIMEOUT |  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme<br>Die Zeit, bevor bei dem SAN-Erkennungsprozess eine Zeitlimitüberschreitung auftritt.     |
|  AIX-Betriebssysteme<br> Linux-Betriebssysteme<br> Windows-Betriebssysteme<br>SANREFRESHTIME     |  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme<br>Die Zeit, bevor zwischengespeicherte SAN-Erkennungsinformationen aktualisiert werden. |
| SEARCHMPQUEUE   | Die Reihenfolge, in der der Server Anforderungen in der Ladewarteschlange ausführt.  |
| SERVERDEDUPTXNLIMIT   | Gibt die maximale Größe von Objekten an, die auf dem Server dedupliziert werden können   |

## Client/Server-Optionen

Sie können Serveroptionen verwenden, um die Client/Server-Verarbeitung zu steuern.

Tabelle 1. Client/Server-Optionen







| Option                  | Beschreibung   |
|-------------------------|--|
| COMMTIMEOUT             | Die Anzahl Sekunden, die der Server auf eine Antwort von einem Client wartet, bevor die Clientsitzung wegen Zeitüberschreitung beendet wird. |
| DISABLESCHEDS           | Angabe, ob Verwaltungszeitpläne und Clientzeitpläne während der Wiederherstellung des IBM Spectrum Protect-Servers inaktiviert werden        |
| IDLETIMEOUT             | Die Anzahl Minuten, die eine Clientsitzung inaktiv sein darf, bevor der Server die Clientsitzung wegen Zeitüberschreitung beendet.           |
| MAXSESSIONS             | Die maximal zulässige Anzahl gleichzeitig stattfindender Clientsitzungen für den Server.   |
| THROUGHPUTDATATHRESHOLD | Die Durchsatzschwelle, die eine Clientsitzung erreichen muss, damit sie nicht abgebrochen wird, wenn die Zeitschwelle erreicht wird          |
| THROUGHPUTTIMETHRESHOLD | Die Zeitschwelle für eine Sitzung, nach deren Ablauf die Sitzung aufgrund zu geringen Durchsatzes abgebrochen werden kann                    |

| Option    | Beschreibung  |
|-----------|---|
| VERBCHECK | Angabe, ob eine zusätzliche Fehlerprüfung für Befehle erfolgt, die vom Client gesendet werden |

## Optionen für Datum, Zahlen, Uhrzeit und Sprache

Sie können Serveroptionen verwenden, um Anzeigeformate für Datums-, Uhrzeit- und Zahlenangaben sowie für die Landessprache anzugeben.

Tabelle 1. Optionen für Datum, Zahlen, Uhrzeit und Sprache

| Option  | Beschreibung  |
|---|---|
|  Windows-BetriebssystemeDATEFORMAT       |  Windows-BetriebssystemeDas Anzeigeformat für Datumsangaben  |
| LANGUAGE  | Clientnachrichten werden in der Landessprache angezeigt.  |
|  Windows-Betriebssysteme<br>NUMBERFORMAT |  Windows-BetriebssystemeDas Anzeigeformat für Zahlen         |
|  Windows-BetriebssystemeTIMEFORMAT       |  Windows-BetriebssystemeDas Anzeigeformat für Uhrzeitangaben |

## Datenbankoptionen

Mit Serveroptionen können Sie bestimmte Aspekte bei der Datenbankverarbeitung steuern.

Tabelle 1. Datenbankoptionen

| Option                   | Beschreibung  |
|--------------------------|---|
| ACTIVELOGDIRECTORY       | Das neue Verzeichnis für die Position, an der die aktive Protokolldatei gespeichert wird. Verwenden Sie diese Option, um die Position der aktiven Protokolldatei zu ändern. |
| ACTIVELOGSIZE            | Die maximale Größe der aktiven Protokolldatei.  |
| ALLOWREORGINDEX          | Vom Server eingeleitete Indexreorganisation.  |
| ALLOWREORGTABLE          | Vom Server eingeleitete Tabellenreorganisation.   |
| ARCHLOGDIRECTORY         | Das Verzeichnis, in dem der Datenbankmanager eine Protokolldatei archivieren kann, nachdem alle in dieser Protokolldatei angegebenen Transaktionen abgeschlossen wurden.    |
| ARCHFAILOVERLOGDIRECTORY | Das Verzeichnis, in dem der Server Archivprotokolldateien speichert, die nicht im Verzeichnis für Archivprotokolle gespeichert werden können.                               |
| DBDIAGLOGSIZE            | Die maximale Größe der Diagnoseprotokolldateien des Datenbankmanagers.  |
| DBDIAGPATHFSTHRESHOLD    | Der Schwellenwert für freien Speicherbereich in dem Dateisystem oder auf der Platte, das bzw. die die Diagnoseprotokolldateien des Datenbankmanagers enthält.               |
| DBMEMPERCENT             | Der Prozentsatz des Systemspeichers, der der Datenbank zugeordnet ist.  |
| DISABLEREORGTABLE        | Inaktivierung der Tabellenreorganisation für bestimmte Tabellen.  |
| FSUSEDTHRESHOLD          | Der Prozentsatz des Dateisystems, der von der Datenbank verwendet werden kann, bevor eine Alernachricht ausgegeben wird.  |
| MIRRORLOGDIRECTORY       | Das Verzeichnis zum Spiegeln des Pfads für aktive Protokolldateien.   |
| REORGBEGINTIME           | Die früheste Zeit, zu der der IBM Spectrum Protect-Server eine Tabellen- oder Indexreorganisation starten kann.   |
| REORGDURATION            | Das Intervall, in dem eine vom Server eingeleitete Tabellen- oder Indexreorganisation starten kann.   |

## Datenübertragungsoptionen

Mit Serveroptionen können Sie steuern, wie IBM Spectrum Protect Daten gruppiert und überträgt.

Tabelle 1. Gruppenoptionen

| Option               | Beschreibung   |
|----------------------|--|
| MOVEBATCHSIZE        | Die Anzahl Dateien, die innerhalb einer Transaktion als Stapel gruppiert und versetzt werden sollen.   |
| MOVESIZETHRESH       | Gibt den Grenzwert für die innerhalb einer Transaktion als Stapel zu versetzende Datenmenge an.  |
| NDMPPORTRANGE        | Die IP-Adresse, die der Schnittstelle zugeordnet ist, in der der Server alle NDMP-Sicherungsdaten (NDMP = Network Data Management Protocol) empfängt |
| NDMPREFDATAINTERFACE | Die IP-Adresse, die der Schnittstelle zugeordnet ist, in der der Server alle NDMP-Sicherungsdaten (NDMP = Network Data Management Protocol) empfängt |
| REPLBATCHSIZE        | Die Anzahl Dateien, die innerhalb derselben Servertransaktion als Stapel repliziert werden sollen.   |
| REPLSIZETHRESH       | Gibt den Grenzwert für die innerhalb derselben Servertransaktion als Stapel zu replizierende Datenmenge an.  |
| TXNGROUPMAX          | Die Anzahl Dateien, die als Gruppe zwischen einem Client und dem Server zwischen Transaktions-COMMIT-Punkten übertragen werden.                      |

## Nachrichtenoptionen

Mit Serveroptionen lässt sich die Nachrichtenausgabe in IBM Spectrum Protect flexibler gestalten.

Tabelle 1. Nachrichtenoptionen

| Option        | Beschreibung  |
|---------------|---|
| EXPQUIET      | Angabe, ob IBM Spectrum Protect detaillierte Informationsnachrichten während der Verfallsverarbeitung sendet                        |
| MESSAGEFORMAT | Angabe, ob eine Nachrichtennummer in allen Zeilen angezeigt wird, wenn sich die Nachricht über mehrere Zeilen erstreckt             |
| MSGINTERVAL   | Die Zeit in Minuten zwischen Nachrichten, in denen ein Bediener zum Einlegen eines Bands für IBM Spectrum Protect aufgefordert wird |

## Optionen für die Aufzeichnung des Ereignisprotokolls

Optionen können bei der Verwaltung von Ereignisprotokollempfängern helfen.

Tabelle 1. Optionen für die Aufzeichnung des Ereignisprotokolls









| Option               | Beschreibung   |
|----------------------|--|
| EVENTSERVER          | Angabe, ob der Server beim Serverstart eine Verbindung zum Ereignisserver herstellen soll.   |
| FILEEXIT             | Eine Datei, an die aktivierte Ereignisse weitergeleitet werden (binäres Format)  |
| FILETEXTIT           | Eine Datei, an die aktivierte Ereignisse weitergeleitet werden (lesbares Format)   |
| REPORTRETRIEVE       | Zeichnet Clientzurückschreibungs- und -abrufoperationen auf  |
| TECBEGINEVENTLOGGING | Angabe, ob die Ereignisprotokollierung für den TIVOLI-Empfänger beim Serverstart beginnen soll.  |
| TECHOST              | Der Hostname oder die IP-Adresse für den Tivoli Enterprise Console-Ereignisserver (TEC-Ereignisserver)   |
| TECPORT              | Die TCP/IP-Anschlussadresse, an der der Tivoli Enterprise Console-Ereignisserver empfangsbereit ist  |
| TECUTF8EVENT         | Ein Tivoli Enterprise Console-Ereignis, das vom IBM Spectrum Protect-Server im UTF8-Format gesendet wurde  |
| UNIQUEDPTEEVENTS     | Ereignisse von einem IBM Spectrum Protect Data Protection-Client, die als eindeutige Ereignisse an die Tivoli Enterprise Console gesendet werden |
| UNIQUETECEVENTS      | Ereignisse, die als eindeutige Ereignisse an die Tivoli Enterprise Console gesendet werden   |

| Option   | Beschreibung  |
|----------|---|
| USEREXIT | Ein benutzerdefinierter Exit, dem die Steuerung für die Verwaltung eines Ereignisses übergeben wird |

## Optionen für Sicherheit und Lizenzierung

Sie können Serveroptionen verwenden, um Serversicherheits- und -lizenzprüfungen anzupassen.

Tabelle 1. Optionen für Sicherheit und Lizenzierung

| Option  | Beschreibung  |
|---|---|
|  Windows-Betriebssysteme<br>ADSMGROUPNAME  |  Windows-Betriebssysteme<br>Der Name einer Windows-Gruppe  |
| AUDITSTORAGE  | Gibt an, dass der Server als Teil einer Lizenzprüfung den Umfang des belegten Sicherungs-, Archivierungs- und Speicherverwaltungsspeichers nach Knoten berechnet  |
| BACKUPINITIATIONROOT  | Gibt an, ob der Server Knotenparameterwerte für Benutzer überschreibt, die keine berechtigten IBM Spectrum Protect-Benutzer sind.   |
| LDAPURL   | Gibt den LDAP-Verzeichnisserver an. Jede Einstellung muss den Namen des LDAP-Verzeichnisservers, eine Anschlussnummer und den Basis-DN des Namensbereichs (oder Suffix) enthalten, den der Server verwaltet.  |
|  Windows-Betriebssysteme<br>NPAUDITFAILURE |  Windows-Betriebssysteme<br>Gibt an, dass ein Knoten nur auf seine eigenen Daten zugreifen kann  |
|  Windows-Betriebssysteme<br>NPAUDITSUCCESS |  Windows-Betriebssysteme<br>Gibt an, dass ein Ereignis an das Ereignisprotokoll gesendet wird, wenn für einen Clientknotenbenutzer über SECUREPIPE eine Identifikationsprüfung durchgeführt wird, bevor er auf den Server zugreifen kann |
| QUERYAUTH   | Die Administratorberechtigungsstufe, die für die Ausgabe des Befehls QUERY oder SQL SELECT erforderlich ist   |
| REQSYSAUTHOUTFILE   | Gibt an, ob die Systemberechtigung für Verwaltungsbefehle erforderlich ist, die IBM Spectrum Protect veranlassen, in eine externe Datei zu schreiben  |
|  Windows-Betriebssysteme<br>SECUREPIPES  |  Windows-Betriebssysteme<br>Gibt bei Verwendung des Protokolls für benannte Pipes an, dass der Server die Windows-Gruppe überprüft, um einen Client zu authentifizieren  |
| SHREDDING   | Gibt an, ob das Schreddern von gelöschten sensiblen Daten automatisch oder manuell ausgeführt wird  |

### Zugehörige Verweise:

Serverübertragungsoptionen

## Weitere Optionen

Sie können eine Vielzahl anderer Serveroptionen verwenden, um IBM Spectrum Protect anzupassen.

Tabelle 1. Weitere Optionen

| Option         | Beschreibung  |
|----------------|---|
| ALIASHALT      | Ermöglicht es Administratoren, dem IBM Spectrum Protect-Befehl HALT einen anderen Namen zuzuordnen  |
| DISPLAYLFINFO  | Gibt an, ob Abrechnungssätze und Einträge in der Übersichtstabelle den Speicheragentennamen angeben |
| EXPINTERVAL    | Das Intervall zwischen automatischen Datenträgerbestandsverfallsprozessen.                          |
| FFDCLOGNAME    | Der Name für das FFDC-Protokoll (FFDC = First-Failure Data Capture)                                 |
| FFDCMAXLOGSIZE | Die maximale Größe des FFDC-Protokolls (FFDC = First-Failure Data Capture)                          |

| Option          | Beschreibung  |
|-----------------|---|
| NOPREEMPT       | Gibt an, dass keine Operation das Zugriffsvorrecht auf einen Datenträger besitzen soll. Lediglich einer Datenbanksicherungsoperation kann das Zugriffsvorrecht vor einer anderen Operation eingeräumt werden. |
| NORETRIEVEDATE  | Gibt an, dass der Server das Abrufdatum einer Datei in einem Plattenspeicherpool nicht aktualisiert, wenn ein Client die Datei zurückschreibt oder abrufft  |
| RESTOREINTERVAL | Gibt an, wie lange eine wiederanlauffähige Zurückschreibungssitzung in der Serverdatenbank gesichert werden kann  |
| VOLUMEHISTORY   | Der Name der Datei, die automatisch aktualisiert werden soll, wenn sich History-Informationen von sequenziellen Datenträgern des Servers ändern   |

## 3494SHARED

Die Option 3494SHARED gibt an, ob ein Kassettenarchiv IBM® 3494 andere Anwendungen als IBM Spectrum Protect gemeinsam benutzen kann.

Der Standardwert lautet NO. Dieser Standardwert bedeutet, dass keine andere Anwendung als IBM Spectrum Protect das 3494-Kassettenarchiv verwenden kann. Wird diese Option auf YES gesetzt, bestimmt IBM Spectrum Protect für jede Ladeanforderung, ob alle Laufwerke in Gebrauch sind. Nach Beendigung der Abfrage wählt IBM Spectrum Protect ein verfügbares Laufwerk aus, das nicht von einer anderen Anwendung verwendet wird. Die gemeinsame Benutzung sollte nur aktiviert werden, wenn mehr als zwei Laufwerke in dem Kassettenarchiv vorhanden sind. Wird gerade ein Kassettenarchiv IBM 3494 mit anderen Anwendungen gemeinsam benutzt, muss diese Option angegeben werden.

### Syntax

```
>>-3494SHARED--+-Yes-+-----<<
                '-No--'
```

### Parameter

Yes

Gibt an, dass andere Anwendungen das 3494-Kassettenarchiv verwenden können.

No

Gibt an, dass keine anderen Anwendungen das 3494-Kassettenarchiv verwenden können.

### Beispiele

Die gemeinsame Benutzung eines 3494-Kassettenarchivs aktivieren:

```
3494shared yes
```

## ACSACCESSID

Die Option ACSACCESSID gibt die ID für die ACS-Zugriffssteuerung eines ACSLS-Kassettenarchivs an.

### Syntax

```
>>-ACSACCESSID--Name-----<<
```

### Parameter

## Name

Gibt eine ID an, die aus 1 bis 64 Zeichen besteht. Die Standard-ID ist der Name des lokalen Hosts.

## Beispiele

---

```
acsaccessid region
```

## ACSLOCKDRIVE

---

Die Option ACSLOCKDRIVE gibt an, ob die Laufwerke in den ACSLS-Kassettenarchiven gesperrt sind. Durch das Sperren von Laufwerken wird die exklusive Benutzung der Laufwerke in dem ACSLS-Kassettenarchiv in einer gemeinsamen Umgebung sichergestellt. Die Leistung ist jedoch etwas besser, wenn Kassettenarchive nicht gesperrt werden. Wenn andere Anwendungen die IBM Spectrum Protect-Laufwerke nicht verwenden, ist das Sperren der Laufwerke nicht erforderlich.

## Syntax

---

```
>>-ACSLOCKDRIVE---+-Yes+-----><  
                '-No--'
```

## Parameter

---

### Yes

Gibt an, dass die Laufwerke gesperrt sind.

### No

Gibt an, dass die Laufwerke nicht gesperrt sind.

## Beispiele

---

```
acslockdrive yes
```

## ACSQUICKINIT

---

Die Option ACSQUICKINIT gibt an, ob die Initialisierung des ACSLS-Kassettenarchivs beim Serverstart eine schnelle oder vollständige Initialisierung ist. Der Standardwert ist 'Yes'. Eine schnelle Initialisierung vermeidet den Aufwand, der mit der Synchronisation des Datenträgerbestands des IBM Spectrum Protect-Servers mit dem Datenträgerbestand des ACSLS-Kassettenarchivs verbunden ist (durch eine Prüfung des Kassettenarchivs).

## Syntax

---

```
>>-ACSQUICKINIT---+-Yes+-----><  
                '-No--'
```

## Parameter

---

### Yes

Gibt an, dass eine schnelle Initialisierung des ACSLS-Kassettenarchivs ausgeführt wird. Wird die Option auf Yes gesetzt, übergeht IBM Spectrum Protect die Überprüfung des Datenträgerbestands im Kassettenarchiv. Das Kassettenarchiv wird schnell initialisiert und IBM Spectrum Protect schneller zur Verfügung gestellt als bei einer vollständigen Initialisierung.

Diese Option sollte auf Yes gesetzt werden, wenn bekannt ist, dass sich der Datenträgerbestand des physischen Kassettenarchivs und der Datenträgerbestand im IBM Spectrum Protect-Kassettenarchiv nicht geändert haben und eine Prüfung nicht erforderlich ist.

### No

Gibt an, dass eine vollständige Initialisierung des ACSLS-Kassettenarchivs und des Datenträgerbestands im Kassettenarchiv ausgeführt wird. Wird die Option auf No gesetzt, synchronisiert IBM Spectrum Protect seinen Datenträgerbestand im Kassettenarchiv mit dem Bestand, der vom ACSLS-Kassettenarchivmanager zurückgemeldet wird.

## Beispiele

---



## ACSTIMEOUTX

---

Die Option ACSTIMEOUTX gibt das Vielfache des integrierten Zeitlimitwerts für ACSLS-APIs an. Der integrierte Zeitlimitwert für die ENTER-, EJECT- und AUDIT-ACS-API beträgt 1800 Sekunden; für alle anderen ACSLS-APIs beträgt der Wert 600 Sekunden. Lautet das angegebene Vielfache beispielsweise 5, beträgt der Zeitlimitwert für die Prüf-API 9000 Sekunden und für alle anderen APIs 3000 Sekunden.

### Syntax

---

```
>>-ACSTIMEOUTX--Wert-----<<
```

### Parameter

---

#### Wert

Gibt das Vielfache des integrierten Zeitlimitwerts für die ACSLS-API an. Der Bereich liegt zwischen 1 und 100. Der Standardwert ist 1.

### Beispiele

---

```
acstimeoutx 1
```

## ACTIVELOGDIRECTORY

---

Die Option ACTIVELOGDIRECTORY gibt den Namen des Verzeichnisses an, in dem alle aktiven Protokolldateien gespeichert werden.

Diese Option wird an die Optionsdatei angehängt, wenn der Befehl DSMSEV FORMAT ausgeführt wird. Unter normalen Betriebsbedingungen muss die Option nicht geändert werden. In DSMSEV FORMAT (Datenbank und Protokoll formatieren) befinden sich Anleitungen zur Verwendung dieser Option.

### Syntax

---

```
>>-ACTIVELOGDirectory--Verzeichnisname-----<<
```

### Parameter

---

#### Verzeichnisname

Gibt einen vollständig qualifizierten Verzeichnisnamen an. Das Verzeichnis muss vorhanden sein, es muss leer sein, und auf das Verzeichnis muss durch die Benutzer-ID des Datenbankmanagers zugegriffen werden können. Wird das Verzeichnis für aktive Protokolldateien geändert, versetzt IBM Spectrum Protect die vorhandenen aktiven Protokolldateien an die Position, die durch dieses Verzeichnis angegeben ist. Die maximale Anzahl Zeichen beträgt 175.

### Beispiele

---

```
activelogdirectory /tsm/activelogdir
```



```
activelogdirectory c:\tsmserv1\activelogdir
```

## ACTIVELOGSIZE

---

Die Option ACTIVELOGSIZE definiert die Gesamtgröße der Protokolldatei.

Diese Option wird an die Optionsdatei angehängt, wenn der Befehl DSMSEV FORMAT ausgeführt wird. Unter normalen Betriebsbedingungen muss die Option nicht geändert werden. In DSMSEV FORMAT (Datenbank und Protokoll formatieren) befinden sich Anleitungen zur Verwendung dieser Option.

## Syntax

---

```
                .-16GB-----.  
>>-ACTIVELOGSize--+-Megabyte-+-----<<
```

## Parameter

---

### Megabyte

Gibt die Größe der aktiven Protokolldatei in Megabyte an. Der Mindestwert ist 2048 MB (2 GB); der Maximalwert ist 524.288 MB (512 GB). Wenn eine ungerade Zahl angegeben wird, wird der Wert auf die nächste gerade Zahl aufgerundet. Der Standardwert ist 16.384 MB (16 GB).

Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option ACTIVELOGSIZE. Richtlinien für den Speicherbedarf befinden sich in der folgenden Tabelle:

Tabelle 1. Schätzung des Datenträger- und Dateispeicherbedarfs

| Wert der Option ACTIVELOGSize | Reservieren Sie diesen freien Speicherbereich im Verzeichnis für aktive Protokolldateien, zusätzlich zum Speicherbereich von ACTIVELOGSize |
|-------------------------------|--|
| 16 GB - 128 GB                | 5120 MB  |
| 129 GB - 256 GB               | 10240 MB   |
| 257 GB - 512 GB               | 20480 MB   |

## Beispiele

---

```
activelogsiz 8192
```

## ADMINCOMMTIMEOUT

---

Die Option ADMINCOMMTIMEOUT gibt an, wie lange der Server während einer Operation, die eine Datenbankaktualisierung zur Folge hat, auf eine erwartete Verwaltungsclientnachricht wartet.

Wenn die Zeitlänge dieses Zeitlimit überschreitet, beendet der Server die Sitzung mit dem Verwaltungsclient. Sie können den Wert für das Zeitlimit erhöhen, um zu verhindern, dass bei Verwaltungsclientsitzungen eine Zeitlimitüberschreitung auftritt.

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

## Syntax

---

```
                .-60-----.  
>>-ADMINCOMMTIMEout--+-Sekunden-+-----<<
```

## Parameter

---

### Sekunden

Gibt die maximale Anzahl Sekunden an, die ein Server auf eine Antwort des Verwaltungsclients wartet. Der Standardwert ist 60. Der Mindestwert ist 1.

## Beispiele

---

```
admincommtimeout 60
```

## ADMINIDLETIMEOUT

---

Die Option ADMINIDLETIMEOUT gibt die Zeit in Minuten an, die eine Verwaltungsclientsitzung inaktiv sein kann, bevor der Server die Sitzung abbricht.

Bei einer hohen Netzauslastung in Ihrer Umgebung können Sie den Wert für das Zeitlimit erhöhen, um zu verhindern, dass bei Verwaltungsclients eine Zeitlimitüberschreitung auftritt. Eine große Anzahl von inaktiven Sitzungen kann jedoch verhindern, dass andere Benutzer eine Verbindung zum Server herstellen können.

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

## Syntax

---

```
                .-15-----.  
>>-ADMINIDLETIMEOUT--+-Minuten+-----><
```

## Parameter

---

### Minuten

Gibt die maximale Anzahl Minuten an, die ein Server auf einen inaktiven Verwaltungsclient wartet. Der Standardwert ist 15 Minuten. Der Mindestwert ist 1 Minute.

## Beispiele

---

```
adminidletimeout 20
```

## ADMINONCLIENTPORT

---

Die Option ADMINONCLIENTPORT gibt an, ob TCPSPORT von Verwaltungssitzungen verwendet werden kann. Der Standardwert ist YES.

## Syntax

---

```
>>-ADMINONCLIENTPORT--+-YES+-----><  
                        '-NO--'
```

## Parameter

---

### YES

Ist die Option auf YES gesetzt, oder haben TCPSPORT und TCPADMINPORT denselben Wert (Standardwert), können Verwaltungssitzungen TCPSPORT verwenden.

### NO

Ist die Option auf NO gesetzt, und weicht der Wert für TCPADMINPORT von dem Wert für TCPSPORT ab, können Verwaltungssitzungen TCPSPORT nicht verwenden.

## Beispiele

---

Angeben, dass TCPSPORT von Verwaltungssitzungen verwendet werden kann.

```
adminonclientport yes
```

 Windows-Betriebssysteme

## ADSMGROUPNAME

---

Die Option ADSMGROUPNAME gibt den Namen einer Windows-Gruppe an. Ein Clientknoten muss Teil dieser Gruppe sein, um mit dem IBM Spectrum Protect-Server über NT Unified Logon arbeiten zu können. Der Clientknoten muss außerdem als IBM Spectrum Protect-Clientknoten registriert sein.

## Syntax

---

```
>>-ADSMGROUName--Gruppenname-----><
```

## Parameter

---

### Gruppenname

Gibt einen Windows-Gruppennamen an.

## Beispiele

---

IDD als Windows-Gruppe angeben:

```
adsmgroup idd
```

## ALIASHALT

---

Die Option ALIASHALT ermöglicht es Administratoren, dem IBM Spectrum Protect-Befehl **HALT** einen anderen Namen zuzuordnen.

Der Verwaltungsclient erkennt einen Aliasnamen für den Befehl HALT, wenn der Client mit der angegebenen Option CHECKALIASHALT gestartet wird. Für ausführliche Informationen siehe Verwaltungsoptionen.

## Syntax

---

```
>>-ALIASHALT--neuer_Name-----<<
```

## Parameter

---

neuer\_Name

Gibt den Aliasnamen des Befehls HALT zum Herunterfahren des IBM Spectrum Protect-Servers an. Die Mindestlänge für *Neuer Name* beträgt 1; die maximale Länge beträgt 16.

## Beispiele

---

```
aliashalt tsmhalt
```

## ALLOWDESAUTH

---

Die Option ALLOWDESAUTH gibt an, ob die Verwendung von Data Encryption Standard (DES) für die Authentifizierung zwischen einem Server und einem Client für Sichern/Archivieren zulässig ist.

Um die Verwendung von DES zu verhindern, geben Sie den Wert NO für die Option ALLOWDESAUTH an.

Um den IBM Spectrum Protect-Server für die Konformität mit dem Standard NIST SP800-131A zu konfigurieren, setzen Sie diese Option auf NO.

Einschränkungen:

- Auf dem Client für Sichern/Archivieren muss Version 6.3 oder höher ausgeführt werden, wenn Sie sich mit dem Wert NO für die Option ALLOWDESAUTH bei einem Server authentifizieren.
- Die automatische Implementierung des Clients für Sichern/Archivieren schlägt fehl, wenn diese Option auf NO gesetzt wird.

## Syntax

---

```
.-ALLOWDESAUTH--Yes-----.  
>>+-----+-----<<  
'-ALLOWDESAUTH---No---+'  
      '-Yes-'
```

## Parameter

---

Yes

Gibt an, dass der Server die Authentifizierung mit Clients für Sichern/Archivieren zulässt, die die DES-basierte Verschlüsselung verwenden. Der Standardwert ist YES.

No

Gibt an, dass der Server alle Clients für Sichern/Archivieren zurückweist, die versuchen, sich mit der DES-basierten Verschlüsselung zu authentifizieren.

## Beispiele

---

Angeben, dass der Server alle Clients für Sichern/Archivieren zurückweist, die versuchen, sich mit der DES-Verschlüsselung zu authentifizieren:

```
allowdesauth no
```

Angeben, dass der Server die Authentifizierung mit Clients für Sichern/Archivieren zulässt, die die DES-Verschlüsselung verwenden:

```
allowdesauth yes
```

## ALLOWREORGINDEX

---

Die Option ALLOWREORGINDEX gibt an, ob die vom Server eingeleitete Indexreorganisation aktiviert oder inaktiviert ist.

Der Standardwert ist YES.

### Syntax

---

```
>>-ALLOWREORGINDEX---+-Yes-+-----<<
                          '-No--'
```

### Parameter

---

Yes

Gibt an, dass die vom Server eingeleitete Indexreorganisation aktiviert ist.

No

Gibt an, dass die vom Server eingeleitete Indexreorganisation inaktiviert ist.

### Beispiel

---

Angeben, dass die vom Server eingeleitete Indexreorganisation aktiviert ist.

```
allowreorgindex yes
```

## ALLOWREORGTABLE

---

Die Option ALLOWREORGTABLE gibt an, ob die vom Server eingeleitete Tabellenreorganisation aktiviert oder inaktiviert ist.

Der Standardwert ist YES.

### Syntax

---

```
>>-ALLOWREORGTABLE---+-Yes-+-----<<
                          '-No--'
```

### Parameter

---

Yes

Gibt an, dass die vom Server eingeleitete Tabellenreorganisation aktiviert ist.

No

Gibt an, dass die vom Server eingeleitete Tabellenreorganisation inaktiviert ist.

### Beispiele

---

Angeben, dass die vom Server eingeleitete Tabellenreorganisation inaktiviert ist.

```
allowreorgtable no
```

## ARCHFAILOVERLOGDIRECTORY

---

Die Option ARCHFAILOVERLOGDIRECTORY gibt das Verzeichnis an, das der Server zum Speichern der Archivprotokolldateien verwendet, die nicht im Verzeichnis für Archivprotokolle gespeichert werden können.

Diese Option wird an die Optionsdatei angehängt, wenn der Befehl DSMSEVER FORMAT ausgeführt wird. Normalerweise muss das Verzeichnis nicht geändert werden.

## Syntax

---

```
>>-ARCHFailoverlogdirectory--Verzeichnisname-----<<
```

## Parameter

---

Verzeichnisname

Gibt einen vollständig qualifizierten Verzeichnisnamen an. Die maximale Anzahl Zeichen beträgt 175.

## Beispiele

---

```
archfailoverlogdirectory /tsm/archfailoverlog
```



```
archfailoverlogdirectory c:\tsmserv1\archfailoverlog
```

## ARCHLOGCOMPRESS

---

Sie können die Komprimierung von Archivprotokollen auf dem IBM Spectrum Protect-Server aktivieren oder inaktivieren. Durch die Komprimierung der Archivprotokolle wird der Speicherbedarf reduziert, der für die Speicherung erforderlich ist.

Die Serveroption ARCHLOGCOMPRESS gibt an, ob Protokolldateien, die in das Archivverzeichnis für Protokolle geschrieben werden, komprimiert werden.

## Syntax

---

```
>>-ARCHLOGCOMPRESS--+-No-- .  
'-----+-----+-----<<  
'-Yes-'
```

## Parameter

---

No

Gibt an, dass Protokolldateien, die in das Archivprotokollverzeichnis geschrieben werden, nicht komprimiert werden. Der Standardwert ist 'No'.

Yes

Gibt an, dass Protokolldateien, die in das Archivprotokollverzeichnis geschrieben werden, komprimiert werden.

Einschränkung: Gehen Sie mit Vorsicht vor, wenn Sie die Serveroption ARCHLOGCOMPRESS auf Systemen mit kontinuierlich hoher Datenträgerverwendung und hoher Auslastung aktivieren. Die Aktivierung dieser Option in dieser Systemumgebung kann Verzögerungen beim Archivieren von Protokolldateien aus dem Dateisystem für aktive Protokolldateien in das Archivprotokolldateisystem zur Folge haben. Diese Verzögerung kann zur Folge haben, dass für das Dateisystem für aktive Protokolldateien der Speicherbereich knapp wird. Stellen Sie sicher, dass der verfügbare Speicherbereich im Dateisystem für aktive Protokolldateien überwacht wird, nachdem die Komprimierung für das Archivprotokoll aktiviert wurde. Wenn die Belegung des Dateisystems für das Verzeichnis für aktive Protokolldateien derart hoch ist, dass fast kein Speicherbereich mehr verfügbar ist, muss die Serveroption ARCHLOGCOMPRESS inaktiviert werden. Mit dem Befehl SETOPT kann die Komprimierung für das Archivprotokoll sofort inaktiviert werden, ohne dass der Server angehalten werden müsste.

## Beispiel

---

Um die Komprimierung von Protokolldateien zu aktivieren, die in das Archivprotokollverzeichnis geschrieben werden, geben Sie die folgende Option an:

```
archlogcompress yes
```

## ARCHLOGDIRECTORY

---

Die Option ARCHLOGDIRECTORY gibt ein Verzeichnis an, in dem der Datenbankmanager eine Protokolldatei archivieren kann, nachdem alle in dieser Protokolldatei angegebenen Transaktionen abgeschlossen wurden.

Diese Option wird an die Optionsdatei angehängt, wenn der Befehl DSMSEV FORMAT ausgeführt wird.

## Syntax

---

```
>>-ARCHLOGDirectory--Verzeichnisname-----<<
```

## Parameter

---

Verzeichnisname

Gibt einen vollständig qualifizierten Verzeichnisnamen an. Die maximale Anzahl Zeichen beträgt 175.

## Beispiele

---

 AIX-Betriebssysteme  Linux-Betriebssysteme

```
archlogdirectory /tsm/archlog
```

 Windows-Betriebssysteme

```
archlogdirectory d:\tmserv1\archlog
```

## ARCHLOGUSEDTHRESHOLD

---

Die Option ARCHLOGUSEDTHRESHOLD gibt an, wann eine automatische Datenbanksicherung in Relation zum Prozentsatz des belegten Speicherbereichs für die Archivprotokolldatei gestartet werden soll. Der Standardwert ist 80 Prozent.

Mit der Option ARCHLOGUSEDTHRESHOLD werden häufige automatische Sicherungen verhindert. Wenn sich beispielsweise das Verzeichnis für Archivprotokolldateien in einem Dateisystem oder auf einem Laufwerk mit 400 GB befindet, wird eine Datenbanksicherung ausgelöst, wenn weniger als 80 GB freier Speicherbereich verfügbar ist. Wiederholte Datenbanksicherungen können zur Folge haben, dass der Server eine übermäßige Anzahl Arbeitsbänder verwendet.

## Syntax

---

```
                .-80---.  
>>-ARCHLOGUSEDTHRESHOLD--+-Wert-+-----<<
```

## Parameter

---

Wert

Der Prozentsatz des belegten Speicherbereichs für die Archivprotokolldatei, bevor eine automatische Sicherung gestartet wird.

Angaben, dass eine automatische Sicherung gestartet werden soll, wenn 90 Prozent des Speicherbereichs für die Archivprotokolldatei belegt sind.

```
archlogusedthreshold 90
```

## ASSISTVCRRECOVERY

---

Die Option ASSISTVCRRECOVERY gibt an, ob IBM Spectrum Protect ein Laufwerk IBM® 3590 bei der Wiederherstellung nach verloren gegangenen oder beschädigten VCR (Vital Cartridge Records) unterstützt. Wird YES (Standardwert) angegeben und erkennt IBM Spectrum Protect während der Ladeverarbeitung einen Fehler, geht TSM während der Entladeverarbeitung an das Datenende, um den Laufwerken die Wiederherstellung der VCR zu ermöglichen. Während der Bandoperation kann dies geringe Auswirkungen auf die Leistung haben, da das Laufwerk keine schnelle Suche mit einem verloren gegangenen oder beschädigten VCR ausführen kann. Es tritt jedoch kein Datenverlust auf.

## Syntax

---

```
>>-ASSISTVCRREcovery---+-Yes-+-----<<  
                        '-No--'
```

## Parameter

---

- Yes  
Gibt an, dass der Server die Wiederherstellung unterstützt.
- No  
Gibt an, dass der Server die Wiederherstellung nicht unterstützt.

## Beispiele

---

Unterstützung bei der Wiederherstellung inaktivieren:

```
assistvcrrecovery no
```

## AUDITSTORAGE

---

Als Teil einer Lizenzprüfung berechnet der Server nach Knoten den Umfang des Serverspeichers, der für Sicherungsdateien, Archivierungsdateien und speicherverwaltete Dateien verwendet wird. Bei Servern, die umfangreiche Datenmengen verwalten, kann diese Berechnung sehr viel CPU-Zeit beanspruchen und andere Serveraktivitäten blockieren. Mit der Option AUDITSTORAGE kann angegeben werden, dass bei der Lizenzprüfung der Speicher nicht berechnet werden soll.

Anmerkung: Diese Option wurde zuvor NOAUDITSTORAGE genannt.

## Syntax

---

```
>>-AUDITStorage--+-Yes-+-----><  
                '-No--'
```

## Parameter

---

- Yes  
Gibt an, dass der Speicher bei der Lizenzprüfung berechnet werden soll. Der Standardwert ist 'Yes'.
- No  
Gibt an, dass der Speicher bei der Lizenzprüfung nicht berechnet werden soll.

## Beispiele

---

```
auditstorage yes
```

## BACKUPINITIATIONROOT

---

Die Option BACKUPINITIATIONROOT gibt an, ob der Server Knotenparameterwerte für Benutzer überschreibt, die keine berechtigten IBM Spectrum Protect-Benutzer sind.

Sie können diese Serveroption aktualisieren, ohne den Server zu stoppen und erneut zu starten, indem Sie den Befehl SETOPT verwenden. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

## Syntax

---

```
>>-BACKUPINITIATIONROOT--+-ON-+-----><  
                '-Off-'
```

## Parameter

---

- ON  
Gibt an, dass das Starten von Sicherungsoperationen in Sitzungen von Clients unter AIX-, Linux-, Mac OS X- und Solaris-Betriebssystemen verhindert wird, wenn die Benutzer keine berechtigten IBM Spectrum Protect-Benutzer sind. Dies ist der Standardwert. Der Server überschreibt den Wert für den Parameter BACKUPINITIATION in den Befehlen REGISTER NODE und UPDATE NODE.  
Tipp: Eine Übersicht über berechnigte IBM Spectrum Protect-Benutzer finden Sie in Tasks für Rootbenutzer und berechnigte Benutzer des UNIX- und Linux-Clients.
- OFF



Gibt an, dass der Knotenwert für den Parameter BACKUPINITIATION verwendet wird. Der Parameter BACKUPINITIATION wird in den Befehlen REGISTER NODE und UPDATE NODE angegeben.

## Beispiel

---

Angeben, dass der Knotenwert für den Parameter BACKUPINITIATION verwendet wird.

```
backupinitiationroot off
```

## CHECKTAPEPOS

---

Die Option CHECKTAPEPOS gibt an, ob der IBM Spectrum Protect-Server die Position von Datenblöcken auf Band überprüft.

Die Option CHECKTAPEPOS gilt nur für Operationen, die Bandlaufwerke verwenden. Sie gilt nicht für Einheitenklassen mit sequenziellem Zugriff, die keine Bänder angeben, wie beispielsweise FILE. Wenn die Serverinformationen zur Position nicht mit der Position übereinstimmen, die von dem Laufwerk ermittelt wird, wird eine Fehlernachricht angezeigt, die Transaktion rückgängig gemacht, und die Daten werden nicht in der Datenbank festgeschrieben.

Mit der Option CHECKTAPEPOS können Sie den Modus 'Nur anhängen' für IBM LTO-Laufwerke der Generation 5 und später sowie für alle Laufwerke aktivieren, die diese Funktion unterstützen. Ist die Funktion aktiviert, gibt das Laufwerk einen Fehler aus, nachdem es Anweisungen zum Überschreiben von Daten auf dem gegenwärtig geladenen Datenträger empfangen hat. Das Band wird vom IBM Spectrum Protect-Server auf den korrekten Block neu positioniert und der Server setzt das Schreiben von Daten fort. Der Modus 'Nur anhängen' stellt einen zusätzlichen Schutz bereit, indem die meisten Situationen, in denen Daten überschrieben werden können, verhindert werden. Wenn Sie ein Laufwerk verwenden, das diese Funktion unterstützt, können Sie mit IBM Spectrum Protect und/oder dem Laufwerk die Datenposition auf dem Band überprüfen.

Anmerkung: Wenn Sie SAN-Bandbeschleunigungsfunktionen in der Struktur verwenden, setzen Sie CHECKTAPEPOS auf 'DRIVEonly' oder 'No', um falsche positive Positionierungsfehler zu vermeiden. Die IBM Spectrum Protect-Serveroption CHECKTAPEPOS erfordert kein für den Modus 'Nur anhängen' fähiges Laufwerk.

Änderungen an der Option CHECKTAPEPOS haben erst Auswirkungen auf Ladevorgänge, nachdem die Aktualisierung für das Laufwerk abgeschlossen wurde.

Der Standardwert ist YES.

## Syntax

---

```
>>-CHECKTAPEPOS---+Yes-----+-----<<
      +-No-----+
      +-TSMonly---+
      '-DRIVEonly-'
```

## Parameter

---

### Yes

Gibt an, dass der IBM Spectrum Protect-Server die Datenposition auf Band überprüft. Für Laufwerke, die den Modus 'Nur anhängen' unterstützen, gibt dieser Parameter an, dass es IBM Spectrum Protect dem Laufwerk ermöglicht, ebenfalls die Datenposition während jeder WRITE-Operation zu überprüfen, um das Überschreiben von Daten zu verhindern. Yes ist der Standardwert.

### No

Gibt an, dass die Überprüfung der Datenposition inaktiviert ist.

### TSMonly

Gibt an, dass der IBM Spectrum Protect-Server die Datenposition auf Band überprüft. Der Server verwendet nicht den Modus 'Nur anhängen', auch wenn das Laufwerk die Funktion unterstützt.

### DRIVEonly

Gibt an, dass der IBM Spectrum Protect-Server den Modus 'Nur anhängen' für Laufwerke aktiviert, die diese Funktion unterstützen. Der Server überprüft nicht die Datenposition auf Band.

## Beispiel

---

Die Datenposition auf Band überprüfen und den Modus 'Nur anhängen' für ein unterstütztes Laufwerk aktivieren:

```
checktapepos yes
```

## CLIENTDEDUPTXNLIMIT

---

Die Option CLIENTDEDUPTXNLIMIT gibt die maximale Größe einer Transaktion an, wenn vom Client deduplizierte Daten gesichert oder archiviert werden.

Wenn die clientseitige Deduplizierung für große Objekte verwendet wird, können lange laufende Transaktionen, die zur Aktualisierung der Datenbank erforderlich sind, eine umfangreiche Datenbankaktivität zur Folge haben. Eine umfangreiche Datenbankaktivität kann die folgenden Symptome zur Folge haben:

- Reduzierter Durchsatz bei Clientsicherungs- und -archivierungsoperationen
- Ressourcenkonflikt aufgrund gleichzeitig ablaufender Serveroperationen
- Exzessive Wiederherstellungsprotokollaktivität

Das Ausmaß, in dem diese Symptome auftreten, hängt von der Anzahl und Größe der Objekte ab, die unter Verwendung der clientseitigen Deduplizierung von Daten gespeichert werden, von der Intensität und dem Typ der gleichzeitig ablaufenden Operationen auf dem IBM Spectrum Protect-Server und von der IBM Spectrum Protect-Serverkonfiguration.

Mit der Serveroption CLIENTDEDUPTXNLIMIT können Sie eine maximale Größe (in Gigabyte) für Transaktionen angeben, wenn vom Client deduplizierte Daten gesichert oder archiviert werden. Wenn ein Objekt oder eine Gruppe von Objekten in einer einzelnen Transaktion den mit CLIENTDEDUPTXNLIMIT angegebenen Grenzwert überschreitet, werden die Objekte nicht vom Client dedupliziert, und die Transaktion kann fehlschlagen. Sie können einen Wert von 32 bis 102400 GB angeben. Der Standardwert ist 5120 GB.

Wenn ein Objekt oder eine Gruppe von Objekten in einer einzelnen Transaktion den mit CLIENTDEDUPTXNLIMIT angegebenen Grenzwert überschreitet, werden die Objekte oder wird die Gruppe von Objekten nicht vom Client dedupliziert. Die Objekte werden jedoch an den Server gesendet. Diese Objekte können auf dem Server dedupliziert werden, abhängig davon, ob der Zielspeicherpool für die Deduplizierung von Daten konfiguriert ist, und abhängig von dem Wert der Option SERVERDEDUPTXNLIMIT. Objekte in einem für die Deduplizierung aktivierten Speicherpool, die kleiner als der Wert der Option SERVERDEDUPTXNLIMIT sind, werden von einem Serverprozess zum Identifizieren doppelter Daten dedupliziert.

Der geeignete Wert für diese Option hängt von der IBM Spectrum Protect-Serverkonfiguration und der gleichzeitig stattfindenden Serveraktivität ab. Sie können einen hohen Wert für diese Option angeben, wenn Sie den Ressourcenkonflikt minimieren. Um den Ressourcenkonflikt zu minimieren, führen Sie Operationen, wie beispielsweise Sicherung, Archivierung, Identifizierung doppelter Daten (Befehl IDENTIFY DUPLICATES) und Wiederherstellung, zu unterschiedlichen Zeiten aus.

Um diese Serveroption zu aktualisieren, ohne den Server zu stoppen und erneut zu starten, verwenden Sie den Befehl SETOPT.

### Syntax

---

```
.-5120-----.  
>>-CLIENTDEDUPTXNlimit--+-Gigabyte+-----<<
```

### Parameter

---

#### Gigabyte

Gibt die maximale Größe (in Gigabyte) von Objekten an, die unter Verwendung der clientseitigen Deduplizierung von Daten gesichert oder archiviert werden können. Sie können einen Wert von 32 bis 102400 angeben. Der Standardwert ist 5120.

### Beispiele

---

Die clientseitige Deduplizierung von Daten für alle Objekte über 80 GB inaktivieren:

```
clientdeduptxnlimit 80
```

## CLIENTDEPLOYCATALOGURL

---

Die Option CLIENTDEPLOYCATALOGURL gibt die Position der Katalogdatei an, die für automatische Clientimplementierungsoperationen verwendet wird.

Sie können diese Serveroption aktualisieren, ohne den Server zu stoppen und erneut zu starten, indem Sie den Befehl SETOPT verwenden. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

### Syntax

---

```
>>-CLIENTDEPLOYCATalogurl----->
    .-https://public.dhe.ibm.com/storage/tivoli-storage-management/catalog/client/catalog.json-.
>--+-URL-----+><
```

## Parameter

---

### URL

Gibt die URL an, von der der Server die Katalogdatei für automatische Clientimplementierungsoperationen herunterlädt. Die Katalogdatei speichert Merkmale für Clientimplementierungsoperationen, einschließlich der Position der Implementierungspakete. Die Standard-URL ist `https://public.dhe.ibm.com/storage/tivoli-storage-management/catalog/client/catalog.json`.

Um anzugeben, dass die Katalogdatei von einer anderen Position heruntergeladen wird, verwenden Sie den Befehl `SETOPT`, um eine angepasste URL anzugeben. Um die URL auf den Standardwert zurückzusetzen, geben Sie den Befehl `SETOPT` mit einer leeren Zeichenfolge aus: `""`. Wird eine angepasste URL angegeben, wird die angepasste URL beibehalten, nachdem für den Server ein Upgrade durchgeführt wurde.

## Beispiel

---

Die angepasste URL `https://customAddress` angeben.

```
setopt clientdeploycatalogurl https://customAddress
```

## Beispiel

---

Den Wert der Option `CLIENTDEPLOYCATALOGURL` auf den Standardwert zurücksetzen.

```
setopt clientdeploycatalogurl ""
```

## CLIENTDEPLOYUSELOCALCATALOG

---

Die Option `CLIENTDEPLOYCATALOGURL` gibt an, ob die lokale Version der Katalogdatei für automatische Clientimplementierungsoperationen verwendet wird.

Sie können diese Serveroption aktualisieren, ohne den Server zu stoppen und erneut zu starten, indem Sie den Befehl `SETOPT` verwenden. Siehe `SETOPT` (Serveroption für dynamisches Aktualisieren definieren).

## Syntax

---

```
                .-No--.
>>-CLIENTDEPLOYUSELOCALcatalog---+Yes+-----><
```

## Parameter

---

### No

Gibt an, dass die lokale Version der Katalogdatei nicht verwendet wird. Stattdessen wird die Katalogdatei von der Position heruntergeladen, die mit der Option `CLIENTDEPLOYCATALOGURL` angegeben wird. Der Standardwert ist `NO`.

### Yes

Gibt an, dass die lokale Version der Katalogdatei verwendet wird. Katalogdateien werden nicht während der Ausführung von Clientimplementierungsoperationen heruntergeladen. Wenn Sie diese Option auf `YES` setzen, wird der Wert beibehalten, nachdem für den Server ein Upgrade durchgeführt wurde.

## Beispiel

---

Angeben, dass die lokale Version der Katalogdatei verwendet wird.

```
setopt clientdeployuselocalcatalog yes
```

## COMMMETHOD

---

Die Option `COMMMETHOD` gibt eine Übertragungsmethode an, die vom Server verwendet werden soll.

Sie können den Server für die Verwendung mehrerer Übertragungsmethoden konfigurieren. Die am häufigsten verwendeten Übertragungsmethoden sind TCPIP, V6TCPIP und SHAREDMEM. Um mehrere Übertragungsmethoden anzugeben, aktivieren Sie jede Methode, indem Sie eine Zeilengruppe COMMETHOD zur Optionsdatei dmserv.opt hinzufügen.

Wichtig: Bei der Aktivierung einer Übertragungsmethode müssen Sie auch die Optionen, die für die Übertragungsmethode bestimmt sind, zur Optionsdatei hinzufügen.

## Syntax

---

```
.-TCPIP-----.  
>>-COMMETHOD--+-NAMEDPIPE-+-----<<  
+-NONE-----+  
+-SHAREDMEM-+  
+-SNMP-----+  
+-TCPIP-----+  
'-V6TCPIP---'
```

## Parameter

---

Es kann eine der folgenden Übertragungsmethoden gewählt werden:

 NAMEDPIPES

 Gibt die Übertragungsmethode mit benannten Pipes an.

NONE

Gibt an, dass keine Übertragungsmethode verwendet wird. Diese Option lässt nicht zu, dass Benutzer den Server ansprechen, und eignet sich deshalb zum Experimentieren mit Maßnahmenbefehlen.

SHAREDMEM

Gibt die Übertragungsmethode für gemeinsam benutzten Speicher an. Bei dieser Methode wird gleichzeitig derselbe Speicherbereich zum Senden von Daten zwischen mehreren Anwendungen verwendet. Sowohl der Server als auch der Client für Sichern/Archivieren müssen für die Unterstützung der Übertragungsmethode für gemeinsam benutzten Speicher konfiguriert und auf demselben Computer installiert sein.

SNMP

Gibt SNMP als Übertragungsmethode an.

TCPIP

Gibt TCP/IP als Übertragungsmethode an. Diese Option ist der Standardwert. Wird TCPIP angegeben, wird ausschließlich TCP/IP Version 4 verwendet.

V6TCPIP

Gibt TCP/IP als Übertragungsmethode an. Sind TCP/IP Version 4 und Version 6 konfiguriert, verwendet IBM Spectrum Protect beide Protokolle gleichzeitig. Wird COMMETHOD TCPIP und COMMETHOD V6TCPIP angegeben, überschreibt V6TCPIP die Angabe von TCPIP. Eine gültige DNS-Umgebung (DNS = Domain Name Server) muss vorhanden sein, damit bei Angabe dieser Option TCP/IP V4 oder TCP/IP V6 verwendet werden kann.

## Beispiele

---

Beispiel für die Angabe mehrerer Übertragungsmethoden, die vom Server verwendet werden sollen (TCP/IP und TCP/IP Version 6):

```
commethod tcpip  
commethod v6tcpip
```

## COMMTIMEOUT

---

Die Option COMMTIMEOUT gibt an, wie lange der Server während einer Operation, die eine Datenbankaktualisierung zur Folge hat, auf eine erwartete Clientnachricht wartet. Wenn die Zeitlänge dieses Zeitlimit überschreitet, beendet der Server die Sitzung mit dem Client. Sie können den Wert für das Zeitlimit erhöhen, damit keine Zeitlimitüberschreitung bei den Clients auftritt. Eine Zeitlimitüberschreitung kann bei Clients auftreten, wenn eine hohe Netzauslastung in Ihrer Umgebung vorhanden ist, oder wenn die Clients große Dateien sichern.

Die Serveroption COMMTIMEOUT wird für Sitzungen verwendet, die keine Verwaltungssitzungen sind. Für Verwaltungsclientsitzungen siehe die Option ADMINCOMMTIMEOUT.

Sie können diese Serveroption aktualisieren, ohne den Server zu stoppen und erneut zu starten, indem Sie den Befehl SETOPT verwenden.

## Syntax

---

```
      .-60-----.  
>>-COMMTIMEOUT--+-Sekunden+-----><
```

## Parameter

---

### Sekunden

Gibt die maximale Anzahl Sekunden an, die ein Server auf eine Antwort vom Client wartet. Der Standardwert ist 60. Der Mindestwert ist 1.

## Beispiele

---

```
commtimeout 60
```

## CONTAINERRESOURCETIMEOUT

---

Die Option CONTAINERRESOURCETIMEOUT gibt an, wie lange der Server auf die Ausführung einer Datenspeicheroperation für einen Containerspeicherpool wartet.

## Syntax

---

Wenn eine Zeitlimitüberschreitung auftritt, verbleiben alle in dem Containerspeicherpool gespeicherten Daten in dem Containerspeicherpool. Die Datenspeicheroperation wird beendet und die Anforderung für die Containerressource wird abgebrochen.

```
      .-180-----.  
>>-CONTAINERRESOURCETIMEOUT--+-Minuten+-----><
```

## Parameter

---

### Minuten

Gibt die maximale Anzahl Minuten an, die ein Server wartet, bevor eine Operation abgebrochen wird. Der Standardwert ist 180 Minuten. Der Mindestwert ist 1 Minute.

## Beispiel

---

Angeben, dass der Server 4 Stunden wartet, bevor eine Datenspeicheroperation für einen Containerspeicherpool abgebrochen wird.

```
containerresourcetimeout 240
```



## DATEFORMAT

---

Die Option DATEFORMAT gibt das Format an, in dem Datumsangaben vom Server angezeigt werden.

Der Wert für DATEFORMAT wird von dem Format der länderspezifischen Angaben überschrieben, wenn die länderspezifischen Angaben beim Serverstart initialisiert werden. Die länderspezifischen Angaben werden in der Option LANGUAGE angegeben.

## Syntax

---

```
>>-DATEFORMAT--n-----><
```

## Parameter

---

### n

Eine Zahl von 1 bis 5 auswählen, um das vom Server verwendete Datumsformat anzugeben. Der Standardwert ist 1.

### 1

MM/DD/YYYY

- 2 DD-MM-YYYY
- 3 YYYY-MM-DD
- 4 DD.MM.YYYY
- 5 YYYY.MM.DD

## Beispiele

dateformat 4

## DBDIAGLOGSIZE

Mit dieser Option können Sie die Größe des Speicherbereichs steuern, der von Diagnoseprotokolldateien verwendet wird.

Der Datenbankmanager verwendet Diagnoseprotokolldateien zum Protokollieren von Nachrichten. Sie müssen die Größe der Protokolldateien steuern, damit sie nicht das Dateisystem füllen. Verwenden Sie die Option DBDIAGLOGSIZE, um die Größe des Speicherbereichs zu definieren, der von den Protokolldateien verwendet wird.

Wenn Sie einen Wert im Bereich von 2 bis 9999 definieren, werden maximal 10 rollierende Diagnoseprotokolldateien aufbewahrt. Jeder Dateiname gibt die Reihenfolge an, in der die Datei erstellt wurde. Wenn eine Datei voll ist, wird die nächste Datei erstellt. Wenn die zehnte Datei voll ist, wird die älteste Datei gelöscht und eine neue Datei erstellt. Das folgende Beispiel zeigt, wie die rollierenden Protokolldateien aussehen können:

```
db2diag.14.log, db2diag.15.log, ... , db2diag.22.log, db2diag.23.log
```

Wenn db2diag.23.log voll ist, wird db2diag.14.log gelöscht und db2diag.24.log erstellt.

Der Server überprüft stündlich den Dateibereich, der die Diagnoseprotokolldateien enthält. Nachrichten werden alle 12 Stunden angezeigt, wenn eine der folgenden Bedingungen auftritt:

- Der verfügbare Speicherplatz in dem Dateisystem, in dem sich die Diagnoseprotokolldateien befinden, beträgt weniger als 20 % des gesamten Dateisystembereichs.
- Der verfügbare Speicherplatz in dem Dateisystem, in dem sich das Serverinstanzverzeichnis befindet, beträgt weniger als 1 GB.

Wenn Sie den Wert 0 angeben, wird nur eine Protokolldatei (db2diag.log) für alle Diagnosenachrichten verwendet. Für die Größe der Protokolldatei gibt es keine Begrenzung.

Einschränkung: Sie müssen die Größe der Diagnoseprotokolldateien überwachen, um sicherzustellen, dass sie nicht den gesamten verfügbaren Speicherbereich im Dateisystem verwenden. Ist nicht genügend Speicherbereich verfügbar, erfolgt möglicherweise keine Reaktion durch den Server.

## Syntax

```
.-1024-----.  
>>-DBDIAGLOGSize---+Megabyte+-----<<
```

## Parameter

### Megabyte

Gibt die Größe des Speicherbereichs in Megabyte an, der von Diagnoseprotokolldateien verwendet wird. Geben Sie einen Wert im Bereich von 2 bis 9999 oder den Wert 0 an. Der Standardwert ist 1024.

Wenn Sie einen Wert im Bereich von 2 bis 9999 angeben, werden rollierende Protokolldateien verwendet, und der Wert gibt die Gesamtgröße aller 10 Protokolldateien in Megabyte an. Der Wert wird auf 1024 zurückgesetzt, wenn der Server erneut gestartet wird.

Wenn Sie den Wert 0 angeben, wird eine Protokolldatei verwendet, und es gibt für die Größe der Protokolldatei keine Begrenzung.

Sollen Nachrichten archiviert werden, geben Sie den Wert 0 an, um sicherzustellen, dass die Datei db2diag.log den gesamten verfügbaren Speicherbereich ohne die Verwendung rollierender Protokolldateien verwenden kann.

Nachdem Sie den Wert des Parameters Megabyte mit der Option DBDIAGLOGSIZE auf 0 gesetzt haben, werden Nachrichten anfänglich in rollierende Protokolldateien geschrieben. Nach dem Neustart des Servers werden Nachrichten in die Datei db2diag.log geschrieben.

Tipp: Wenn Sie einen Wert im Bereich von 2 bis 9999 mithilfe der Serveroptionsdatei dmserv.opt angeben, wird der Wert beim Serverstart nicht automatisch zurückgesetzt. Der Wert bleibt unverändert, bis er mit dem Befehl SETOPT geändert oder aus der Datei dmserv.opt entfernt wird.

## Beispiel: Eine maximale Größe von 5120 Megabyte angeben

---

Die Größe der Diagnoseprotokolldateien mit 5120 Megabyte (5 GB) angeben:

```
dbdiaglogsize 5120
```

## Beispiel: Nachrichten in einer einzelnen Protokolldatei archivieren

---

Nachrichten archivieren, indem angegeben wird, dass die Nachrichten in die Datei db2diag.log geschrieben werden:

```
dbdiaglogsize 0
```

### Zugehörige Informationen:

 Produktinformation zu DB2 Version 10.5

## DBDIAGPATHFSTHRESHOLD

---

Die Option DBDIAGPATHFSTHRESHOLD gibt den Schwellenwert für freien Speicherbereich in dem Dateisystem oder auf der Platte an, das bzw. die die Datei db2diag.log enthält.

Wenn der freie Speicherbereich kleiner-gleich dem angegebenen Schwellenwert ist, wird die Fehlermeldung ANR1545W angezeigt. Standardmäßig wird die Nachricht angezeigt, wenn das Dateisystem oder die Platte 20 % oder weniger freien Plattenspeicherplatz hat.

Sie können diese Serveroption aktualisieren, ohne den Server zu stoppen und erneut zu starten, indem Sie den Befehl SETOPT verwenden. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

## Syntax

---

```
>>-DBDIAGPATHFSTHreshold--Prozent-----<<
```

## Parameter

---

### Prozent

Gibt den Prozentsatz des verfügbaren Speicherbereichs im Dateisystem an. Gültige Werte sind 0 bis 100. Der Standardwert ist 20. Tipp: Um die besten Ergebnisse zu erzielen, geben Sie keine niedrigen oder hohen Werte für den Parameter Prozent an. Ein niedriger Wert kann zur Folge haben, dass das Dateisystem voll ist, bevor Sie das Problem korrigieren können. Ein volles Dateisystem kann die Serverdatenbank beschädigen. Ein hoher Wert kann dazu führen, dass viele Nachrichten ANR1545W im Serveraktivitätenprotokoll angezeigt werden.

## Beispiel

---

Den Schwellenwert auf 10% setzen.

```
setopt DBDIAGPATHFSTH 10
```

## DBMEMPERCENT

---

Verwenden Sie diese Option, um den Prozentsatz des virtuellen Adressraums anzugeben, der den Datenbankmanagerprozessen zugeordnet ist.

Werden andere Anwendungen als der IBM Spectrum Protect-Server auf dem System ausgeführt, stellen Sie sicher, dass der Wert einen angemessenen Speicher für die anderen Anwendungen vorsieht.

## Syntax

---

```
>>-DBMEMPERCENT---+Prozent-+-----<<  
'-AUTO----'
```

## Parameter

---

### Prozent

Definieren Sie einen Wert von 10 bis 99.

### AUTO

Der Datenbankmanager setzt den Prozentsatz automatisch auf einen Wert, der zwischen 75 Prozent und 95 Prozent des Systemarbeitspeichers liegt. Der Standardwert ist AUTO.

## Beispiele

---

```
dbmempercent 50
```

## DBMTCPPORT

---

Die Option DBMTCPPORT gibt die Nummer des Anschlusses an, an dem der TCP/IP-DFV-Treiber für den Datenbankmanager auf Anforderungen für Clientsitzungen.

Die angegebene Anschlussnummer muss für die Verwendung durch den Datenbankmanager reserviert werden.

Standardmäßig verwendet der IBM Spectrum Protect-Server die Interprozesskommunikation (IPC), um Verbindungen für die ersten beiden Verbindungspools mit maximal 480 Verbindungen für jeden Pool herzustellen. Nachdem die ersten 960 Verbindungen hergestellt wurden, verwendet der IBM Spectrum Protect-Server TCP/IP für alle weiteren Verbindungen.

## Syntax

---

```
>>-DBMTCPPort--Anschlussnummer----->>
```

## Parameter

---

### Anschlussnummer

Gibt die Nummer des TCP/IP-Anschlusses an, an dem der Datenbankmanager auf die Übertragung vom Server wartet. Gültige Werte sind ganze Zahlen von 1024 bis 65535.

Die Standardanschlussnummer ist der Wert der Serveroption TCPPOINT plus 50.000. Hat die Serveroption TCPPOINT beispielsweise den Wert 1500, lautet die Standardanschlussnummer für DBMTCPPORT 51500.

Ist die Serveroption TCPPOINT größer als 9999, fügen Sie die letzten vier Ziffern des Werts dem Wert 50000 hinzu. Hat die Option TCPPOINT beispielsweise den Wert 11500, wird 1550 dem Wert 50000 hinzugefügt. Daraus ergibt sich eine Anschlussnummer für DBMTCPPORT mit dem Wert 51500.

## Beispiel

---

```
dbmtcport 51500
```

## DEDUPREQUIRESBACKUP

---

Die Option DEDUPREQUIRESBACKUP gibt an, ob Datenträger in primären Speicherpools mit sequenziellem Zugriff, die für die Deduplizierung von Daten definiert sind, wiederhergestellt und doppelte Daten gelöscht werden können, bevor die Speicherpools gesichert werden.

Lautet der Wert dieser Option YES (Standardwert), müssen Sie Daten in Kopierspeicherpools sichern, die nicht für die Deduplizierung von Daten definiert sind. Verwenden Sie den Befehl BACKUP STGPOOL, um Daten in Kopierspeicherpools zu sichern.

Beachten Sie, dass die Wiederherstellung eines Datenträgers in einem Speicherpool, der für die Deduplizierung von Daten definiert ist, möglicherweise nicht erfolgt, wenn der Datenträger zum ersten Mal auswählbar ist. Der Server führt zusätzliche Überprüfungen durch, um sicherzustellen, dass Daten aus einem Speicherpool, der für die Deduplizierung von Daten definiert ist, in einen Kopierspeicherpool gesichert wurden. Diese Überprüfungen erfordern mehrere BACKUP STGPOOL-Instanzen, bevor der Server einen Datenträger wiederherstellt. Nachdem der Server geprüft hat, dass die Daten gesichert wurden, wird der Datenträger wiederhergestellt.

Sie können diese Option mit dem Befehl SETOPT dynamisch ändern.

Achtung: Um die Möglichkeit eines Datenverlusts zu minimieren, ändern Sie nicht die Standardeinstellung für diese Serveroption. Geben Sie den Wert NO nur an, wenn Sie keine Kopierspeicherpools haben und Sie keine Speicherpoolsicherungen ausführen.



## Syntax

---

```
>>-DEDUPREQUIRESBACKUP--+-Yes-+-----<<
      '-No--'
```

## Parameter

---

### Yes

Gibt an, dass der Speicherpool gesichert werden muss, bevor Datenträger wiederhergestellt und doppelte Daten gelöscht werden können. Dies ist der Standardwert.

### No

Gibt an, dass Datenträger in primären Speicherpools mit sequenziellem Zugriff, die für die Deduplizierung von Daten definiert sind, wiederhergestellt und doppelte Daten gelöscht werden können, wenn die Speicherpools nicht gesichert werden.

## Beispiele

---

Angaben, dass primäre Speicherpools mit sequenziellem Zugriff, die für die Deduplizierung von Daten definiert sind, nicht gesichert werden müssen.

```
deduprequiresbackup no
```

## DEDUPTIER2FILESIZE

---

Die Option DEDUPTIER2FILESIZE gibt an, bei welcher Dateigröße IBM Spectrum Protect beginnt, die Schicht 2 der Dateneduplizierung zu verwenden.

## Syntax

---

```
>>-DEDUPTIER2FILESIZE--nnn-----<<
```

## Parameter

---

### nnn

Gibt die Dateigröße in Gigabyte an, bei der der IBM Spectrum Protect-Server beginnt, die Schicht 2 der Dateneduplizierung zu verwenden. Sie können einen Wert von 20 bis 9999 angeben. Der Standardwert ist 100.

Anmerkung: Wenn der für diese Option angegebene Wert oder der standardmäßig angenommene Wert größer als der Wert für die Option SERVERDEDUPTXNLIMIT ist, wird diese Option für die Serverdateneduplizierung ignoriert. Wenn der für diese Option angegebene Wert oder der standardmäßig angenommene Wert größer als der Wert für die Option CLIENTDEDUPTXNLIMIT ist, wird diese Option für die Clientdateneduplizierung ignoriert.

## Beispiele

---

```
deduptier2filesize 550
```

## DEDUPTIER3FILESIZE

---

Die Option DEDUPTIER3FILESIZE gibt an, bei welcher Dateigröße IBM Spectrum Protect beginnt, die Schicht 3 der Dateneduplizierung zu verwenden.

## Syntax

---

```
>>-DEDUPTIER3FILESIZE--nnn-----<<
```

## Parameter

---

### nnn

Gibt die Dateigröße in Gigabyte an, bei der der IBM Spectrum Protect-Server beginnt, die Schicht 3 der Dateneduplizierung zu verwenden. Sie können einen Wert von 90 bis 9999 angeben. Der Standardwert ist 400.

- Wenn der für diese Option angegebene Wert oder der standardmäßig angenommene Wert größer als der Wert für die Option SERVERDEDUPTXNLIMIT ist, wird diese Option für die Serverdateneduplizierung ignoriert.
- Wenn der für diese Option angegebene Wert oder der standardmäßig angenommene Wert größer als der Wert für die Option CLIENTDEDUPTXNLIMIT ist, wird diese Option für die Clientdateneduplizierung ignoriert.
- Wenn der für diese Option angegebene Wert oder der standardmäßig angenommene Wert kleiner als der Wert ist, der für die Option DEDUPTIER2FILESIZE angegeben ist oder standardmäßig angenommen wird, wird der Wert von DEDUPTIER2FILESIZE für diese Option verwendet.

## Beispiele

---

```
deduptier3filesize 1150
```

## DEVCONFIG

---

Die Option DEVCONFIG gibt den Namen einer Datei an, in der IBM Spectrum Protect eine Sicherungskopie der Einheitenkonfigurationsinformationen speichern soll.

IBM Spectrum Protect speichert folgende Informationen in der Einheitenkonfigurationsdatei:

- Mit dem Befehl DEFINE DEVCLASS erstellte Einheitenklassendefinitionen
- Mit dem Befehl DEFINE DRIVE erstellte Laufwerkdefinitionen
- Kassettenarchivdefinitionen, die mit dem Befehl DEFINE LIBRARY erstellt wurden
- Informationen zum Datenträgerbestand im Kassettenarchiv für die automatisierten Kassettenarchive mit LIBTYPE=SCSI
- Pfaddefinitionen, die mit dem Befehl DEFINE PATH erstellt wurden
- Serverdefinitionen, die mit dem Befehl DEFINE SERVER erstellt wurden
- Servername, der mit dem Befehl SET SERVERNAME erstellt wurde
- Serverkennwort, das mit dem Befehl SET SERVERPASSWORD erstellt wurde

Anmerkung:

- Nur Pfaddefinitionen mit SRCTYPE=SERVER werden in der Einheitenkonfigurationsdatei gesichert. Pfade mit SRCTYPE=DATAMOVER werden nicht in die Datei geschrieben.
- Informationen zur Datenträgerposition im Kassettenarchiv werden als Kommentare (*/\*...\*/*) in der Einheitenkonfigurationsdatei gespeichert, wenn die Befehle CHECKIN LIBVOLUME, CHECKOUT LIBVOLUME und AUDIT LIBRARY für SCSI-Kassettenarchive ausgegeben werden.

Achtung: Um die Datenbank nach einem Katastrophenfall zurückzuschreiben, benötigen Sie eine Kopie der aktuellen Einheitenkonfigurationsdatei. Die Einheitenkonfigurationsdatei kann nicht erneut erstellt werden.

Es können eine oder mehrere Optionen DEVCONFIG in die Serveroptionsdatei eingeschlossen werden. Wird mit mehreren DEVCONFIG-Optionen gearbeitet, aktualisiert IBM Spectrum Protect automatisch die Einheitenkonfigurationsinformationen in jeder angegebenen Datei und erstellt eine Sicherungskopie.

## Syntax

---

```
>>-DEVCONFig--Dateiname-----<<
```

## Parameter

---

Dateiname

Gibt den Namen einer Datei an, in der eine Sicherungskopie der Einheitenkonfigurationsinformationen gespeichert werden soll.

## Beispiele

---

```
devconfig devices.sav
```

## DISABLEREORGTABLE

---

Die Option DISABLEREORGTABLE gibt an, ob die Onlinetabellenreorganisation für Tabellennamen inaktiviert wird, die in der Tabellenliste angegeben sind.

Um die Option DISABLEREORGTABLE zu verwenden, müssen Sie den Server anhalten, die Optionsdatei aktualisieren und dann den Server erneut starten.

## Syntax

---

```
>>-DISABLEREORGTabe---Tabellenliste-----<<
```

## Parameter

---

### Tabellenliste

Gibt eine Liste der Tabellennamen an, für die die Tabellenreorganisation inaktiviert wird. Werden keine Tabellennamen mit der Option angegeben oder ist die Option nicht in der Optionsdatei enthalten, werden keine Tabellen inaktiviert.

Einschränkung: Die folgenden Tabellen sind bereits von der Tabellenreorganisationsverarbeitung ausgeschlossen und können für diese Option nicht angegeben werden:

- STAGED\_EXPIRING\_OBJECTS
- STAGED\_OBJECT\_IDS
- BF\_DEREFERENCED\_CHUNKS
- BF\_QUEUED\_CHUNKS

## Beispiel

---

```
DISABLEREORGTABLE BF_BITFILE_EXTENTS,REPLICATING_OBJECTS
```

## DISABLESCHEDS

---

Die Option DISABLESCHEDS gibt an, ob Verwaltungszeitpläne und Clientzeitpläne während der Wiederherstellung des IBM Spectrum Protect-Servers inaktiviert sind.

## Syntax

---

```
>>-DISABLEScheds---Yes+-----<<  
      '-No--'
```

## Parameter

---

### Yes

Gibt an, dass Verwaltungszeitpläne und Clientzeitpläne inaktiviert sind.

### No

Gibt an, dass Verwaltungszeitpläne und Clientzeitpläne aktiviert sind.

## Beispiele

---

```
disablescheds no
```

## DISPLAYLFINFO

---

Die Option DISPLAYLFINFO gibt an, wie die Abrechnungssätze und Einträge in der Übersichtstabelle den Knotennamen angeben.

Ist diese Option aktiviert, geben die Abrechnungssätze und Einträge in der Übersichtstabelle Knotenname(Speicheragentenname) für den Knotennamen an. Ist diese Option nicht aktiviert, geben die Abrechnungssätze und Einträge in der Übersichtstabelle nur Knotenname für den Knotennamen an. Der Standardwert ist 'No'.

## Syntax

---

```
>>-DISPLAYLFINFO---Yes+-----<<  
      '-No--'
```

## Parameter

---

### Yes

Gibt an, dass die Abrechnungssätze und Einträge in der Übersichtstabelle den Speicheragentennamen angeben.

No

Gibt an, dass die Abrechnungssätze und Einträge in der Übersichtstabelle den Speicheragentennamen nicht angeben. Dies ist der Standardwert.

## Beispiele

---

```
displaylfinfo yes
```

Das Ergebnis zeigt den folgenden Abrechnungssatz mit dem angezeigten Speicheragentennamen (STA53):

```
5,0,ADSM,07/13/2004,15:35:14,COLIND-TUC(STA53),,WinNT,1,Tcp/Ip,1,0,0,0,0,223,4063,0,0,222,7,8,3,1,4,0,0,0,0,3,0
```

In der entsprechenden Übersichtstabelle wird ebenfalls der Speicheragentenname angezeigt:

```
START_TIME: 2004-07-13 15:35:07.000000
END_TIME: 2004-07-13 15:35:14.000000
ACTIVITY: BACKUP
NUMBER: 8
ENTITY: COLIND-TUC (STA53)
COMMETH: Tcp/Ip
ADDRESS: colind-tuc:2229
SCHEDULE_NAME:
EXAMINED: 0
AFFECTED: 223
FAILED: 0
BYTES: 4160875
IDLE: 8
MEDIAW: 1
PROCESSES: 1
SUCCESSFUL: YES
VOLUME_NAME:
DRIVE_NAME:
LIBRARY_NAME:
LAST_USE:
COMM_WAIT: 3
NUM_OFFSITE_VOLS:
```

## DNSLOOKUP

---

Die Option DNSLOOKUP gibt an, ob der Server System-API-Aufrufe verwendet, um die DNS-Namen (DNS = Domain Name Server) von Systemen zu bestimmen, die den Server ansprechen.

### Syntax

---

```
>>-DNSLOOKUP---Yes+-----><
      '-No--'
```

### Parameter

---

Yes

Gibt an, dass der Server die DNS-Namen von Systemen abrufen, die den Server ansprechen. Yes ist der Standardwert.

No

Gibt an, dass der Server die DNS-Namen von Systemen nicht abrufen, die den Server ansprechen.

## Beispiele

---

```
dnslookup yes
```

## DRIVEACQUIRERETRY

---

Mit der Option DRIVEACQUIRERETRY kann angegeben werden, wie oft der Server versuchen soll, ein Laufwerk in einem Kassettenarchiv IBM® 349x anzufordern. Wird das Kassettenarchiv von mehreren Anwendungen gemeinsam benutzt, scheinen seine Laufwerke für den Server verfügbar zu sein (durch die Verwendung eines Sendeaufrufprozesses im Hintergrund), obwohl sie es nicht sind.

Diese Option ist nur gültig, wenn 3494SHARED YES in der Datei dsmserv.opt angegeben wurde. Wurde DRIVEACQUIRERETRY NEVER angegeben, müssen Sie überwachen, wie lange Jobs auf Laufwerke gewartet haben und wie lange der Server die Laufwerke abgefragt

hat. Außerdem müssen Sie möglicherweise den Status dieser Laufwerke in den anderen IBM Spectrum Protect-Servern überprüfen. Möglicherweise stecken Kassetten in den Laufwerken und die anderen IBM Spectrum Protect-Server haben die Laufwerke gegebenenfalls als *Offline* markiert. Ist dies der Fall, müssen Sie die Laufwerke auf dem IBM Spectrum Protect-Server als *Offline* markieren, der die Laufwerke abfragt. Falls erforderlich, brechen Sie auch alle wartenden Jobs ab.

## Syntax

---

```
>>-DRIVEACquireretry--+-Forever-----+-----><
                    +-Never-----+
                    '-Anzahl_Versuche-'
```

## Parameter

---

### Forever

Die Anforderung eines Laufwerks wird so lange wiederholt, bis ein Laufwerk erfolgreich angefordert wurde. Dies ist der Standardwert.

### Never

Die Anforderung eines Laufwerks wird vom Server nicht wiederholt, und die Operation schlägt fehl.

### Anzahl\_Versuche

Gibt die maximale Anzahl der Versuche (1 bis 9999) durch den Server an, ein Laufwerk anzufordern.

## Beispiele

---

Angeben, dass der Server maximal 10 Mal versuchen soll, das Laufwerk anzufordern:

```
driveacquireretry 10
```

## ENABLENASDEDUP

---

Die Serveroption ENABLENASDEDUP gibt an, ob der Server Daten dedupliziert, die von einem NAS-Dateiserver gespeichert werden. Diese Option gilt nur für NetApp-Dateiserver.

Lautet der Wert dieser Option NO, werden die vom Dateiserver gespeicherten Daten während des Prozesses zum Identifizieren doppelter Daten übersprungen. Lautet der Wert dieser Option YES, muss der Parameter DEDUPLICATE in der Speicherpooldefinition den Wert YES haben.

## Syntax

---

```
>>-ENABLENASDEDUP--+-No--+------><
                    '-Yes-'
```

## Parameter

---

### Yes

Gibt an, dass der IBM Spectrum Protect-Server Daten dedupliziert, die von einem NetApp-Dateiserver gespeichert werden.

### No

Gibt an, dass der Server keine Daten dedupliziert, die von einem NetApp-Dateiserver gespeichert werden.

## Beispiel

---

Angeben, dass der Server Daten dedupliziert, die von einem NetApp-Dateiserver gespeichert werden.

```
enablenasdedup yes
```

## EVENTSERVER

---

Die Option EVENTSERVER gibt an, ob der Server beim Systemstart eine Verbindung zum Ereignisserver herstellen soll.

## Syntax

---

```
>>-EVENTSERVER--+-Yes-+-----><
      '-No--'
```

## Parameter

---

### Yes

Gibt an, dass der Server versucht, beim Systemstart eine Verbindung zum Ereignisserver herzustellen. Eine Verbindung kann nur hergestellt werden, wenn bereits ein Befehl DEFINE EVENTSERVER ausgegeben wurde. Dies ist der Standardwert.

### No

Gibt an, dass der Server nicht versucht, beim Systemstart eine Verbindung zum Ereignisserver herzustellen.

## Beispiele

---

```
eventserver yes
```

## EXPINTERVAL

---

Die Option EXPINTERVAL gibt das Intervall (in Stunden) an, in dem automatische Bestandsverfallsprozesse in IBM Spectrum Protect stattfinden. Beim Datenträgerbestandsverfall werden Clientsicherungs- und Archivierungsdateikopien aus dem Server gelöscht, und zwar wie von den Verwaltungsklassen angegeben, denen die Clientdateien zugeordnet sind. Findet nicht regelmäßig ein Datenträgerverfall statt, wird kein Speicherpoolbereich von abgelaufenen Clientdateien zurückgefordert, so dass für den Server mehr Speicherbereich benötigt wird, als für die Maßnahme eigentlich nötig wäre.

Der Datenträgerbestandsverfall kann auch über den Befehl EXPIRE INVENTORY gestartet werden. Durch den Datenträgerverfall wird Speicherbereich für weitere Clientsicherungs- und Archivierungsdateien in den Speicherpools verfügbar.

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

## Syntax

---

```
      .-24-----.
>>-EXPINterval--+-Stunden-+-----><
```

## Parameter

---

### Stunden

Gibt die Zeit in Stunden zwischen den automatischen Bestandsverfallsprozessen an. Es können 0 bis 336 Stunden (14 Tage) angegeben werden. Der Wert 0 bedeutet, dass der Datenträgerbestandsverfall mit dem Befehl EXPIRE INVENTORY gestartet werden muss. Der Standardwert ist 24.

## Beispiele

---

```
expinterval 5
```

## EXPQUIET

---

Die Option EXPQUIET gibt an, ob IBM Spectrum Protect detaillierte Nachrichten während der Verfallsverarbeitung sendet.

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

## Syntax

---

```
>>-EXPQUIet--+- --No--+-----><
      '- --Yes-'
```

## Parameter

---

### No

Gibt an, dass der Server ausführliche Nachrichten sendet. Dies ist der Standardwert.

Yes

Gibt an, dass der Server nur knappe Nachrichten sendet. Diese Nachrichten werden nur für Dateien gesendet, die aufgrund der Kopiergruppe in der Standardverwaltungsklasse oder aufgrund des für die Domäne gültigen Aufbewahrungszeitraums abgelaufen sind.

## Beispiele

---

```
expquiet no
```

 Linux-Betriebssysteme

## FASPBEGPORT

---

Die Option FASPBEGPORT gibt die Anfangsnummer des Bereichs von Anschlussnummern an, die für die Netzkommunikation mit der Aspera FASP-Technologie (Fast Adaptive Secure Protocol) verwendet werden.

Um den Bereich von Anschlussnummern zu definieren, geben Sie sowohl die Option FASPBEGPORT als auch die Option FASPENDDPORT an.

## Syntax

---

```
.-15100-----.  
>>-FASPBEGPort--+-Anfangsanschlussnummer+-----<<
```

## Parameter

---

Anfangsanschlussnummer

Gibt die Anfangsanschlussnummer für die Netzkommunikation mit der Aspera FASP-Technologie an. Der Standardwert ist 15100. Bitten Sie Ihren Netzadministrator um Unterstützung bei der Definition des Bereichs der Anschlussnummern:

- Wenn Sie das SSL-Protokoll (SSL = Secure Sockets Layer) für das Serverpaar nicht aktiviert haben, stellen Sie sicher, dass die Anschlüsse für TCP-Sockets (TCP = Transmission Control Protocol) verwendet werden können.
- Stellen Sie sicher, dass die Anschlüsse für UDP-Verbindungen (UDP = User Datagram Protocol) verwendet werden können.
- Stellen Sie sicher, dass die Anschlüsse mit Firewallregeln kompatibel sind.

## Beispiel

---

Wenn Firewallregeln erfordern, dass Anschlussnummern größer als 1800 sind, geben Sie als kleinste Anschlussnummer 1801 an:

```
faspbegport 1801
```

**Zugehörige Verweise:**

FASPENDDPORT

 Linux-Betriebssysteme

## FASPENDDPORT

---

Die Option FASPENDDPORT gibt die Endnummer des Bereichs von Anschlussnummern an, die für die Netzkommunikation mit der Aspera FASP-Technologie (Fast Adaptive Secure Protocol) verwendet werden.

Um den Bereich von Anschlussnummern zu definieren, geben Sie sowohl die Option FASPBEGPORT als auch die Option FASPENDDPORT an.

## Syntax

---

```
.-15199-----.  
>>-FASPENDDPort--+-Endanschlussnummer+-----<<
```

## Parameter

---

Endanschlussnummer

Gibt die Endanschlussnummer für die Netzkommunikation mit der Aspera FASP-Technologie an. Der Standardwert ist 15199. Bitte Sie Ihren Netzadministrator um Unterstützung bei der Definition des Bereichs der Anschlussnummern:

- Wenn Sie das SSL-Protokoll (SSL = Secure Sockets Layer) für das Serverpaar nicht aktiviert haben, stellen Sie sicher, dass die Anschlüsse für TCP-Sockets (TCP = Transmission Control Protocol) verwendet werden können.
- Stellen Sie sicher, dass die Anschlüsse für UDP-Verbindungen (UDP = User Datagram Protocol) verwendet werden können.
- Stellen Sie sicher, dass die Anschlüsse mit Firewallregeln kompatibel sind.

## Beispiel

---

Wenn Firewallregeln erfordern, dass Anschlussnummern kleiner als 1900 sind, geben Sie als größte Anschlussnummer 1899 an:

```
faspendport 1899
```

### Zugehörige Verweise:

FASPBEGPORT

 Linux-Betriebssysteme

## FASPTARGETRATE

---

Die Option FASPTARGETRATE gibt die Zielgeschwindigkeit für die Datenübertragung mit der Aspera FASP-Technologie (Fast Adaptive Secure Protocol) an. Mit der Angabe der Zielgeschwindigkeit begrenzen Sie die Bandbreite jeder Netzverbindung, die die Aspera FASP-Technologie verwendet. Auf diese Weise können Sie sicherstellen, dass genügend Bandbreite für alle Netzverbindungen verfügbar ist.

## Syntax

---

```
.-250000-----.  
>>-FaspTargetRate--+-Zielgeschwindigkeit+-----<<
```

## Parameter

---

### Zielgeschwindigkeit

Gibt die maximale Geschwindigkeit in Kb/s für die Datenübertragung während einer Sitzung an. Der Standardwert ist 250000. Sie können Werte im Bereich von 100 bis 100000000 angeben.

Beispiel: Wenn Sie den Befehl PROTECT STGPOOL ausgeben, um zwei parallele Operationen mit der Standardzielgeschwindigkeit auszuführen, überschreitet der Gesamtdurchsatz nicht 500.000 Kb/s. Wenn Ihr Dateisystem zwei Operationen zum Schützen von Speicherpools mit weit höheren Geschwindigkeiten als 500.000 Kb/s des Gesamtdurchsatzes unterstützen kann und genügend Netzbandbreite verfügbar ist, können Sie die Zielgeschwindigkeit erhöhen.

Um die entsprechende Zielgeschwindigkeit zu bestimmen, ziehen Sie Ihren Netzadministrator zu Rate.

## Beispiele

---

Wenn die zugewiesene Netzbandbreite 150.000 Kb/s beträgt, können Sie die Zielgeschwindigkeit auf 75.000 setzen und die Standardanzahl Sitzungen (zwei) für den Befehl PROTECT STGPOOL verwenden.

```
fasptargetrate 75000
```

Wenn in einer großen Blueprint-Konfiguration die zugewiesene Netzbandbreite 6.000.000 Kb/s beträgt, können Sie die Zielgeschwindigkeit auf 750.000 setzen und acht Sitzungen für den Befehl PROTECT STGPOOL verwenden.

```
fasptargetrate 750000
```

## FFDCLOGLEVEL

---

Die Option FFDCLOGLEVEL gibt den Typ von allgemeinen Servernachrichten an, die im FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) angezeigt werden.

Das FFDC-Protokoll enthält drei Kategorien von allgemeinen Servernachrichten. Die Definition der Option FFDCLOGLEVEL betrifft die folgenden Kategorien:

- FFDC\_GENERAL\_SERVER\_INFO
- FFDC\_GENERAL\_SERVER\_WARNING
- FFDC\_GENERAL\_SERVER\_ERROR



## Syntax

---

```
.-FFDCLOGLevel---ALL-----.  
>>+-FFDCLOGLevel---+ALL---+-----<<  
      +-WARN--+  
      '-ERRor-'
```

## Parameter

---

### ALL

Gibt an, dass alle allgemeinen FFDC-Serverprotokollnachrichten im Protokoll angezeigt werden. Dieser Wert ist der Standardwert.

### WARN

Gibt an, dass die Nachrichten FFDC\_GENERAL\_SERVER\_WARNING und FFDC\_GENERAL\_SERVER\_ERROR im Protokoll angezeigt werden.

### ERRor

Gibt an, dass nur die Nachrichten FFDC\_GENERAL\_SERVER\_ERROR im Protokoll angezeigt werden.

## Beispiel

---

```
ffdcloglevel warn
```

## FFDCLOGNAME

---

Die Option FFDCLOGNAME gibt einen Namen für das FFDC-Protokoll (FFDC = First-Failure Data Capture) an.

Die FFDC-Protokolldatei wird verwendet, um Diagnoseinformationen zum Server zu erfassen. Wenn ein Fehler auftritt, werden Daten zu dem Fehler in die FFDC-Protokolldatei geschrieben. Diese Informationen können dem IBM Support zur Fehlerdiagnose zur Verfügung gestellt werden. Die FFDC-Protokolldatei befindet sich im Serverinstanzverzeichnis.

## Syntax

---

```
.-dsmffdc.log-.  
>>-FFDCLOGNAME--+-Dateiname---+-----<<
```

## Parameter

---

### Dateiname

Gibt einen Dateinamen für die FFDC-Protokolldatei an. Der Dateiname kann ein vollständig qualifizierter Dateiname oder ein Dateiname sein, der sich auf das Serverinstanzverzeichnis bezieht. Der Standardwert ist dsmffdc.log.

## Beispiele

---

```
ffdclogname /tsminst1/tsmffdc.log  
ffdclogname tsmffdc.log  
ffdclogname c:\tsmserv1\tsmffdc.log
```

### Zugehörige Verweise:

FFDCMAXLOGSIZE  
FFDCNUMLOGS

## FFDCMAXLOGSIZE

---

Die Option FFDCMAXLOGSIZE gibt die Größe für die FFDC-Protokolldatei (FFDC = First-Failure Data Capture) an.

Die FFDC-Protokolldatei wird verwendet, um Diagnoseinformationen zum Server zu erfassen. Wenn ein Fehler auftritt, werden Daten zu dem Fehler in die FFDC-Protokolldatei geschrieben. Diese Informationen können dem IBM Support zur Fehlerdiagnose zur Verfügung gestellt werden.

## Syntax

---

```
.-1024-----.  
>>-FFDCMAXLOGSIZE--+-Kilobyte+-----><
```

## Parameter

---

### Kilobyte

Gibt die maximale Größe für die FFDC-Protokolldatei an, bevor ein Umlauf erfolgt. Der Mindestwert ist 500. Der Maximalwert ist 2097151. Der Standardwert ist 1024.

Soll die Größe der Protokolldatei unendlich sein, geben Sie den Wert -1 an. Um das Protokoll zu inaktivieren, geben Sie 0 an.

## Beispiele

---

```
ffdcmaxlogsize 2000
```

### Zugehörige Verweise:

FFDCLOGNAME  
FFDCNUMLOGS

## FFDCNUMLOGS

---

Die Option FFDCNUMLOGS gibt die Anzahl der Protokolldateien an, die für die Umlaufprotokollierung verwendet werden können. Der Standardwert ist 10.

Die Umlaufprotokollierung verwendet einen Protokolldateiring, um eine Wiederherstellung nach Transaktionsfehlern und Systemabstürzen bereitzustellen. Wenn beispielsweise die Datei dsmffdc.log voll ist, wird sie in dsmffdc.log.1 umbenannt. Ist eine Datei dsmffdc.log.1 vorhanden, wird die Datei dsmffdc.log.1 in dsmffdc.log.2 umbenannt. Ist eine Datei dsmffdc.log.2 vorhanden, wird die Datei dsmffdc.log.2 in dsmffdc.log.3 umbenannt. Dies wird fortgesetzt, bis der Wert für FFDCNUMLOGS erreicht wird. Wird eine Protokolldatei umbenannt, wenn der Wert für FFDCNUMLOGS erreicht ist, wird diese Protokolldatei gelöscht.

Der Mindestwert ist 1. Der Maximalwert ist 100. Der Standardwert ist 10.

## Syntax

---

```
.-10---.  
>>-FFDCNUMLOGS--+-Wert+-----><
```

## Parameter

---

### Wert

Gibt die Anzahl der Protokolldateien an, die für die Umlaufprotokollierung verwendet werden.

Wird der Wert 1 angegeben und erreicht die Protokolldateigröße den Wert für FFDCMAXLOGSIZE, schreibt der Server weiter in die Protokolldatei. Alle Protokolldaten werden überschrieben und der Server schreibt weiter in die Protokolldatei.

## Beispiele

---

```
ffdcnumlogs 20
```

## FILEEXIT

---

Die Option FILEEXIT gibt eine Datei an, an die aktivierte Ereignisse weitergeleitet werden. Jedes protokollierte Ereignis ist ein Satz in der Datei.

## Syntax

---

```
>>-FILEEXIT--+-No---Dateiname---REPLACE---><  
          '-Yes-'                  +-APPEND---+
```


## Parameter

---

- Yes**  
Gibt an, dass das Ereignisprotokoll für den Dateiausgangsempfänger automatisch beim Serverstart gestartet wird.
- No**  
Gibt an, dass das Ereignisprotokoll für den Dateiausgangsempfänger nicht automatisch beim Serverstart gestartet wird. Wurde dieser Parameter angegeben, muss das Ereignisprotokoll manuell durch Eingabe des Befehls `BEGIN EVENTLOGGING` gestartet werden.
- Dateiname**  
Gibt den Namen der Datei an, in der die Ereignisse gespeichert werden.
- REPLACE**  
Gibt an, dass die Datei überschrieben wird, falls sie bereits vorhanden ist.
- APPEND**  
Gibt an, dass die Daten an die Datei angefügt werden, falls die Datei bereits vorhanden ist.
- PRESERVE**  
Gibt an, dass die Datei nicht überschrieben wird, falls sie bereits vorhanden ist.

## Beispiele

---

 Windows-Betriebssysteme

```
fileexit yes \tsm\server\data replace
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

```
fileexit yes /tsm/server/data replace
```

## FILETEXTEXIT

---

Die Option FILETEXTEXIT gibt eine Datei an, an die aktivierte Ereignisse weitergeleitet werden. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.

## Syntax

---

```
>>-FILETEXTEXIT--+-No---Dateiname--+-REPLACE---+-----<<  
                '-Yes-'                +-APPEND---+  
                                         '-PRESERVE-'
```

## Parameter

---

- Yes**  
Gibt an, dass das Ereignisprotokoll für den Dateiausgangsempfänger automatisch beim Serverstart gestartet wird.
- No**  
Gibt an, dass das Ereignisprotokoll für den Dateiausgangsempfänger nicht automatisch beim Serverstart gestartet wird. Wurde dieser Parameter angegeben, muss das Ereignisprotokoll manuell durch Eingabe des Befehls `BEGIN EVENTLOGGING` gestartet werden.
- Dateiname**  
Gibt den Namen der Datei an, in der die Ereignisse gespeichert werden.
- REPLACE**  
Gibt an, dass die Datei überschrieben wird, falls sie bereits vorhanden ist.
- APPEND**  
Gibt an, dass die Daten an die Datei angefügt werden, falls die Datei bereits vorhanden ist.
- PRESERVE**  
Gibt an, dass die Datei nicht überschrieben wird, falls sie bereits vorhanden ist.

## Beispiele

---

 Windows-Betriebssysteme

```
filetextexit yes \tsm\server\data replace
```

## FSUSEDTHRESHOLD

---

Die Option FSUSEDTHRESHOLD gibt den Prozentsatz des Dateisystems an, der von der Datenbank ausgefüllt werden kann, bevor eine Alernachricht ausgegeben wird.

Sie können diese Serveroption aktualisieren, ohne den Server zu stoppen und erneut zu starten, indem Sie den Befehl SETOPT verwenden.

Wird dieser Wert auf eine niedrige Zahl gesetzt, kann das Aktivitätenprotokoll mit Nachrichten überschwemmt werden, die angeben, dass der Datenbankbereich ausgefüllt ist, auch wenn noch Speicherbereich verfügbar ist. Wird der Wert zu hoch definiert, kann der Datenbankbereich ausgefüllt sein, bevor Sie dem Dateisystem weiteren Speicherbereich hinzufügen können.

### Syntax

---

```
>>-FSUSEDThreshhold--Prozent-----><
```

### Parameter

---

Prozent

Gibt den Wert des verwendeten Speicherbereichs in der Datenbank an. Es kann ein Wert von 0 bis 100 angegeben werden. Der Standardwert ist 90.

### Beispiele

---

```
fsusedthreshold 70
```

## IDLETIMEOUT

---

Die Option IDLETIMEOUT gibt die Zeit in Minuten an, die eine Clientsitzung inaktiv sein kann, bevor der Server die Sitzung abbricht. Sie können den Wert für das Zeitlimit erhöhen, damit bei hoher Netzauslastung in Ihrer Umgebung keine Zeitlimitüberschreitung bei den Clients auftritt. Beachten Sie jedoch, dass bei einer großen Anzahl von inaktiven Sitzungen andere Benutzer möglicherweise keine Verbindung zu dem Server herstellen können.

Die Serveroption IDLETIMEOUT wird für Sitzungen verwendet, die keine Verwaltungssitzungen sind. Für Verwaltungsclientsitzungen siehe die Option ADMINIDLETIMEOUT.

Sie können diese Serveroption aktualisieren, ohne den Server zu stoppen und erneut zu starten, indem Sie den Befehl SETOPT verwenden.

### Syntax

---

```
.-15-----.  
>>-IDLETimeout--+-Minuten+-----><
```

### Parameter

---

Minuten

Gibt die maximale Anzahl Minuten an, die ein Server auf einen inaktiven Client wartet. Der Standardwert ist 15 Minuten. Der Mindestwert ist 1 Minute.

### Beispiele

---

```
idletimeout 15
```

## KEEPALIVE

---

Die Option KEEPALIVE gibt an, ob die TCP-Keepalive-Funktion (TCP = Transmission Control Protocol) für abgehende TCP-Sockets aktiviert ist. Die TCP-Keepalive-Funktion sendet eine Übertragung von einer Einheit zu einer anderen Einheit, um zu überprüfen, ob die Verbindung zwischen den beiden Einheiten betriebsbereit ist.

Bei Verwendung der Knotenreplikation können Sie die Option KEEPALIVE auf dem Quellenreplikationsserver verwenden, um die TCP-Keepalive-Funktion zu aktivieren. Die Option KEEPALIVE ist auf dem Zielreplikationsserver nur erforderlich, wenn Sie die bidirektionale Replikation angeben. In diesem Fall wird der Zielsever zum Quellenreplikationsserver.

## Syntax

---

```
.-Yes-.  
>>-KEEPALIVE--+No--+-----<
```

## Parameter

---

### Yes

Gibt an, dass die TCP-Keepalive-Funktion für abgehende TCP-Sockets aktiviert ist. Dieser Wert ist der Standardwert. Wenn die Option KEEPALIVE aktiviert ist, werden für die Optionen KEEPALIVETIME und KEEPALIVEINTERVAL Standardwerte verwendet.

### No

Gibt an, dass die TCP-Keepalive-Funktion für abgehende TCP-Sockets nicht aktiviert ist. Wenn Sie den Wert NO angeben, hat dies keine Auswirkungen auf aktuelle TCP-Socketverbindungen, die von Anforderungen für abgehende Verbindungen stammen, während die Option KEEPALIVE auf YES gesetzt war. Der Wert YES gilt für diese Sockets, bis die zugehörige Sitzung beendet und das Socket geschlossen wird.

## Beispiel

---

Verwenden Sie den Befehl SETOPT, um die Keepalive-Funktion zu aktivieren, ohne den Server zu inaktivieren oder anzuhalten:

```
setopt keepalive yes
```

### Zugehörige Verweise:

KEEPALIVEINTERVAL  
KEEPALIVETIME

## KEEPALIVETIME

---

Die Option KEEPALIVETIME gibt an, wie oft TCP eine Keepalive-Übertragung sendet, wenn eine Antwort empfangen wird. Diese Option gilt nur, wenn die Option KEEPALIVE auf YES gesetzt wurde.

## Syntax

---

```
.-300-----.  
>>-KEEPALIVETIME--+Sekunden+-----<
```

## Parameter

---

### Sekunden

Gibt an, wie oft TCP Keepalive-Übertragungen sendet, um zu prüfen, ob eine inaktive Verbindung noch aktiv ist. Der Wert wird in Sekunden angegeben.

Sie können einen Wert im Bereich von 1 bis 4294967 angeben. Der Standardwert ist 300 (5 Minuten).

## Beispiel

---

Die Option KEEPALIVETIME auf 120 Sekunden setzen:

```
keepalivetime 120
```

### Zugehörige Verweise:

KEEPALIVE  
KEEPALIVEINTERVAL

## KEEPALIVEINTERVAL

Die Option KEEPALIVEINTERVAL gibt an, wie oft eine Keepalive-Übertragung gesendet wird, wenn keine Antwort empfangen wird. Diese Option gilt nur, wenn die Option KEEPALIVE auf YES gesetzt wurde.

### Syntax

```
                .-30-----.  
>>-KEEPALIVEINTERVAL--+--Sekunden--+-----<<
```

### Parameter

Sekunden

Gibt die Zeit in Sekunden zwischen Keepalive-Übertragungen an, wenn keine Antwort empfangen wird. Der Wert wird in Sekunden angegeben.

Sie können einen Wert im Bereich von 1 bis 4294967 angeben. Der Standardwert ist 30 Sekunden.

### Beispiel

Die Option KEEPALIVEINTERVAL auf 45 Sekunden setzen:

```
keepaliveinterval 45
```

#### Zugehörige Verweise:



KEEPALIVE


KEEPALIVETIME

## LANGUAGE

Die Option LANGUAGE steuert die Initialisierung von länderspezifischen Angaben. Die länderspezifischen Angaben enthalten unter anderem die Landessprache sowie die Datums-, Uhrzeit- und Zahlenformate, die für die Konsole und den Server verwendet werden sollen.

Werden Ihr Client und Ihr Server in unterschiedlichen Sprachen ausgeführt, sind die generierten Nachrichten möglicherweise nicht verständlich, wenn Nachrichten vom Client an den Server ausgegeben werden oder wenn der Server eine Ausgabe an den Client sendet.

 AIX-Betriebssysteme  Linux-Betriebssysteme Kann die Locale nicht initialisiert werden, verwendet der Server standardmäßig amerikanisches Englisch.

 Windows-Betriebssysteme Kann die Ländereinstellung nicht initialisiert werden, verwendet der Server standardmäßig amerikanisches Englisch und die mit den Serveroptionen DATEFORMAT, TIMEFORMAT und NUMBERFORMAT definierten Formate für Datum, Uhrzeit und Zahlen.

### Syntax

```
                (1)  
>>-LANGuage--+--AMENG-----<<  
                |                |  
                |                | (2) |  
                +-en_US-----+  
                |                | (3) |  
                '-Länderspezifische_Angaben-----'
```

Anmerkungen:



1. AMENG ist nur unter HP-UX, Solaris und Windows verfügbar.
2. en\_US ist nur unter AIX und Linux verfügbar.
3. Die *Ländereinstellung* ist nur unter AIX, HP-UX, Solaris, Linux und Windows verfügbar.

### Parameter

 Windows-Betriebssysteme AMENG

 Windows-Betriebssysteme Gibt an, dass amerikanisches Englisch als Standardsprache für den Server verwendet wird.

 AIX-Betriebssysteme  Linux-Betriebssysteme en\_US

  Gibt an, dass amerikanisches Englisch als Standardsprache für den Server verwendet wird.

Länderspezifische\_Angaben

Gibt den Namen der vom Server unterstützten Ländereinstellung an. Die folgenden Tabellen enthalten Informationen zu den unterstützten länderspezifischen Angaben nach Betriebssystem.

Anmerkung: IBM Spectrum Protect kann in jeder Locale ausgeführt werden, der Standardwert ist jedoch amerikanisches Englisch. Für die aufgelisteten Locales steht Sprachunterstützung zur Verfügung.



Tabelle 1. Serversprachen für AIX

| <b>Sprache</b>  | <b>Wert der Option LANGUAGE</b> |
|---|---------------------------------|
| Chinesisch, vereinfacht   | zh_CN                           |
| Chinesisch, vereinfacht   | Zh_CN                           |
| Chinesisch, vereinfacht (UTF-8)   | ZH_CN                           |
| Chinesisch, traditionell (Big5)   | Zh_TW                           |
| Chinesisch, traditionell (UTF-8)  | ZH_TW                           |
| Chinesisch, traditionell (euc_tw)   | zh_TW                           |
| Englisch  | en_US                           |
| Englisch (UTF-8)  | EN_US                           |
| Französisch   | fr_FR                           |
| Französisch (UTF-8)   | FR_FR                           |
| Deutsch   | de_DE                           |
| Deutsch (UTF-8)   | DE_DE                           |
| Italienisch   | it_IT                           |
| Italienisch (UTF-8)   | IT_IT                           |
| Japanisch, EUC  | ja_JP                           |
| Japanisch, PC   | Ja_JP                           |
| Japanisch, UTF8   | JA_JP                           |
| Koreanisch  | ko_KR                           |
| Koreanisch (UTF-8)  | KO_KR                           |
| Portugiesisch, Brasilien  | pt_BR                           |
| Portugiesisch, Brasilianisch (UTF-8)  | PT_BR                           |
| Russisch  | ru_RU                           |
| Russisch (UTF-8)  | RU_RU                           |
| Spanisch  | es_ES                           |
| Spanisch (UTF-8)  | ES_ES                           |
| Anmerkung: Für das System muss die Unterstützung der Umgebung en_US installiert sein. |                                 |

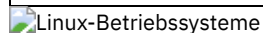


Tabelle 2. Serversprachen für Linux

| <b>LANGUAGE</b>              | <b>Wert der Option LANGUAGE</b> |
|------------------------------|---------------------------------|
| Chinesisch, vereinfacht      | zh_CN                           |
|                              | zh_CN.gb18030                   |
|                              | zh_CN.utf8                      |
| Chinesisch, traditionell     | Big5 / Zh_TW                    |
|                              | zh_TW                           |
|                              | zh_TW.utf8                      |
| Englisch, Vereinigte Staaten | en_US                           |

| LANGUAGE                 | Wert der Option LANGUAGE |
|--------------------------|--------------------------|
|                          | en_US.utf8               |
| Französisch              | fr_FR                    |
|                          | fr_FR.utf8               |
| Deutsch                  | de_DE                    |
|                          | de_DE.utf8               |
| Italienisch              | it_IT                    |
|                          | it_IT.utf8               |
| Japanisch                | ja_JP                    |
|                          | ja_JP.utf8               |
| Koreanisch               | ko_KR                    |
|                          | ko_KR.utf8               |
| Portugiesisch, Brasilien | pt_BR                    |
|                          | pt_BR.utf8               |
| Russisch                 | ru_RU                    |
|                          | ru_RU.utf8               |
| Spanisch                 | es_ES                    |
|                          | es_ES.utf8               |


 Windows-Betriebssysteme

Tabelle 3. Serversprachen für Windows

| Sprache                  | Wert der Option LANGUAGE |
|--------------------------|--------------------------|
| Chinesisch, vereinfacht  | chs                      |
| Chinesisch, traditionell | cht                      |
| Englisch                 | ameng                    |
| Französisch              | fra                      |
| Deutsch                  | deu                      |
| Italienisch              | ita                      |
| Japanisch                | jpn                      |
| Koreanisch               | kor                      |
| Portugiesisch, Brasilien | ptb                      |
| Russisch                 | rus                      |
| Spanisch                 | esp                      |

## Beispiele

 AIX-Betriebssysteme  Linux-Betriebssysteme

```
lang ja_JP
```

 Windows-Betriebssysteme

```
lang jpn
```

## LDAPCACHEDURATION

Die Option LDAPCACHEDURATION bestimmt die Zeit, die der IBM Spectrum Protect-Server Informationen zur LDAP-Kennwortauthentifizierung zwischenspeichert.

Nach einer erfolgreichen LDAP-Bindung bestimmt der eingegebene Wert die Zeit, die Informationen zum LDAP-Verzeichnisserver verfügbar bleiben. Je höher der Wert ist, desto besser ist die Leistung des LDAP-Verzeichnisseservers. Während der Cache-Periode werden



Änderungen auf dem LDAP-Verzeichnisserver jedoch nicht sofort auf dem Knoten wirksam. Beispielsweise können alte Kennwörter für einige Zeit vorhanden sein, nachdem sie auf dem LDAP-Server geändert oder gesperrt wurden.

Schließen Sie die Option LDAPCACHEDURATION in einen Befehl SETOPT ein, damit die Option sofort wirksam wird.

Einschränkung: Die Option LDAPCACHEDURATION gilt nicht für Speicheragenten.

## Syntax

---

```
>>-LDAPCACHEDURATION--Minuten-----><
```

## Parameter

---

Minuten

Gibt die Höchstdauer nach einer erfolgreichen LDAP-Bindung an, während der nachfolgende Sitzungen für denselben Knoten oder Administrator sekundäre LDAP-Bindungsoperationen überspringen. Die Werte befinden sich im Bereich von 0 bis 360 Minuten.

## Beispiel: Den Wert für LDAPCACHEDURATION auf 6 Stunden setzen (Maximum)

---

Geben Sie in der Datei dsmserv.opt den folgenden Wert an:

```
ldapcacheduration 360
```

Nachdem sich ein Knoten oder Administrator mit einem externen Verzeichnisserver authentifiziert hat, wird die LDAP-Bindung für alle Sitzungen für 360 Minuten übersprungen.

## LDAPURL

---

Die Option LDAPURL gibt die Position Ihres Lightweight Directory Access Protocol-Servers (LDAP-Servers) an. Definieren Sie die Option LDAPURL nach der Konfiguration des LDAP-Servers.

Tipp: Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.

Es gelten die folgenden Einschränkungen:

- Die Option LDAPURL kann nicht in Kombination mit dem Befehl SETOPT verwendet werden.
- Die Option LDAPURL gilt nicht für Speicheragenten.

## Syntax

---

```
>>-LDAPURL--Wert_für_LDAP_URL-----><
```

## Parameter

---

Wert\_für\_LDAP\_URL

Gibt die URL eines einzelnen LDAP-Servers oder die URLs mehrerer LDAP-Server an. Sie können mehrere Werte eingeben. Dabei kann jeder URL-Wert maximal 1024 Zeichen umfassen. Die Anschlussnummer ist optional und nimmt standardmäßig den Wert 389 an. Jeder URL-Wert muss einen LDAP-Servernamen enthalten. Beispielsweise ist das Format des Servernamens `server1.storage.us.ibm.com` und der LDAP-Anschluss ist 341. Der Wert der Option LDAPURL muss den folgenden Spezifikationen entsprechen:

- Wenn Sie mehrere URLs angeben, muss sich jede URL in einer separaten Zeile befinden.
- Wenn Sie mehrere URLs angeben, muss jede URL auf ein anderes externes Verzeichnis zeigen und alle externen Verzeichnisse müssen dieselben Daten enthalten.
- Jede URL muss mit `ldap://` beginnen.  
Einschränkung: Die URL, die Sie angeben, darf nicht mit `ldaps://` beginnen.

IBM Spectrum Protect unterstützt LDAP-Verbindungen, die mit der LDAPv3-Standardoperation StartTLS geschützt werden. Mit dieser Operation wird ein sicherer TLS-Austausch (TLS = Transport Layer Security) über eine vorhandene LDAP-Verbindung eingerichtet. Mit der LDAP-Operation Simple Bind, die von IBM Spectrum Protect verwendet wird, wird das Kennwort beim Senden nicht geschützt. Eine sichere TLS-Verbindung ist erforderlich, um das Kennwort zu schützen.

## Beispiel: Anschlusswert für einen LDAP-Server definieren

---

In der Datei dmserv.opt den Anschlusswert 341 für einen LDAP-Server angeben:

```
ldapurl ldap://server1.storage.us.ibm.com:341/dc=storage,dc=us,dc=ibm,dc=com
```

## MAXSESSIONS

---

Die Option MAXSESSIONS gibt die maximal zulässige Anzahl gleichzeitig stattfindender Clientsitzungen für den Server an.

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

### Syntax

---

```
                .-25-----.  
>>-MAXSessions--+-Anzahl_Sitzungen+-----<<
```

### Parameter

---

Anzahl\_Sitzungen

Gibt die maximal zulässige Anzahl gleichzeitig stattfindender Clientsitzungen an. Der Standardwert ist 25 Clientsitzungen. Der Mindestwert ist zwei Clientsitzungen. Der Maximalwert wird nur durch die Größe des verfügbaren virtuellen Speichers oder Übertragungsressourcen begrenzt.

### Beispiele

---

```
maxsessions 25
```

## MESSAGEFORMAT

---

Die Option MESSAGEFORMAT gibt an, ob eine Nachrichtennummer in allen Zeilen angezeigt wird, wenn sich die Nachricht über mehrere Zeilen erstreckt.

### Syntax

---

```
>>-MESsageformat--Zahl-----<<
```

### Parameter

---

Zahl

Eine Zahl auswählen, um anzugeben, ob eine Nachrichtennummer nur in der ersten Zeile einer mehrzeiligen Nachricht oder in allen Zeilen angezeigt werden soll.

1

Die Nachrichtennummer wird nur in der ersten Zeile einer Nachricht angezeigt. Dies ist der Standardwert.

2

Die Nachrichtennummer wird in jeder Nachrichtenzeile angezeigt.

### Beispiele

---

```
messageformat 2
```

## MIRRORLOGDIRECTORY

---

Die Option MIRRORLOGDIRECTORY gibt das Verzeichnis zum Spiegeln des Pfads für aktive Protokolldateien an.

Alle Änderungen, die am Verzeichnis für aktive Protokolldateien vorgenommen werden, werden auch in dieses Spiegelverzeichnis geschrieben. Diese Option wird an die Optionsdatei angehängt, wenn der Befehl DSMSERV FORMAT ausgeführt wird. Normalerweise muss das Verzeichnis nicht geändert werden.

## Syntax

---

```
>>-MIRRorlogdirectory--Verzeichnisname-----<<
```

## Parameter

---

### Verzeichnisname

Gibt einen vollständig qualifizierten Verzeichnisnamen für den Spiegel der aktiven Protokolldatei an. Die maximale Anzahl Zeichen beträgt 175.

## Beispiele

---

```
mirrorlogdirectory /tsm/mirrorlog
```



```
mirrorlogdirectory c:\tsmserv1\mirrorlog
```

## MOVEBATCHSIZE

---

Die Option MOVEBATCHSIZE gibt die Anzahl Clientdateien an, die innerhalb derselben Servertransaktion als Stapel gruppiert und versetzt werden sollen. Dieses Versetzen von Daten resultiert aus Speicherpoolsicherungen und -zurückschreibungen, Umlagerungsoperationen, Wiederherstellungsoperationen und MOVE DATA-Operationen. Diese Option arbeitet zusammen mit der Option MOVESIZETHRESH.

## Syntax

---

```
                  .-1000-----.  
>>-MOVEBatchsize--+-Anzahl_Dateien+-----<<
```

## Parameter

---

### Anzahl\_Dateien

Gibt eine Anzahl Dateien zwischen 1 und 1000 an. Der Standardwert ist 1000.

## Beispiele

---

```
movebatchsize 100
```

## MOVESIZETHRESH

---

Die Option MOVESIZETHRESH gibt den Grenzwert für die Datenmenge an (in Megabyte), die innerhalb derselben Servertransaktion als Stapel versetzt werden soll. Wenn diese Schwelle erreicht ist, werden dem aktuellen Stapel keine weiteren Dateien hinzugefügt. Nachdem der aktuelle Stapel versetzt wurde, wird eine neue Transaktion gestartet.

## Syntax

---

```
                  .-4096-----.  
>>-MOVESizethresh--+- Megabyte+-----<<
```

## Parameter

---

### Megabyte

Gibt die Anzahl Megabyte als ganze Zahl von 1 bis 32768 an. Der Standardwert ist 4096. Diese Option wird mit der Option MOVEBATCHSIZE verwendet.

## Beispiele

---

## MSGINTERVAL

---

Die Option MSGINTERVAL gibt die Zeit in Minuten zwischen Nachrichten an, in denen ein Bediener zum Einlegen eines Bands für den Server aufgefordert wird.

### Syntax

---

```
.-1-----.  
>>-MSGINTERval--+-Minuten+-----><
```

### Parameter

---

#### Minuten

Gibt das Zeitintervall an, in dem der Operator vom Server dazu aufgefordert wird, ein Band einzulegen. Der Standardwert ist 1 Minute. Der Mindestwert ist 1 Minute.

### Beispiele

---

```
msginterval 2
```

 Windows-Betriebssysteme

## NAMEDPIPENAME

---

Die Option NAMEDPIPENAME gibt eine Übertragungsmethode an, mit der Prozesse miteinander kommunizieren können, ohne wissen zu müssen, wo sich die Send- und Empfangsprozesse befinden. Der Name fungiert als Aliasname und verbindet die beiden Prozesse unabhängig davon, ob sie sich auf demselben Rechner oder in verbundenen Domänen befinden.

### Syntax

---

```
>>-NAMEPipename--Name-----><
```

### Parameter

---

#### Name

Gibt die benannten Pipes an, die der Server verwenden soll. Benannte Pipes eignen sich besonders für eine Umgebung, in der sich Client und Server auf derselben Maschine befinden. In diesem Fall wird nämlich keine DFV-Software und keine Konfiguration benötigt.

### Beispiele

---

```
namedpipename \\.\PIPE\TSMPIPE
```

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## NDMPCONNECTIONTIMEOUT

---

Die Serveroption NDMPCONNECTIONTIMEOUT gibt die Zeit in Stunden an, die der IBM Spectrum Protect-Server auf den Empfang von Statusaktualisierungen während der Ausführung von NDMP-Zurückschreibungsoperationen über das LAN wartet. NDMP-Zurückschreibungsoperationen mit großen NAS-Dateisystemen können einen langen Inaktivitätszeitraum aufweisen. Der Standardwert ist 6 Stunden.

### Syntax

---

```
.-6-----.  
>>-NDMPCONNECTIONTIMEOUT--+-Stunden+-----><
```

## Parameter

---

### Stunden

Die Anzahl der Stunden, die der IBM Spectrum Protect-Server auf den Empfang von Statusaktualisierungen während der Ausführung einer NDMP-Zurückschreibungsoperation über das LAN wartet. Der Standardwert ist 6. Der Mindestwert ist 1 Stunde. Der maximale Wert ist 48 Stunden.

## Beispiel

---

Geben Sie ein Zeitlimit von 10 Stunden an, bevor eine Zeitlimitüberschreitung für die NDMP-Verbindung auftritt:

```
ndmpconnectiontimeout 10
```

## NDMPCONTROLPORT

---

Die Option NDMPCONTROLPORT gibt die Anschlussnummer an, die für interne Übertragungen für bestimmte NDMP-Operationen (NDMP = Network Data Management Protocol) verwendet werden soll. Der IBM Spectrum Protect-Server arbeitet nicht als allgemeiner NDMP-Bandservice.

## Syntax

---

```
                .-10000-----.  
>>-NDMPControlport--+Anschlussnummer-+-----<<
```

## Parameter

---

### Anschlussnummer

Die Anschlussnummer, die für interne Übertragungen für bestimmte NDMP-Operationen verwendet werden soll. Die Anschlussnummer muss zwischen 1024 und 32767 liegen. Der Standardwert ist 10000.

## Beispiele

---

```
ndmpcontrolport 9999
```

## NDMPENABLEKEEPALIVE

---

Die Serveroption NDMPENABLEKEEPALIVE gibt an, ob der IBM Spectrum Protect-Server TCP-Keepalive (TCP = Transmission Control Protocol) für NDMP-Steuerverbindungen (NDMP = Network Data Management Protocol) zu NAS-Einheiten (NAS = Network-attached Storage) aktiviert. Der Standardwert ist NO.

TCP-Keepalive wird innerhalb der Netzunterstützung eines Betriebssystems implementiert. Mit TCP-Keepalive wird verhindert, dass eine lange laufende inaktive Verbindung von Firewall-Software geschlossen wird, die inaktive Verbindungen erkennt und schließt.

Einschränkung: Um Fehler zu verhindern, darf TCP-Keepalive in bestimmten Typen von Umgebungen nicht aktiviert werden. Ein Beispiel sind Umgebungen, die keine Firewall zwischen dem IBM Spectrum Protect-Server und einer NAS-Einheit haben. Ein anderes Beispiel sind Umgebungen mit Firewalls, die lange laufende inaktive Verbindungen tolerieren. Die Aktivierung von TCP-Keepalive in diesem Typ von Umgebung kann zur Folge haben, dass eine inaktive Verbindung versehentlich geschlossen wird, wenn der Verbindungspartner vorübergehend nicht auf TCP-Keepalive-Pakete antwortet.

## Syntax

---

```
>>-NDMPENABLEKEEPALIVES--+NO--+-----<<  
                '-YES-'
```

## Parameter

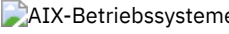

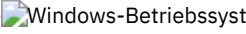
---

### NO

TCP-Keepalive für alle NDMP-Steuerverbindungen inaktivieren. NO ist der Standardwert.

### YES

TCP-Keepalive für alle NDMP-Steuerverbindungen aktivieren. Die Standardleerlaufzeit, bevor das erste TCP-Keepalive-Paket gesendet wird, beträgt 120 Minuten.



   Um die Leerlaufzeit zu ändern, verwenden Sie die Serveroption NDMPKEEPIDLEMINUTES.

## Beispiel

---

TCP-Keepalive für alle NDMP-Steuerverbindungen aktivieren, damit inaktive NDMP-Verbindungen nicht geschlossen werden:

```
ndmpenablekeepalive yes
```

## NDMPKEEPIDLEMINUTES

---

Die Serveroption NDMPKEEPIDLEMINUTES gibt die Zeit in Minuten an, bevor das Betriebssystem das erste TCP-Keepalive-Paket (TCP = Transmission Control Protocol) für eine NDMP-Steuerverbindung (NDMP = Network Data Management Protocol) überträgt. Der Standardwert ist 120 Minuten.

Voraussetzung: Verwenden Sie diese Option nur nach dem Definieren des Werts YES für die Serveroption NDMPENABLEKEEPALIVES.

## Syntax

---

```
                .-120-----.  
>>-NDMPKEEPIDLEMINUTES--+-Minuten+-----<<
```

## Parameter

---

Minuten

Die Anzahl der Minuten der Inaktivität für NDMP-Steuerverbindungen, bevor TCP-Keepalive-Pakete übertragen werden. Der Standardwert ist 120. Der Mindestwert ist 1 Minute. Der maximale Wert ist 600 Minuten.

## Beispiel

---

Eine Leerlaufzeit von 15 Minuten angeben, bevor das erste TCP-Keepalive-Paket gesendet wird:

```
ndmpkeepidleminutes 15
```

## NDMPPORTRANGE

---

Die Option NDMPPORTRANGE gibt den Bereich der Anschlussnummern an, in dem IBM Spectrum Protect navigiert, um eine Anschlussnummer zum Akzeptieren einer Sitzung von einer NAS-Einheit für die Datenübertragung zu erhalten. Der Standardwert 0,0 bedeutet, dass IBM Spectrum Protect einen Anschluss vom Betriebssystem zur Verfügung stellen lässt (ephemerer Anschluss).

Sind alle angegebenen Anschlüsse belegt, wenn eine NAS-Einheit versucht, die Verbindung zum Server herzustellen, schlägt die Operation fehl. Wird eine einzelne Anschlussnummer ausgewählt (kein Komma und keine Anschlussnummer für den oberen Wert), ist der Standardwert für die obere Anschlussnummer die untere Anschlussnummer plus 100.

Werden NDMP-Daten (NDMP = Network Data Management Protocol) an einen nativen IBM Spectrum Protect-Pool übertragen, kann die Übertragung entweder von den NDMP-Systemen oder vom IBM Spectrum Protect-Server eingeleitet werden. Wenn eine Firewall den Server und die NAS-Einheiten trennt, kann es erforderlich sein, Anschlussnummern in Firewallregeln anzugeben, damit der Datenverkehr zu und von den NAS-Einheiten fließen kann. NAS-Einheiten teilen dem IBM Spectrum Protect-Server die Anschlussnummern mit, die sie verwenden, wenn der Server angesprochen wird. Die Anschlussnummern des Servers werden durch die NDMPPortrange-Optionen gesteuert. Die Steuerung der Anschlussnummern für NAS-Einheiten ist lieferantenspezifisch. Lesen Sie in der Dokumentation des Lieferanten.

## Syntax

---

```
>>-NDMPPortrange----->  
>--untere_Anschlussnummer+-----+-----<<  
                ',Obere_Anschlussnummer-'
```

## Parameter

---

untere\_Anschlussnummer

Die untere Anschlussnummer, bei der IBM Spectrum Protect mit der Navigation beginnt, wenn eine Anschlussnummer zum Akzeptieren einer Sitzung von einer NAS-Einheit für die Datenübertragung benötigt wird. Der Mindestwert für die Anschlussnummer ist 1024.

Obere\_Anschlussnummer

Die obere Anschlussnummer, bis zu der IBM Spectrum Protect navigieren kann, wenn eine Anschlussnummer zum Akzeptieren einer Sitzung von einer NAS-Einheit für die Datenübertragung benötigt wird. Der Maximalwert für die Anschlussnummer ist 32767. Die obere Anschlussnummer muss mit der unteren Anschlussnummer übereinstimmen oder höher als die untere Anschlussnummer sein.

## Beispiele

---

Angeben, dass IBM Spectrum Protect im Anschlussnummernbereich 1024 - 2024 navigieren kann.

```
ndmportrange 1024,2024
```

## NDMPREFDATAINTERFACE

---

Diese Option gibt die IP-Adresse an, die der Schnittstelle zugeordnet ist, in der der Server alle NDMP-Sicherungsdaten (NDMP = Network Data Management Protocol) empfangen soll.

Diese Option betrifft alle nachfolgenden Operationen zwischen NDMP-Dateiserver und Server, aber hat keinen Einfluss auf NDMP-Steuerverbindungen, die die Standardnetzschnittstelle des Systems verwenden. Der Wert dieser Option ist ein Hostname oder eine IPV4-Adresse, der bzw. die einer der aktiven Netzschnittstellen des Systems zugeordnet ist, auf dem der IBM Spectrum Protect-Server ausgeführt wird. Diese Schnittstelle muss für IPV4 aktiviert sein.

Sie können diese Serveroption aktualisieren, ohne den Server zu stoppen und erneut zu starten, indem Sie den Befehl SETOPT verwenden.

## Syntax

---

```
>>-NDMPREFDATAINTERFACE--IP-Adresse-----<<
```

## Parameter

---

*IP-Adresse*

Geben Sie eine Adresse in Schreibweise mit Trennzeichen oder im Hostnamensformat an. Wird eine Adresse in der Schreibweise mit Trennzeichen angegeben, wird die Adresse nicht mit einem Domänennamensserver geprüft. Ist die Adresse nicht korrekt, kann dies zu Fehlern führen, wenn der Server versucht, am Anfang einer Sicherung zwischen NDMP-Dateiserver und Server ein Socket zu öffnen.

Adressen im Hostnamensformat werden mit einem Domänennamensserver geprüft. Es gibt keinen Standardwert. Wird kein Wert definiert, verwenden alle NDMP-Operationen die Netzschnittstelle des IBM Spectrum Protect-Servers zum Empfangen von Sicherungsdaten während der Sicherungsoperationen zwischen NDMP-Dateiserver und Server.

Um den Optionswert zu löschen, geben Sie den Befehl SETOPT mit einem Nullwert ("" ) an.

## Beispiele:

---

```
ndmmprefdatainterface net1.tucson.ibm.com
```

```
ndmmprefdatainterface 9.11.152.89
```

## NOPREEMPT

---

Der Server ermöglicht bestimmten Operationen das Zugriffsvorrecht für Datenträger und Einheiten. Durch Angabe von NOPREEMPT kann das Zugriffsvorrecht inaktiviert werden. In diesem Fall hat dann keine Operation das Zugriffsvorrecht auf einen Datenträger und lediglich einer Datenbanksicherungsoperation kann das Zugriffsvorrecht für eine Einheit vor einer anderen Operation eingeräumt werden.

Beispielsweise hat eine Clientoperation zum Zurückschreiben von Daten Vorrang vor einer Clientdatensicherung, wenn es darum geht, eine bestimmte Einheit zu verwenden oder auf einen bestimmten Datenträger zuzugreifen.

## Syntax

---

>>-NOPREEMPT-----<<

## Parameter

---

Keine.

## Beispiele

---

Zugriffsvorrecht unter Serveroperationen inaktivieren:

```
nopreempt
```

## NORETRIEVEDATE

---

Die Option NORETRIEVEDATE gibt an, dass der Server das Abrufdatum einer Datei in einem Plattenspeicherpool nicht aktualisiert, wenn ein Client die Datei zurückschreibt oder abrufen. Diese Option und der Speicherpoolparameter MIGDELAY steuern, wann der Server Dateien umgelagert.

Wird NORETRIEVEDATE nicht angegeben, lagert der Server Dateien um, nachdem sie sich die in dem Parameter MIGDELAY angegebene Anzahl Tage in dem Speicherpool befunden haben. Die Anzahl Tage wird ab dem Tag gezählt, an dem die Datei in dem Speicherpool gespeichert wurde oder von einem Client abgerufen wurde, je nachdem, welches Datum aktueller ist. Wird NORETRIEVEDATE angegeben, wird das Abrufdatum einer Datei von dem Server nicht aktualisiert, und die Anzahl Tage wird ab dem Tag gezählt, an dem die Datei in den Plattenspeicherpool gestellt wurde.

Wird diese Option angegeben und ist Caching für einen Plattenspeicherpool aktiviert, ist die Wiederherstellung von Cache-Speicherbereich betroffen. Wird Speicherbereich in einem Plattenspeicherpool benötigt, der Cache-Dateien enthält, holt der Server den Speicherbereich durch das selektive Löschen von Cache-Kopien. Dateien, die die ältesten Abrufdaten haben und den meisten Speicherbereich belegen, werden zum Löschen ausgewählt. Wird NORETRIEVEDATE angegeben, wird das Abrufdatum von dem Server nicht aktualisiert, wenn eine Datei abgerufen wird. Dies kann dazu führen, dass Cache-Kopien entfernt werden, auch wenn sie kürzlich von einem Client abgerufen wurden.

## Syntax

---

>>-NORETRIEVEDATE-----<<

## Parameter

---

Keine.

## Beispiele

---

Angaben, dass die Abrufdaten von Dateien in Plattenspeicherpools nicht aktualisiert werden, wenn Clients die Dateien zurückschreiben und abrufen:

```
noretrievedate
```

 Windows-Betriebssysteme

## NPAUDITFAILURE

---

Die Option NPAUDITFAILURE gibt an, ob ein Ereignis an das Ereignisprotokoll gesendet wird, wenn ein Knoten sich bei dem Server anmeldet und dabei einen Namen verwendet, der sich zwar in der Windows-Gruppe befindet, aber nicht mit dem Windows-Kontoanmeldenamen übereinstimmt. Um sicherzustellen, dass ein Knoten nur auf seine eigenen Daten zugreifen kann, müssen der Knotenname und der Windows-Kontoanname übereinstimmen.

## Syntax

---

>>-NPAUDITFailure---Yes-----<<  
'-No--'



## Parameter

---

Yes

Gibt an, dass ein Ereignis an das Ereignisprotokoll gesendet wird, wenn ein Knoten sich bei dem Server anmeldet und dabei einen Namen verwendet, der sich in der Windows-Gruppe befindet. Dieser Name stimmt jedoch nicht mit dem Windows-Kontoanmeldenamen überein.

No


Gibt an, dass kein Ereignis über einen Prüffehler an das Ereignisprotokoll gesendet wird.

## Beispiele

---

Angaben, dass ein Ereignis an das Ereignisprotokoll gesendet wird, wenn ein Knoten sich bei dem Server anmeldet und dabei einen Namen verwendet, der sich in der Windows-Gruppe befindet. Dieser Name stimmt jedoch nicht mit dem Windows-Kontoanmeldenamen überein.

```
npauditfailure yes
```

 Windows-Betriebssysteme

## NPAUDITSUCCESS

---

Die Option NPAUDITSUCCESS gibt an, dass ein Ereignis an das Ereignisprotokoll gesendet wird, wenn für einen Clientknotenbenutzer über SECUREPIPE eine Identifikationsprüfung durchgeführt wird, bevor er auf den Server zugreifen kann.

## Syntax

---

```
>>-NPAUDITSUCCESS--+-Yes-+-----<<  
                    '-No--'
```

## Parameter

---

Yes

Gibt an, dass ein Ereignis an das Ereignisprotokoll gesendet wird, wenn für einen Clientknotenbenutzer über SECUREPIPES eine Identifikationsprüfung durchgeführt wird, bevor er auf den Server zugreifen kann.

No


Gibt an, dass kein Ereignis an das Windows-Protokoll gesendet wird.

## Beispiele

---

Angaben, dass ein Ereignis an das Ereignisprotokoll gesendet wird, wenn für einen Clientknoten eine Identifikationsprüfung durchgeführt wird, bevor er auf den Server zugreifen kann.

```
npauditsuccess yes
```

 Windows-Betriebssysteme

## NPBUFFERSIZE

---

Die Option NPBUFFERSIZE gibt die Größe des Kommunikationspuffers für benannte Pipes an.

## Syntax

---

```
                .-8-----.  
>>-NPBUffersize--+-Kilobyte-+-----<<
```

## Parameter

---

Kilobyte

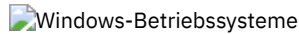
Gibt die Größe des Kommunikationspuffers für benannte Pipes in Kilobyte an. Der Standardwert ist 8.

## Beispiele

---

Einen Kommunikationspuffer mit 16 KB für benannte Pipes angeben:

```
npbuffersize 16
```



## NUMBERFORMAT

---

Die Option NUMBERFORMAT gibt das Format an, in dem der Server Zahlen anzeigt.

Der Wert von NUMBERFORMAT wird von dem Zahlenformat überschrieben, das in den länderspezifischen Angaben definiert ist, wenn die länderspezifischen Angaben beim Starten des Servers erfolgreich initialisiert wurden. Die länderspezifischen Angaben werden in der Option LANGUAGE angegeben.

### Syntax

---

```
>>-NUMberformat--Zahl-----<<
```

### Parameter

---

Zahl

Eine Zahl von 1 bis 6 auswählen, um das vom Server verwendete Zahlenformat anzugeben. Der Standardwert ist 1.

|   |          |
|---|----------|
| 1 | 1,000.00 |
| 2 | 1,000,00 |
| 3 | 1 000,00 |
| 4 | 1 000.00 |
| 5 | 1.000,00 |
| 6 | 1'000,00 |

### Beispiele

---

```
numberformat 4
```

## NUMOPENVOLSALLOWED

---

Die Option NUMOPENVOLSALLOWED gibt die Anzahl der FILE-Eingabedatenträger in einem deduplizierten Speicherpool an, die gleichzeitig geöffnet sein können.

Eingabedatenträger enthalten Daten, die während der Ausführung von Clientzurückschreibungsoperationen und Serverprozessen, wie beispielsweise Wiederherstellung und Umlagerung, gelesen werden sollen. Mit dieser Option kann die Leistung verbessert werden, indem die Häufigkeit reduziert wird, mit der Datenträger geöffnet und geschlossen werden.

Jede Sitzung innerhalb einer Clientoperation oder eines Serverprozesses kann über so viele geöffnete FILE-Datenträger verfügen, wie mit dieser Option angegeben wird. Eine Sitzung wird durch eine Clientoperation oder einen Serverprozess eingeleitet. Es können jeweils Mehrfachsitzenungen gestartet werden.

Während einer Clientzurückschreibungsoperation können Datenträger für die Dauer einer Clientzurückschreibungsoperation und so lange geöffnet bleiben, wie eine Clientsitzung aktiv ist. Bei der Ausführung einer Zurückschreibungsoperation ohne Abfrage bleiben die Datenträger geöffnet, bis die Zurückschreibung ohne Abfrage beendet ist. Zu diesem Zeitpunkt werden alle Datenträger geschlossen und freigegeben. Bei einer klassischen Zurückschreibungsoperation, die im Dialogmodus gestartet wird, können die Datenträger jedoch am Ende der Zurückschreibungsoperation geöffnet bleiben. Die Datenträger werden geschlossen und freigegeben, wenn die nächste klassische Zurückschreibungsoperation angefordert wird.

Definieren Sie diesen Wert in der Serveroptionsdatei oder mit dem Befehl SETOPT.

Tipp: Mit dieser Option kann die Anzahl der jeweils verwendeten Datenträger und Mountpunkte erheblich erhöht werden. Um die Leistung zu optimieren, führen Sie diese Schritte aus:

- Um NUMOPENVOLSALLOWED zu definieren, wählen Sie einen Anfangswert aus (der Standardwert wird empfohlen). Überwachen Sie Clientsitzungen und Serverprozesse. Überprüfen Sie die höchste Anzahl der Datenträger, die für eine einzelne Sitzung oder einen einzelnen Prozess geöffnet sind. Erhöhen Sie die Einstellung von NUMOPENVOLSALLOWED, wenn die höchste Anzahl der geöffneten Datenträger dem mit NUMOPENVOLSALLOWED angegebenen Wert entspricht.
- Um zu verhindern, dass Sitzungen oder Prozesse auf einen Mountpunkt warten müssen, erhöhen Sie den Wert des Parameters MOUNTLIMIT in der Einheitenklassendefinition. Geben Sie für den Parameter MOUNTLIMIT einen so hohen Wert an, dass alle Clientsitzungen und Serverprozesse, die deduplizierte Speicherpools verwenden, die Anzahl der Datenträger öffnen können, die mit der Option NUMOPENVOLSALLOWED angegeben ist. Überprüfen Sie für Clientsitzungen das Ziel in der Kopiengruppendefinition, um die Anzahl der Knoten zu bestimmen, die Daten in dem deduplizierten Speicherpool speichern. Überprüfen Sie für Serverprozesse die Anzahl der Prozesse, die für jeden Prozess für den Speicherpool zulässig sind.
- Es kann eine Situation auftreten, in der ein Knoten gleichzeitig in einem deduplizierten Speicherpool sichert und aus einem deduplizierten Speicherpool zurückschreibt oder gleichzeitig in einem deduplizierten Speicherpool archiviert und aus einem deduplizierten Speicherpool abruf. Alle für diese Operationen erforderlichen Mountpunkte erhöhen die Gesamtzahl der Mountpunkte, die von dem Knoten benötigt werden.

Als Ergebnis kann der Knoten möglicherweise keine weiteren Sicherungssitzungen starten, wenn für ihn bereits mehr Mountpunkte geöffnet sind als der Parameter MAXNUMMP in der Clientknotendefinition erlaubt. Diese Situation kann auftreten, obwohl der Wert für MOUNTLIMIT für die Einheitenklasse nicht überschritten wurde.

Um zu verhindern, dass Sicherungs- und Abrufoperationen fehlschlagen, setzen Sie den Wert des Parameters MAXNUMMP in der Clientknotendefinition auf einen Wert, der mindestens so hoch wie der Wert der Option NUMOPENVOLSALLOWED ist. Erhöhen Sie diesen Wert, wenn Sie feststellen, dass der Knoten Sicherungs- oder Abrufoperationen nicht ausführt, da der Wert von MAXNUMMP überschritten wird.

## Syntax

---

```
>>-NUMOPENVOLsallowed--Anzahl_geöffneter_Datenträger-----<<
```

## Parameter

---

Anzahl\_geöffneter\_Datenträger




Gibt die Anzahl der FILE-Eingabedatenträger in einem deduplizierten Speicherpool an, die gleichzeitig geöffnet sein können. Der Standardwert ist 10. Der Mindestwert ist 3. Der Maximalwert ist 999.

## Beispiele

---

Angaben, dass bis zu 5 Datenträger in einem deduplizierten Speicherpool gleichzeitig geöffnet sein können.

```
numopenvolsallowed 5
```

## PUSHSTATUS

---

Die Option PUSHSTATUS wird auf Peripherieservern verwendet, um sicherzustellen, dass Statusinformationen an den Hub-Server gesendet werden. Aktualisieren Sie diese Option nur, wenn Sie die Konfiguration des Operations Center im vorkonfigurierten Zustand zurückschreiben müssen, in dem die IBM Spectrum Protect-Server nicht als Hub-Server oder Peripherieserver definiert sind.

Wenn Sie die Konfiguration des Operations Center im vorkonfigurierten Zustand zurückschreiben müssen, müssen Sie den folgenden Befehl auf jedem Peripherieserver ausgeben:

```
SETOPT PUSHSTATUS NO
```

## QUERYAUTH

---

Die Option QUERYAUTH gibt die Administratorberechtigungsstufe an, die für die Ausgabe des Befehls QUERY oder SQL SELECT erforderlich ist. Standardmäßig kann jeder Administrator die Befehle QUERY und SELECT ausgeben. Mit dieser Option kann die Verwendung dieser Befehle eingeschränkt werden.

## Syntax

---

```
>>-QUERYAuth--+-NOne-----+-----<<
+-System---+
```

```
+Policy---+
+Storage---+
'-Operator-'
```

## Parameter

---

### NOne

Jeder Administrator kann den Befehl QUERY oder SELECT ausgeben, ohne dass eine Administratorberechtigung erforderlich ist.

### System

Administratoren müssen über die Berechtigung SYSTEM verfügen, um den Befehl QUERY oder SELECT ausgeben zu können.

### POlICY

Administratoren müssen über die Berechtigung POLICY für eine oder mehrere Maßnahmendomänen oder über die Berechtigung SYSTEM verfügen, um den Befehl QUERY oder SELECT ausgeben zu können.

### STorage

Administratoren müssen über die Berechtigung STORAGE für einen oder mehrere Speicherpools oder über die Berechtigung SYSTEM verfügen, um den Befehl QUERY oder SELECT ausgeben zu können.

### OPerator

Administratoren müssen über die Berechtigung OPERATOR oder SYSTEM verfügen, um den Befehl QUERY oder SELECT ausgeben zu können.

## Beispiele

---

Um die Verwendung der Befehle QUERY und SELECT auf Administratoren mit System- oder Speicherberechtigung zu beschränken, folgendes eingeben:

```
queryauth storage
```

## RECLAIMDELAY

---

Mit dieser Option wird die Wiederherstellung eines SnapLock-Datenträgers verzögert. Damit wird es ermöglicht, dass verbleibende Daten verfallen können, so dass keine Notwendigkeit zur Wiederherstellung des Datenträgers besteht.

## Syntax

---

```
.-4-----.  
>>-RECLAIMDELAY--+-Anzahl_Tage+-----<<
```

## Parameter

---

### Anzahl\_Tage

Gibt die Anzahl der Tage an, die die Wiederherstellung eines SnapLock-Datenträgers verzögert werden soll. Bevor ein SnapLock-Datenträger wiederhergestellt wird, lässt der IBM Spectrum Protect-Server die angegebene Anzahl Tage verstreichen und bietet so die Möglichkeit, dass alle verbleibenden Dateien auf dem Datenträger verfallen können. Der standardmäßige Zeitraum für die Wiederherstellungsverzögerung sind 4 Tage. Es kann ein Wert zwischen 1 und 120 Tage definiert werden.

## Beispiele

---

Angeben, dass die Anzahl Tage für die Verzögerung der Wiederherstellung 30 Tage beträgt:

```
reclaimdelay 30
```

## RECLAIMPERIOD

---

Mit dieser Option können Sie die Anzahl der Tage für den Wiederherstellungszeitraum eines SnapLock-Datenträgers definieren.

## Syntax

---

```
.-30-----.  
>>-RECLAIMPERIOD--+-Anzahl_Tage+-----<<
```

## Parameter

---

### Anzahl\_Tage

Gibt die Anzahl der Tage an, die für den Wiederherstellungszeitraum eines SnapLock-Datenträgers zulässig sind. Nachdem die Aufbewahrungsdauer eines SnapLock-Datenträgers abgelaufen ist, stellt der IBM Spectrum Protect-Server den Datenträger innerhalb der angegebenen Anzahl Tage wieder her, wenn sich noch Daten auf dem Datenträger befinden. Der standardmäßige Wiederherstellungszeitraum beträgt 30 Tage. Es kann ein Wert zwischen 7 und 365 Tage definiert werden.

Der Wiederherstellungszeitraum beginnt erst nach Ablauf des RECLAIMDELAY-Zeitraums.

## Beispiele

---

Angaben, dass der Wiederherstellungszeitraum 45 Tage beträgt:

```
reclaimperiod 45
```

## REORGBEGINTIME

---

Die Option REORGBEGINTIME gibt die früheste Zeit an, zu der der IBM Spectrum Protect-Server eine Tabellen- oder Indexreorganisation starten kann.

Planen Sie den Start der vom Server eingeleiteten Reorganisationen während eines Zeitraums, in dem die Serveraktivität niedrig ist. Verwenden Sie diese Option zusammen mit der Option REORGDURATION. Die Option REORGDURATION gibt ein Intervall an, in dem die Reorganisation starten kann.

## Syntax

---

```
>>-REORGBEGINTime--hh:mm-----<<
```

## Parameter

---

### hh:mm

Gibt die Zeit an, zu der der Server eine Reorganisation starten kann: Die Standardstartzeit ist 6:00. Verwenden Sie ein 24-Stunden-Format, um die Zeit anzugeben.

| Zeit | Beschreibung          | Werte                                 |
|------|-----------------------|---------------------------------------|
| hh   | Die Stunde des Tages  | Geben Sie eine Zahl von 00 bis 23 an. |
| mm   | Die Minute der Stunde | Geben Sie eine Zahl von 00 bis 59 an. |

## Beispiele

---

6:00 Uhr als früheste Zeit angeben, zu der eine Reorganisation gestartet werden kann.

```
reorgbegintime 06:00
```

20 Uhr 30 als früheste Zeit angeben, zu der eine Reorganisation gestartet werden kann.

```
reorgbegintime 20:30
```

12 Uhr mittags als früheste Zeit angeben, zu der eine Reorganisation gestartet werden kann.

```
reorgbegintime 12:00
```

15 Uhr 30 als früheste Zeit angeben, zu der eine Reorganisation gestartet werden kann.

```
reorgbegintime 15:30
```

Mitternacht als früheste Zeit angeben, zu der eine Reorganisation gestartet werden kann.

```
reorgbegintime 00:00
```

## REORGDURATION

---

Die Option REORGDURATION gibt ein Intervall an, in dem die vom Server eingeleitete Tabellen- oder Indexreorganisation gestartet werden kann.

Planen Sie den Start der vom Server eingeleiteten Reorganisationen während eines Zeitraums, in dem die Serveraktivität niedrig ist. Verwenden Sie diese Option zusammen mit der Option REORGBEGINTIME. Die Option REORGBEGINTIME gibt die früheste Zeit an, zu der der Server eine Reorganisation starten kann.

## Syntax

---

```
>>-REORGDuration--nn-----<
```

## Parameter

---

nn  
Gibt die Anzahl der Stunden an, in denen eine Reorganisation gestartet werden kann. Der Mindestwert ist 1, der Maximalwert ist 24. Der Standardwert ist 24.

## Beispiel

---

Ein Intervall von vier Stunden angeben, in denen eine Reorganisation gestartet werden kann.

```
reorgduration 4
```

## REPORTRETRIEVE

---

Die Option REPORTRETRIEVE erstellt Berichte zu Zurückschreibungs- oder Abrufoperationen, die von Clientknoten oder Administratoren ausgeführt werden. Der Standardwert ist NO.

## Syntax

---

```
>>-REPORTRETRIEVE---YES+-----<  
'-NO--'
```

## Parameter

---

YES  
Gibt an, dass Nachrichten an der Serverkonsole ausgegeben und im Aktivitätenprotokoll gespeichert werden, wenn Dateien vom IBM Spectrum Protect-Server zurückgeschrieben oder abgerufen werden. Die Nachrichten geben den Namen der Objekte an, die zurückgeschrieben oder abgerufen werden, und identifizieren den Clientknoten oder den Administrator, der die Operation ausführt.

NO  
Gibt an, dass keine Nachrichten ausgegeben werden.

## Beispiele

---

Angeben, dass Nachrichten im Aktivitätenprotokoll ausgegeben und gespeichert werden, wenn Dateien vom IBM Spectrum Protect-Server zurückgeschrieben oder abgerufen werden:

```
reportretrieve yes
```

Die folgende Nachricht wird für eine Verwaltungsclientsitzung ausgegeben:

```
ANR0411I Sitzung 8 für Administrator COLIND-TUC, der am Knoten COLIND-TUC  
angemeldet ist, hat das Sicherungsobjekt zurückgeschrieben oder abgerufen: Knoten COLIND-TUC,  
Dateibereich \\colind-tuc\c$, object\CODE\TESTDATA\ XXX.OUT
```

## REPLBATCHSIZE

---

Die Option REPLBATCHSIZE gibt die Anzahl Clientdateien an, die innerhalb derselben Servertransaktion als Stapel repliziert werden sollen. Diese Option betrifft nur die Knotenreplikationsprozesse und arbeitet mit der Option REPLSIZETHRESH, um die Knotenreplikationsverarbeitung zu verbessern.

Die Option REPLBATCHSIZE begrenzt die Anzahl der Dateien in einer Transaktion und die Option REPLSIZETHRESH begrenzt die Anzahl der Byte in einer Transaktion. Die Transaktion wird beendet, wenn entweder der Schwellenwert für REPLBATCHSIZE oder der Schwellenwert für REPLSIZETHRESH erreicht wird.

## Syntax

---

```
                .-4096-----.  
>>-REPLBatchsize---+Anzahl_Dateien+-----><
```

## Parameter

---

Anzahl\_Dateien

Gibt eine Anzahl Dateien zwischen 1 und 32768 an. Der Standardwert ist 4096.

## Beispiele

---

```
replbatchsize 25000
```

## REPLSIZETHRESH

---

Die Option REPLSIZETHRESH gibt einen Schwellenwert (in Megabyte) für das replizierte Datenvolumen innerhalb derselben Servertransaktion an.

Das Datenvolumen basiert auf der nicht deduplizierten Größe der Datei. Dies ist die Originalgröße der Datei. Das Datenvolumen, das repliziert wird, wird durch den Schwellenwert gesteuert. Wenn das Datenvolumen den Schwellenwert überschreitet, beendet der Server die Transaktion und es werden keine weiteren Dateien dem aktuellen Stapel hinzugefügt. Eine neue Transaktion wird gestartet, nachdem der aktuelle Stapel repliziert wurde. Diese Option wird mit der Option REPLBATCHSIZE verwendet.

Beispiel: Angenommen, eine Datei hat 10 MB und wird in einem Speicherpool gespeichert, der für die Dateneduplizierung aktiviert ist, und nur 2 MB der Datei werden während der Replikation übertragen. Das replizierte Datenvolumen schließt die Größe von 10 MB der Datei ein und schließt die übertragenen 2 MB aus. Wenn das replizierte Datenvolumen den für den REPLSIZETHRESH-Schwellenwert angegebenen Wert überschreitet, wird die Transaktion beendet.

Tipp: Falls Sie Daten von einem Quellenserver in der Cloud replizieren und auf dem Zielsystem häufig die Servernachricht ANR1880W empfangen, verringern Sie den Wert der Option REPLSIZETHRESH auf dem Quellenserver.

## Syntax

---

```
                .-4096-----.  
>>-REPLSizethresh---+ Megabyte+-----><
```

## Parameter

---

Megabyte

Gibt die Anzahl Megabyte als ganze Zahl von 1 bis 32768 an. Der Standardwert ist 4096.

## Beispiele

---

```
replsizethresh 2000
```

## REQSYSAUTHOUTFILE

---

Die Option REQSYSAUTHOUTFILE gibt an, ob die Systemberechtigung für Verwaltungsbefehle erforderlich ist, die IBM Spectrum Protect veranlassen, in eine externe Datei zu schreiben.

Diese Option gilt für folgende Befehle:

- BACKUP DEVCONFIG mit dem Parameter FILENAMES
- BACKUP VOLHISTORY mit dem Parameter FILENAMES
- DEFINE BACKUPSET
- DELETE BACKUPSET
- GENERATE BACKUPSET

- MOVE DRMEDIA mit dem Parameter CMD
- MOVE MEDIA mit dem Parameter CMD
- QUERY DRMEDIA mit dem Parameter CMD
- QUERY MEDIA mit dem Parameter CMD
- QUERY SCRIPT mit dem Parameter OUTPUTFILE

## Syntax

---

```
>>-REQSYSauthoutfile--+-Yes-+-----><
                        '-No--'
```

## Parameter

---

Yes

Die Systemberechtigung ist für Verwaltungsbefehle erforderlich, die IBM Spectrum Protect veranlassen, in eine externe Datei zu schreiben.

No

Die Systemberechtigung ist für Verwaltungsbefehle nicht erforderlich, die IBM Spectrum Protect veranlassen, in eine externe Datei zu schreiben. Dies bedeutet, dass die Berechtigungsstufe zur Ausgabe des Befehls nicht geändert werden muss.

## Beispiele

---

```
reqsysauthoutfile no
```

## RESOURCETIMEOUT

---

Die Option RESOURCETIMEOUT gibt an, wie lange der Server auf eine Ressource wartet, bevor die anstehende Anforderung einer Ressource abgebrochen wird. Tritt eine Zeitlimitüberschreitung auf, wird die Anforderung der Ressource abgebrochen.

Anmerkung: Wird eine Gruppe von gemeinsam benutzten Kassettenarchivressourcen verwaltet, wie beispielsweise Server, die als Kassettenarchivmanager und -clients bestimmt sind, sollte diese Option für alle Teilnehmer an der gemeinsam benutzten Konfiguration auf dasselbe Zeitlimit gesetzt werden. Bei jeder Fehlerbehebung verwendet IBM Spectrum Protect immer das längste Zeitlimit.

## Syntax

---

```
                .-60-----.
>>-RESOURCETimeout--+-Minuten+-----><
```

## Parameter

---

Minuten

Gibt die maximale Anzahl Minuten an, die der Server auf eine Ressource wartet. Der Standardwert ist 60 Minuten. Der Mindestwert ist 1 Minute.

## Beispiele

---

Angeben, dass der Server 15 Minuten auf eine Serverressource wartet:

```
resourcetimeout 15
```

## RESTHTTPSPORT

---

Die Option RESTHTTPSPORT gibt die Anschlussnummer an, die für die HTTPS-Kommunikation (HTTPS = Hypertext Transfer Protocol Secure) zwischen dem Operations Center und dem Hub-Server verwendet werden soll.

## Syntax

---

```
                .-8443-----.
>>-RESTHTTPSport--+-sicherer_Anschluss+-----><
```



## Parameter

---

### sicherer\_Anschluss

Gibt die Anschlussnummer an, die für die sichere Kommunikation zwischen dem Hub-Server und dem Operations Center verwendet wird. Der Wertebereich ist 1025 bis 32767; der Standardwert ist 8443.

## Beispiel

---

Angeben, dass die Anschlussnummer 8444 für die HTTPS-Kommunikation verwendet wird.

```
resthttpsport 8444
```

## RESTOREINTERVAL

---

Die Option RESTOREINTERVAL gibt an, wie lange eine wiederanlauffähige Zurückschreibungssitzung in der Serverdatenbank gesichert werden kann. Solange die Zurückschreibungssitzung in der Datenbank gesichert ist, kann sie ab dem Punkt, an dem sie gestoppt wurde, erneut gestartet werden.

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

## Syntax

---

```
.-1440----.  
>>-RESTOREINTERVAL--+-Minuten+-----><
```

## Parameter

---

### Minuten

Gibt an, wie lange sich eine wiederanlauffähige Zurückschreibungssitzung in der Datenbank befinden kann, bevor sie ihre Gültigkeit verliert (Angabe in Minuten). Der Mindestwert ist 0, der Höchstwert beträgt 10080 Minuten (eine Woche). Der Standardwert ist 1440 Minuten (24 Stunden). Wird der Wert auf 0 gesetzt und die Zurückschreibung unterbrochen oder abgebrochen, wird die Zurückschreibung dennoch in den Status "wiederanlauffähig" versetzt. Sie kann jedoch sofort als "Verfallskandidat" ausgewählt werden.

## Beispiele

---

```
restoreinterval 1440
```

## RETENTIONEXTENSION

---

Die Option RETENTIONEXTENSION gibt die Anzahl der Tage an, um die das Ende des Aufbewahrungszeitraums eines SnapLock-Datenträgers erweitert werden soll. Mit dieser Option kann der Server das Ende des Aufbewahrungszeitraums eines SnapLock-Datenträgers erweitern, um eine übermäßige Wiederherstellung zu vermeiden.

## Syntax

---

```
>>-RETENTIONEXTENSION--Anzahl_Tage-----><
```

## Parameter

---

### Anzahl\_Tage

Gibt die Anzahl der Tage an, um die das Ende des Aufbewahrungszeitraums eines SnapLock-Datenträgers erweitert werden soll. Der Mindestwert ist 30 Tage; der Maximalwert ist 9999 Tage; der Standardwert ist 365.

Wenn Sie den Wert 0 (null) für den Parameter RETVER einer Archivierungskopiengruppe angeben, ist der tatsächliche Wert, der für RETVER verwendet wird, der Wert der Option RETENTIONEXTENSION, wenn eine der folgenden Bedingungen zutrifft:

- Der Zielspeicherpool für die Archivierungskopiengruppe ist ein SnapLock-Speicherpool.
- Der Speicherpool, der das Ziel für eine Speicherpoolumlagerung oder eines Befehls MOVE DATA oder MOVE NODEDATA ist, ist ein SnapLock-Speicherpool.

Ist ein SnapLock-Datenträger der Zieldatenträger für Daten von einem anderen SnapLock-Datenträger und ist die verbleibende Aufbewahrungsdauer der Daten auf dem Datenträger geringer als der angegebene Wert, wird das Ende des Aufbewahrungszeitraums unter Verwendung des angegebenen Werts definiert. Andernfalls wird die verbleibende Aufbewahrungsdauer der Daten verwendet, um die Aufbewahrungsdauer des Datenträgers zu definieren. Befindet sich ein SnapLock-Datenträger innerhalb der Wiederherstellungsperiode, aber hat der Prozentsatz des wiederherstellbaren Speicherbereichs des Datenträgers nicht den Wiederherstellungsschwellenwert des Speicherpools oder den im Parameter THRESHOLD eines Befehls RECLAIM STGPOOL angegebenen Wert überschritten, wird das Ende des Aufbewahrungszeitraums des SnapLock-Datenträgers um den Wert erweitert, der mit der Option RETENTIONEXTENSION angegeben ist.

## Beispiele

Angaben, dass das Ende des Aufbewahrungszeitraums um 60 Tage erweitert wird:

```
retentionextension 60
```

## SANDISCOVERY

Die Option SANDISCOVERY gibt an, ob die SAN-Erkennungsfunktion von IBM Spectrum Protect aktiviert ist.

Um die SAN-Erkennung verwenden zu können, müssen alle Einheiten in dem SAN eine eindeutige Einheitenseriennummer haben. Ist die Option auf ON gesetzt, führt der Server in den folgenden Situationen eine SAN-Erkennung durch:

- Wenn der Einheitenpfad geändert wird
- Wenn der Befehl QUERY SAN ausgegeben wird

Bei Verwendung der SAN-Erkennung kann der Server automatisch den Gerätedateinamen für eine Einheit korrigieren, wenn sich der Name für eine angegebene Bändeinheit ändert.

Der IBM Spectrum Protect-Server benötigt keine persistente Bindung mit der aktivierten SAN-Erkennungsfunktion. Um eine Liste der Einheiten für den Server anzuzeigen, können Sie den Befehl QUERY SAN ausgeben.

## Syntax

```
.-SANDISCOVERY-----OFF-----
>>+-----+-----><
'|-SANDISCOVERY-----+ON-----+'
      '-UNSCANNEDPATHOFF-'
```

## Parameter

ON

Gibt an, dass der Server eine SAN-Erkennung ausführt, wenn der Einheitenpfad geändert oder der Befehl QUERY SAN ausgegeben wird.

OFF

Gibt an, dass der Server keine SAN-Erkennung ausführt, wenn der Einheitenpfad geändert oder der Befehl QUERY SAN ausgegeben wird. Wenn der IBM Spectrum Protect-Server eine Einheit nicht öffnen kann, wird eine Nachricht ausgegeben, aber der Pfad, der der Einheit zugeordnet ist, wird nicht offline gesetzt. Dieser Wert ist der Standardwert.

UNSCANNEDPATHOFF

Gibt an, dass der Server keine SAN-Erkennung ausführt, wenn der Einheitenpfad geändert oder der Befehl QUERY SAN ausgegeben wird. Wenn der IBM Spectrum Protect-Server eine Einheit nicht öffnen kann, wird eine Nachricht ausgegeben und der Pfad zu der Einheit wird offline gesetzt.

## Beispiele


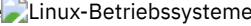
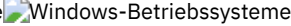
```
sandiscovery on
```

## Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SANDISCOVERY

| Befehl | Beschreibung |
|--------|--------------|
|--------|--------------|

| Befehl            | Beschreibung  |
|-------------------|---|
| PERFORM LIBACTION | Definiert alle Laufwerke und Pfade für ein Kassettenarchiv. |

## SANDISCOVERYTIMEOUT

Die Option SANDISCOVERYTIMEOUT gibt die Zeit an, die für die Antwort von Hostbusadaptern zulässig ist, wenn sie von dem SAN-Erkennungsprozess abgefragt werden. Sobald die für SANDISCOVERYTIMEOUT angegebene Zeit erreicht wird, tritt bei dem Prozess eine Zeitlimitüberschreitung auf.

### Syntax

```
>>-SANDISCOVERYTIMEOUT--Wert-----<<
```

### Parameter

Wert

Gibt die Zeit an, die vergehen darf, bevor bei dem SAN-Erkennungsprozess eine Zeitlimitüberschreitung auftritt. Der Bereich liegt zwischen 15 und 1800 Sekunden. Der Standardwert ist 15 Sekunden.

### Beispiele

```
sandiscoverytimeout 45
```

## SANREFRESHTIME

Die Option SANREFRESHTIME gibt die Zeit an, die vergeht, bevor die zwischengespeicherten SAN-Erkennungsinformationen aktualisiert werden. Die Option SANREFRESHTIME hat den Standardwert 0, der angibt, dass kein SAN-Erkennungscache vorhanden ist. Bei jeder Ausführung einer SAN-Erkennungsoperation durch den Server werden die Informationen direkt von dem Hostbusadapter abgerufen.

Anmerkung: Der Serverbefehl QUERY SAN empfängt SAN-Informationen immer zu dem Zeitpunkt, an dem der Befehl ausgegeben wird, und ignoriert den Wert, der für SANREFRESHTIME angegeben ist.

### Syntax

```
.-0----.
>>-SANREFRESHTIME--+-Zeit+-----<<
```

### Parameter

Zeit

Die Zeit in Sekunden, bevor die zwischengespeicherten SAN-Erkennungsinformationen aktualisiert werden. Der Standardwert ist 0 und gibt an, dass SAN-Erkennungsinformationen nicht zwischengespeichert werden. Wird ein anderer Wert als 0 angegeben, beispielsweise 100 Sekunden, werden die SAN-Erkennungsinformationen 100 Sekunden nach der vorherigen SAN-Erkennungsoperation aktualisiert.

### Beispiele

Die SAN-Erkennungsinformationen nach 100 Sekunden aktualisieren.

```
sanrefreshtime 100
```

Das Caching der SAN-Erkennungsinformationen inaktivieren.

```
sanrefreshtime 0
```

## SEARCHMPQUEUE

Die Option SEARCHMPQUEUE gibt die Reihenfolge an, in der der Server Anforderungen in der Ladewarteschlange ausführt. Wird die Option angegeben, versucht der Server zuerst, Anforderungen für Datenträger auszuführen, die bereits geladen sind. Diese Anforderungen können vor anderen Anforderungen ausgeführt werden, auch wenn die anderen Anforderungen schon länger auf den Mountpunkt warten. Wird diese Option nicht angegeben, führt der Server Anforderungen in der Reihenfolge aus, in der sie empfangen werden.

## Syntax

---

```
>>-SEARCHMPQUEUE-----<<
```

## Parameter

---


Keine.

## Beispiele

---

Angaben, dass der Server zuerst versucht, eine Anforderung für einen Datenträger auszuführen, der bereits geladen ist:

```
searchmpqueue
```

 Windows-Betriebssysteme

## SECUREPIPES

---

Bei Verwendung des Protokolls mit benannten Pipes führt das Aktivieren von SECUREPIPES dazu, dass der Server die über ADMSGROUPNAME angegebene Windows-Gruppe prüft, um einen Clientknoten/Benutzer zu authentifizieren.

Anhand des in der Windows-Gruppe definierten Benutzernamens und Kennworts wird der Knoten/Benutzer für den Zugriff auf die Serverdaten authentifiziert. Der Knoten/Benutzer muss außerdem als IBM Spectrum Protect-Clientknoten registriert sein. Das Kennwort für den IBM Spectrum Protect-Clientknoten wird jedoch ignoriert und statt dessen das für den Benutzer vergebene Windows-Kennwort verwendet.

## Syntax

---

```
>>-SECUREPipes--+-Yes-+-----<<
                '-No--'
```

## Parameter

---

Yes

Gibt an, dass IBM Spectrum Protect die über ADMSGROUPNAME angegebene Windows-Gruppe prüft, um einen Clientknoten/Benutzer zu authentifizieren.

No

Gibt an, dass IBM Spectrum Protect die über ADMSGROUPNAME angegebene Windows-Gruppe nicht prüft, um einen Clientknoten/Benutzer zu authentifizieren.

## Beispiele

---

Angaben, dass IBM Spectrum Protect die Windows-Gruppe prüft, um Clientknoten zu authentifizieren.

```
securepipes yes
```

## SERVERDEDUPTXNLIMIT

---

Die Option SERVERDEDUPTXNLIMIT gibt die maximale Größe von Objekten an, die auf dem Server dedupliziert werden können.

Wenn Sie Prozesse zum Identifizieren doppelter Daten (Befehl IDENTIFY DUPLICATES) für große Objekte verwenden, können lange laufende Transaktionen, die zur Aktualisierung der Datenbank erforderlich sind, eine umfangreiche Datenbankaktivität zur Folge haben. Eine umfangreiche Datenbankaktivität kann die folgenden Symptome zur Folge haben:

- Reduzierter Durchsatz bei Clientsicherungs- und -archivierungsoperationen
- Ressourcenkonflikt aufgrund gleichzeitig ablaufender Serveroperationen

- Exzessive Wiederherstellungsprotokollaktivität

Das Ausmaß, in dem diese Symptome auftreten, hängt von der Anzahl und Größe der Objekte ab, die verarbeitet werden, von der Intensität und dem Typ der gleichzeitig ablaufenden Operationen auf dem IBM Spectrum Protect-Server und von der IBM Spectrum Protect-Serverkonfiguration.

Mit der Serveroption SERVERDEDUPTXNLIMIT können Sie eine maximale Größe (in Gigabyte) für Objekte angeben, die auf dem Server dedupliziert werden können. Wenn ein Objekt oder eine Gruppe von Objekten in einer einzelnen Transaktion den mit SERVERDEDUPTXNLIMIT angegebenen Grenzwert überschreitet, werden die Objekte nicht vom Server dedupliziert. Sie können einen Wert von 32 bis 102400 GB angeben. Der Standardwert ist 5120 GB.

Wird der Wert dieser Option erhöht, sucht der IBM Spectrum Protect-Server nach zuvor zurückgehaltenen Objekten, deren Größe unter den neuen Transaktionsgrenzwert fällt.

Hinweis: Die Suche nach zuvor zurückgehaltenen Objekten kann einige Zeit in Anspruch nehmen. Gehen Sie mit Vorsicht vor, wenn Sie den Wert von SERVERDEDUPTXNLIMIT erhöhen. Wird der Wert dieser Option verringert, sucht IBM Spectrum Protect nicht nach zurückgehaltenen Objekten.

Der geeignete Wert für diese Option hängt von der IBM Spectrum Protect-Serverkonfiguration und der gleichzeitig stattfindenden Serveraktivität ab. Sie können einen hohen Wert für diese Option angeben, wenn Sie den Ressourcenkonflikt minimieren. Um den Ressourcenkonflikt zu minimieren, führen Sie Operationen, wie beispielsweise Sicherung, Archivierung, Identifizierung doppelter Daten und Wiederherstellung, zu unterschiedlichen Zeiten aus.

Um diese Serveroption zu aktualisieren, ohne den Server zu stoppen und erneut zu starten, verwenden Sie den Befehl SETOPT.

## Syntax

---

```

                .-5120-----.
>>-SERVERDEDUPTXNlimit--+-Gigabyte+-----<<

```

## Parameter

---

### Gigabyte

Gibt die maximale Größe (in Gigabyte) von Objekten an, die auf dem Server dedupliziert werden können. Sie können einen Wert von 32 bis 102400 angeben. Der Standardwert ist 5120.

## Beispiele


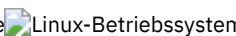
---

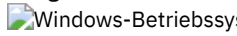
Die serverseitige Deduplizierung für alle Objekte über 120 GB inaktivieren:

```
serverdeduptxnlimit 120
```

## SHMPORT

---

  Die Option SHMPORT gibt die TCP/IP-Anschlussadresse eines Servers bei Verwendung von gemeinsam benutztem Speicher an. Jede Übertragung mit gemeinsam benutztem Speicher beginnt mit einer TCP/IP-Verbindung.

 Die Option SHMPORT gibt den Anschluss an, an dem der Server für Verbindungen mit gemeinsam genutztem Speicher empfängsbereit ist.

## Syntax


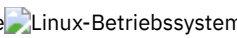
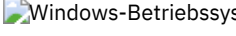
---

```
>>-SHMPort--Anschlussnummer-----<<
```

## Parameter

---

### Anschlussnummer

Gibt die Anschlussnummer an.   Sie können einen Wert von 1024 bis 32767 angeben. Der Standardwert ist 1510.  Sie können einen Wert von 1 bis 32767 angeben. Der Standardwert ist 1.

## Beispiele

---

## SHREDDING

---

Die Option SHREDDING gibt an, ob das Schreddern von gelöschten sensiblen Daten automatisch oder manuell ausgeführt wird. Das Schreddern gilt nur für Daten in Speicherpools, die explizit für die Unterstützung des Schredderns konfiguriert wurden.

### Syntax

---

```
>>-SHREDDing--+-AUTOMATIC-+-----><
                '-MANual----'
```

### Parameter

---

#### AUTOMATIC

Gibt an, dass das Schreddern automatisch erfolgt, wenn sensible Daten gelöscht werden. Verwenden Sie diese Option, um sensible Daten so schnell wie möglich nach dem Löschen zu schreddern. Wird die Option SHREDDING nicht angegeben, ist dies das Standardverhalten. Tritt während des automatischen Schredderns ein E/A-Fehler auf, wird ein Fehler zurückgemeldet und das Schreddern des aktuellen Objekts wird angehalten. Kann der E/A-Fehler nicht korrigiert werden, müssen Sie möglicherweise das Schreddern manuell ausführen und das Schlüsselwort IOERROR verwenden.

#### MANUAL

Gibt an, dass das Schreddern manuell erfolgt, und zwar nur dann, wenn der Befehl SHRED DATA aufgerufen wird. Mit dieser Option können Sie den Zeitpunkt für das Schreddern steuern und sicherstellen, dass das Schreddern nicht andere Serveraktivitäten stört.

Tipp: Wenn Sie das manuelle Schreddern angeben, führen Sie den Befehl SHRED DATA regelmäßig aus, aber mindestens so oft wie Sie andere routinemäßige Serververwaltungstasks ausführen (beispielsweise Verfallsverarbeitung, Wiederherstellung usw.). Damit können Leistungseinbußen bei bestimmten Serverprozessen (besonders bei der Umlagerung) verhindert werden. Die besten Ergebnisse werden erzielt, wenn Sie SHRED DATA nach jeder Operation ausführen (beispielsweise Verfallsverarbeitung und Umlagerung), bei der Dateien aus einem Schredderpool gelöscht werden.

### Beispiele

---

Angeben, dass IBM Spectrum Protect automatisch Daten in einem Speicherpool schreddert, der für das Schreddern konfiguriert ist, nachdem diese Daten gelöscht wurden:

```
shredding automatic
```

## SNMPHEARTBEATINTERVAL

---

Die Option SNMPHEARTBEATINTERVAL gibt das Intervall zwischen den Abfragen des IBM Spectrum Protect-Servers in Minuten an.

### Syntax

---

```
>>-SNMPHEARTBEATINTERVAL--+-Minuten-+-----><
                .-5-----.
```

### Parameter

---

#### Minuten

Gibt das Intervall für das Überwachungssignal in Minuten an. Gültige Werte sind 0 bis 1440 (ein Tag). 5 Minuten sind der Standardwert.

### Beispiele

---

```
snmpheartbeatinterval 20
```

## SNMPMESSAGECATEGORY

---

Die Option SNMPMESSAGECATEGORY gibt die Abfangarten an, die verwendet werden, wenn Nachrichten des Servers über den SNMP-Subagenten (SNMP = Simple Network Management Protocol) an den SNMP-Manager weitergeleitet werden.

### Syntax

---

```
>>-SNMPMESSAGECATEGORY--+-SEVERITY---+-----><
      '-INDIVIDUAL-'
```

### Parameter

---

#### SEVERITY

Gibt an, dass es vier Abfangarten gibt, und zwar abhängig von der Bewertungsstufe der Nachricht:

- 1 Schwerwiegend
- 2 Fehler
- 3 Warnung
- 4 Information

Dies ist der Standardwert.

#### INDIVIDUAL

Gibt an, dass für jede Nachricht eine separate Abfangart verwendet wird. Der numerische Teil der Nachrichten-ID gibt die Abfangart an.

### Beispiele

---

```
snmpmessagecategory individual
```

## SNMPSUBAGENT

---

Die Option SNMPSUBAGENT gibt die Parameter an, die erforderlich sind, damit der IBM Spectrum Protect-Subagent mit dem SNMP-Dämon (SNMP = Simple Network Management Protocol) kommunizieren kann. Diese Option betrifft nur das Konfigurieren des SNMP-Subagenten, damit dieser mit dem SNMP-Agenten kommunizieren kann; die Option wird vom Server ignoriert.

### Syntax

---

```
>>-SNMPSUBAGENT--+------>
      '-HOSTname--Hostname-'
>--+------>
      '-COMMunityname -Benutzergemeinschaft-'
>--+------><
      '-TIMEOUT -Sekunden-'
```

### Parameter

---

#### HOSTname Hostname

Gibt den TCP/IP-Namen oder die Nummer des Hosts an, der den SNMP-Agenten ausführt, zu dem der IBM Spectrum Protect SNMP-Subagent die Verbindung herstellt. Dieser Parameter ist wahlfrei. Der Standardname lautet *localhost*.

#### COMMunityname Benutzergemeinschaft

Gibt den Namen der Benutzergemeinschaft auf dem System an, das den SNMP-Agenten ausführt. Dieser Parameter ist wahlfrei. Der Standardname lautet *public*.

#### TIMEOUT Sekunden

Gibt die Zeitspanne an (in Sekunden), innerhalb der eine Anforderung empfangen werden muss. Dieser Parameter ist wahlfrei. Der Standardwert ist 600.

## Beispiele

---

```
snmpsubagent hostname jimbo communityname public timeout 2600
```

## SNMPSUBAGENTHOST

---

Die Option SNMPSUBAGENTHOST gibt den Standort des IBM Spectrum Protect SNMP-Subagenten (SNMP = Simple Network Management Protocol) an. Der Standardwert für diese Option lautet 127.0.0.1.

### Syntax

---

```
>>-SNMPSUBAGENTHOST--Hostname-----<<
```

### Parameter

---

#### Hostname

Gibt den TCP/IP-Namen oder die Nummer des Hosts an, auf dem sich der IBM Spectrum Protect SNMP-Subagent befindet. Subagent und Server müssen sich auf demselben Knoten befinden.

## Beispiele

---

```
snmpsubagenthost 9.116.23.450
```

## SNMPSUBAGENTPORT

---

Die Option SNMPSUBAGENTPORT gibt die Anschlussnummer des IBM Spectrum Protect SNMP-Subagenten (SNMP = Simple Network Management Protocol) an.

### Syntax

---

```
>>-SNMPSUBAGENTPORT--Anschlussnummer-----<<
```

### Parameter

---

#### Anschlussnummer

Gibt die Anschlussnummer des IBM Spectrum Protect SNMP-Subagenten an. Gültige Werte sind 1000 - 32767. Der Standardwert ist 1521.

## Beispiele

---

```
snmpsubagentport 1525
```

## SSLFIPSMODE

---

Die Option SSLFIPSMODE gibt an, ob der FIPS-Modus (Federal Information Processing Standards) für Secure Sockets Layer (SSL) aktiv ist. Der Standardwert ist NO.

Da SSLv3 nicht vom FIPS-Modus unterstützt wird, wenn SSL mit Clients der Version 6.1 oder Version 5.5 verwendet wird, müssen Sie den FIPS-Modus inaktivieren.

### Syntax

---

```
.-SSLFIPSMODE-----No-----.  
>>+-----+-----<<  
'-SSLFIPSMODE-----+No--+'  
      '-Yes-'
```

### Parameter

---



No

Gibt an, dass der SSL FIPS-Modus auf dem Server nicht aktiv ist. Diese Einstellung ist erforderlich, wenn Clients für Sichern/Archivieren vor IBM Spectrum Protect Version 6.3 die Verbindung zum Server unter Verwendung von SSL herstellen sollen.

Yes

Der Wert YES gibt an, dass der SSL FIPS-Modus auf dem Server aktiv ist. Diese Einstellung beschränkt die SSL-Sitzungsvereinbarung auf die Verwendung von FIPS-konformen Cipher-Suites. Die Angabe von YES wird empfohlen, wenn die SSL-Übertragung aktiviert ist und alle Clients für Sichern/Archivieren die Version 6.3 oder eine höhere Version haben.

Geben Sie Folgendes an, um den SSL FIPS-Modus auf dem Server zu inaktivieren:

```
SSLFIPSMODE no
```

## SSLINITTIMEOUT

---

Die Option SSLINITTIMEOUT gibt die Zeit in Minuten an, die der Server darauf wartet, dass eine SSL-Sitzung (SSL = Secure Sockets Layer) die Initialisierung beendet, bevor der Server die Sitzung abbricht.

Wenn Sie diese Option angeben, wird eine SSL-Sitzung abgebrochen, wenn ein Client, ein Server oder ein Speicheragent nicht für SSL konfiguriert ist und versucht, eine SSL-Sitzung zu starten. Eine SSL-Sitzung wird auch abgebrochen, wenn eine Client-SSL-Sitzung und ein Server nicht mit derselben TLS-Version (TLS = Transport Layer Security) konfiguriert sind. In diesen Situationen kann die SSL-Sitzung möglicherweise nicht vollständig initialisiert werden. Der Server bricht die Sitzung ab, wenn das angegebene Zeitlimit erreicht wird.

### Syntax

---

```
.-2-----.  
>>-SSLINITTIMEout-+-Minuten-+-----<<
```

### Parameter

---

Minuten

Gibt die maximale Anzahl Minuten an, die ein Server darauf wartet, dass eine SSL-Sitzung die Initialisierung beendet. Der Standardwert ist 2 Minuten. Der Mindestwert ist 1 Minute.

### Beispiel

---

```
sslinittimeout 1
```

## SSLTCPADMINPORT

---

Die Option SSLTCPADMINPORT gibt die Anschlussadresse an, an der der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen nur für SSL-aktivierte Sitzungen wartet. Die Sitzungen gelten für den Verwaltungsbefehlszeilenclient.

Anmerkung: Ab IBM Spectrum Protect Version 8.1.2 und Tivoli Storage Manager Version 7.1.8 müssen Sie nicht mehr die Option SSLTCPADMINPORT oder SSLTCPADMINPORT verwenden, um SSL-fähige Sitzungen vom Client zu ermöglichen. Die in der Option TCPADMINPORT oder SSLTCPADMINPORT angegebene Anschlussnummer ist sowohl für TCP/IP-Sitzungen als auch für SSL-fähige Clientsitzungen empfangsbereit.

Die folgenden Typen von Sitzungen verwenden nicht das Protokoll Secure Sockets Layer (SSL):

- Network Data Management Protocol (NDMP)
- Automated Cartridge System Library Software (ACSL)
- Datenbankzurückschreibungsoperationen

Ist die Option ADMINONCLIENTPORT auf NO gesetzt, erfordern SSL-fähige Sitzungen für den Verwaltungsclient unterschiedliche Anschlussnummern für die Optionen SSLTCPADMINPORT und SSLTCPADMINPORT.

Einschränkungen:

Die folgenden Einschränkungen gelten, wenn Sie die Serveranschlüsse, die nur für SSL gelten (SSLTCPADMINPORT und SSLTCPADMINPORT), angeben:

- Wenn Sie den Serveranschluss, der nur für SSL gilt, für LLADDRESS im Befehl DEFINE SERVER oder UPDATE SERVER angeben, müssen Sie auch den Parameter SSL=YES angeben.
- Wenn Sie den Serveranschluss, der nur für SSL gilt, für die Clientoption TCPADMINPORT angeben, müssen Sie auch YES für die SSL-Clientoption angeben.

Der TCP/IP-Kommunikationstreiber muss mit COMMMETHOD TCPIP oder COMMMETHOD V6TCPIP aktiviert werden.

## Syntax

---

```
>>-SSLTCPADMINPort--Anschlussnummer-----<<
```

## Parameter

---

Anschlussnummer

Gibt die Anschlussnummer des Servers an. Gültige Werte sind 1024 - 32767. Es gibt keinen Standardwert.

## Beispiele

---

```
ssltcpadminport 1543
```

## SSLTCPPOINT

---

Die Option SSLTCPPOINT gibt die SSL-Anschlussnummer (SSL = Secure Sockets Layer) nur für SSL-fähige Sitzungen an. Der TCP/IP-Kommunikationstreiber des Servers wartet an diesem Anschluss auf Anforderungen für SSL-aktivierte Sitzungen vom Client.

Wichtig: Ab IBM Spectrum Protect Version 8.1.2 und Tivoli Storage Manager Version 7.1.8 müssen Sie nicht mehr die Option SSLTCPPOINT oder SSLTCPADMINPORT verwenden, um SSL-fähige Sitzungen vom Client zu ermöglichen. Die in der Option TCPPOINT oder TCPADMINPORT angegebene Anschlussnummer ist sowohl für TCP/IP-Sitzungen als auch für SSL-fähige Clientsitzungen empfangsbereit.

Die folgenden Typen von Sitzungen verwenden nicht SSL:

- Network Data Management Protocol (NDMP)
- Automated Cartridge System Library Software (ACSLs)
- Datenbankzurückschreibungsoperationen

Ist die Option ADMINONCLIENTPORT auf NO gesetzt, erfordern SSL-fähige Sitzungen für den Verwaltungsclient unterschiedliche Anschlussnummern für die Optionen SSLTCPADMINPORT und SSLTCPPOINT.

Wenn Sie dieselbe Anschlussnummer für die Optionen SSLTCPPOINT und TCPPOINT angeben, werden nur SSL-Verbindungen akzeptiert und TCP/IP-Verbindungen werden für den Anschluss inaktiviert.

Einschränkungen:

Die folgenden Einschränkungen gelten, wenn Sie die Serveranschlüsse, die nur für SSL gelten (SSLTCPPOINT und SSLTCPADMINPORT), angeben:

- Wenn Sie den Serveranschluss, der nur für SSL gilt, für LLADDRESS im Befehl DEFINE SERVER oder UPDATE SERVER angeben, müssen Sie auch den Parameter SSL=YES angeben.
- Wenn Sie den Serveranschluss, der nur für SSL gilt, für die Clientoption TCPPOINT angeben, müssen Sie auch YES für die SSL-Clientoption angeben.

Der TCP/IP-Kommunikationstreiber muss mit COMMMETHOD TCPIP oder COMMMETHOD V6TCPIP aktiviert werden.

## Syntax

---

```
>>-SSLTCPPOINT--Anschlussnummer-----<<
```

## Parameter

---

Anschlussnummer

Gibt die Anschlussnummer des Servers an. Gültige Werte sind 1024 - 32767. Es gibt keinen Standardwert.

## Beispiele

---

```
ssltcpport 1542
```

## TCPADMINPORT

---

Die Option TCPADMINPORT gibt die Nummer des Anschlusses an, an dem der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen für andere TCP/IP-Sitzungen und SSL-fähige Sitzungen als Clientsitzungen wartet. Dazu gehören Verwaltungssitzungen, Sitzungen zwischen Servern, Speicheragentensitzungen, Speicherarchivclientsitzungen, Sitzungen verwalteter Server und Ereignisserverversitzungen.

Durch die Verwendung verschiedener Anschlussnummern für die Optionen TCPPORT und TCPADMINPORT können Sie eine Gruppe mit Firewall-Regeln für Clientsitzungen und eine andere Gruppe für die zuvor aufgelisteten Sitzungstypen erstellen. Durch die Verwendung des Parameters SESSIONINITIATION im Befehl REGISTER NODE und UPDATE NODE können Sie den durch TCPPORT an der Firewall angegebenen Anschluss schließen und Knoten angeben, deren geplante Sitzungen vom Server gestartet werden. Sind die beiden Anschlussnummern verschieden, werden separate Threads für Clientsitzungen und die anderen Sitzungstypen verwendet. Sollen die beiden Optionen dieselbe Anschlussnummer verwenden (standardmäßig oder durch explizites Setzen der Optionen auf dieselbe Anschlussnummer), wird ein einzelner Serverthread für alle Sitzungsanforderungen verwendet.

Clientsitzungen, die versuchen, den durch TCPADMINPORT angegebenen Anschluss zu verwenden, werden beendet (wenn TCPPORT und TCPADMINPORT verschiedene Anschlüsse angeben). Verwaltungssitzungen sind an beiden Anschlüssen zulässig, (sofern nicht die Option ADMINONCLIENTPORT auf NO gesetzt ist), sie verwenden jedoch standardmäßig den durch TCPADMINPORT angegebenen Anschluss.

Für SSL-fähige Sitzungen, die die Option TCPADMINPORT verwenden, gelten dieselben Einschränkungen wie bei der Option SSLTCPADMINPORT. Die folgenden Typen von Sitzungen verwenden nicht das Protokoll Secure Sockets Layer (SSL):

- Network Data Management Protocol (NDMP)
- Automated Cartridge System Library Software (ACSL)
- Datenbankzurückschreibungsoperationen

Ist die Option ADMINONCLIENTPORT auf NO gesetzt, erfordern SSL-fähige Sitzungen für den Verwaltungsclient unterschiedliche Anschlussnummern für die Optionen TCPADMINPORT und TCPPORT.

## Syntax

---

```
>>-TCPADMINPort--Anschlussnummer-----<<
```

## Parameter

---

Anschlussnummer

Gibt die Anschlussnummer des Servers an. Gültige Werte sind 1024 - 32767. Der Standardwert ist der Wert von TCPPORT.

## Beispiele

---

```
tcpadminport 1502
```

## TCPBUFSIZE

---

Die Option TCPBUFSIZE gibt die Größe des Puffers an, der für TCP/IP-Sendeanforderungen verwendet wird. Während einer Zurückschreibung werden Clientdaten aus der IBM Spectrum Protect-Sitzungskomponente in einen TCP-DFV-Treiber versetzt. Die Option TCPBUFSIZE bestimmt, ob der Server die Daten direkt aus dem Sitzungspuffer sendet oder die Daten in den TCP-Puffer kopiert. Eine Puffergröße von 32 KB zwingt den Server dazu, Daten in den Kommunikationspuffer zu kopieren und den Inhalt des Puffers zu löschen, wenn er gefüllt ist.

Anmerkung: Diese Option ist nicht mit der Option TCPWINDOWSIZE verbunden.

## Syntax

---

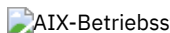
```
>>-TCPBufsize--Kilobyte-----<<
```


## Parameter

---

Kilobyte

Gibt die Größe des Puffers, der für TCP/IP-Sendeanforderungen verwendet wird, in Kilobyte an.

 Der Wertebereich liegt zwischen 1 und 64. Der Standardwert ist 32.

 Linux-Betriebssysteme Der Wertebereich liegt zwischen 1 und 64. Der Standardwert ist 16.

## Beispiele

---

```
tcpbufsize 5
```

## TCPNODELAY

---

Die Option TCPNODELAY gibt an, ob der Server die Verzögerung beim Senden von aufeinanderfolgenden kleinen Paketen im Netz inaktiviert.

Ändern Sie den Standardwert YES nur unter einer der folgenden Bedingungen:

- Sie werden angewiesen, die Option durch Ihren Kundendienst ändern zu lassen.
- Sie kennen die Auswirkungen des TCP-Nagle-Algorithmus bei Übertragungen im Netz. Wird die Option auf NO gesetzt, wird der Nagle-Algorithmus aktiviert, der das Senden kleiner aufeinanderfolgender Pakete verzögert.

## Syntax

---

```
>>-TCPNodelay--+-Yes-+-----<<  
                '-No--'
```

## Parameter

---

Yes

Gibt an, dass der Server das sofortige Senden aufeinanderfolgender kleiner Pakete im Netz zulässt. Wird diese Option auf YES gesetzt, kann die Leistung in einigen Hochgeschwindigkeitsnetzen verbessert werden. Der Standardwert ist YES.

No

Gibt an, dass der Server das sofortige Senden aufeinanderfolgender kleiner Pakete im Netz nicht zulässt

## Beispiele

---

```
tcpnodelay no
```

## TCPPORT

---

Die Option TCPPORT gibt die Nummer des Anschlusses an, an dem der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen für Clientsitzungen wartet. Der TCP/IP-Kommunikationstreiber des Servers ist an diesem Anschluss sowohl für TCP/IP-Sitzungen als auch für SSL-fähige Sitzungen vom Client empfangsbereit.


Durch die Verwendung verschiedener Anschlussnummern für die Optionen TCPPORT und TCPADMINPORT können Sie eine Gruppe mit Firewallregeln für Clientsitzungen und eine andere Gruppe für andere Sitzungstypen erstellen (Verwaltungssitzungen, Sitzungen zwischen Servern, Speicheragentensitzungen, Speicherarchivclientsitzungen, Sitzungen verwalteter Server und Ereignisserversitzungen). Sind die beiden Anschlussnummern verschieden, werden separate Threads für Clientsitzungen und die anderen Sitzungstypen verwendet. Sollen die beiden Optionen dieselbe Anschlussnummer verwenden (standardmäßig oder durch explizites Setzen der Optionen auf dieselbe Anschlussnummer), wird ein einzelner Serverthread für alle Sitzungsanforderungen verwendet.

Für SSL-fähige Clientsitzungen, die die Option TCPPORT verwenden, gelten dieselben Einschränkungen wie bei der Option SSLTCPPOINT. Die folgenden Typen von Sitzungen verwenden nicht SSL:

- Network Data Management Protocol (NDMP)
- Automated Cartridge System Library Software (ACSLs)
- Datenbankzurückschreibungsoperationen

Ist die Option ADMINONCLIENTPORT auf NO gesetzt, erfordern SSL-fähige Sitzungen für den Verwaltungsclient unterschiedliche Anschlussnummern für die Optionen TCPADMINPORT und TCPPOINT.

Wenn Sie dieselbe Anschlussnummer für die beiden Optionen SSLTCPPOINT und TCPPOINT angeben, werden nur SSL-Verbindungen akzeptiert und TCP/IP-Verbindungen werden für den Anschluss inaktiviert.

 Windows-Betriebssysteme Sie können diese Option mit dem Befehl SETOPT ändern. Wenn Sie einen Anschluss ändern, ist der IBM Spectrum Protect-Server sofort an dem neuen Anschluss empfangsbereit. Alle aktuellen Verbindungen bleiben im Gebrauch, bis sie geschlossen werden.

## Syntax

---

```
>>-TCPport--Anschlussnummer-----<<
```

## Parameter

---

Anschlussnummer

Gibt die Anschlussnummer des Servers an. Gültige Werte sind 1024 - 32767. Der Standardwert ist 1500.

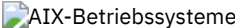

```
tcpport 1500
```

## TCPWINDOWSIZE

---

Die Option TCPWINDOWSIZE gibt den Umfang (in Kilobyte) der Empfangsdaten an, die bei einer TCP/IP-Verbindung gleichzeitig gepuffert werden können. Der sendende Host kann erst dann weitere Daten senden, wenn er eine Bestätigung und eine Aktualisierung des TCP-Empfangsfensters empfängt. Jedes TCP-Paket enthält das entsprechende TCP-Empfangsfenster in der Verbindung. Bei einem größeren Fenster kann der Sender mit dem Senden von Daten fortfahren. Außerdem wird möglicherweise die Übertragungsleistung verbessert, besonders in schnellen Netzen mit hoher Latenzzeit.

Anmerkung:

- Um die Leistung beim Sichern zu verbessern, den Wert für TCPWINDOWSIZE auf dem Server vergrößern. Um die Leistung beim Zurückschreiben zu verbessern, den Wert für TCPWINDOWSIZE auf dem Client vergrößern.
- Das TCP-Fenster agiert als Puffer in dem Netz.
- Überschreitet die Fenstergröße den Pufferspeicherbereich auf dem Netzadapter, kann sich der Durchsatz aufgrund des erneuten Sendens von Paketen, die auf dem Adapter verlorengegangen sind, verschlechtern.
-   Die Option TCPWINDOWSIZE ist nicht mit der Option TCPBUFFSIZE und nicht mit den Sende- und Empfangspuffern verbunden, die im Client- oder Serverspeicher zugeordnet sind.

## Syntax

---

```
>>-TCPWindowsize--Kilobyte-----<<
```

## Parameter

---

Kilobyte

Gibt die Größe, die für das TCP/IP-Schiebefenster für den Clientknoten verwendet werden soll, in Kilobyte an. Es kann ein Wert von 0 bis 2048 angegeben werden. Der Standardwert ist 63. Wird 0 angegeben, verwendet der Server die Standardfenstergröße, die durch das Betriebssystem definiert wird. Werte von 1 bis 2048 geben an, dass sich die Fenstergröße in dem Bereich 1 KB bis 2 MB befindet.

## Beispiele

---

```
tcpwindowsize 63
```

## TECBEGINEVENTLOGGING

---

Die Option TECBEGINEVENTLOGGING gibt an, ob die Ereignisprotokollierung für den TIVOLI-Empfänger beim Serverstart beginnen soll. Wird die Option TECHOST angegeben, wird für TECBEGINEVENTLOGGING standardmäßig der Wert YES angenommen.

## Syntax

---

```
>>-TECBegineventlogging--+-Yes-+-----<<  
'-No--'
```

## Parameter

---

Yes

- No
- Gibt an, dass die Ereignisprotokollierung beginnt, wenn der Server gestartet wird und die Option TECHOST angegeben ist.
- Gibt an, dass die Ereignisprotokollierung nicht beim Serverstart beginnen soll. Soll die Ereignisprotokollierung für den TIVOLI-Empfänger später beginnen (wenn die Option TECHOST angegeben wurde), muss der Befehl BEGIN EVENTLOGGING ausgegeben werden.

## Beispiele

---

```
tecbegineventlogging yes
```

## TECHOST

---

Die Option TECHOST gibt den Hostnamen oder die IP-Adresse für den Tivoli-Ereignisserver an.

### Syntax

---

```
>>-TECHost--Hostname-----<<
```

### Parameter

---

Hostname  
Gibt den Hostnamen oder die IP-Adresse für den Tivoli-Ereignisserver an.

## Beispiele

---

```
techost 9.114.22.345
```

## TECPORT

---

Die Option TECPORT gibt die TCP/IP-Anschlussadresse an, an der der Tivoli-Ereignisserver empfangsbereit ist. Diese Option ist nur erforderlich, wenn sich der Tivoli-Ereignisserver auf einem System befindet, auf dem der Service 'Port Mapper' nicht ausgeführt wird.



### Syntax

---

```
>>-TECPort--Anschlussnummer-----<<
```

### Parameter

---

Anschlussnummer  
Gibt die Anschlussadresse des Tivoli-Ereignisservers an. Der Wert muss zwischen 0 und 32767 liegen.  AIX-Betriebssysteme  
 Linux-Betriebssysteme Diese Option ist nicht erforderlich.

## Beispiele

---

```
tecport 1555
```

## TECUTF8EVENT

---

Die Option TECUTF8EVENT ermöglicht es dem IBM Spectrum Protect-Administrator, Informationen im UTF-8-Datenformat an den Tivoli Enterprise Console (TEC)-Server zu senden. Der Standardwert ist 'No'. Mit dem Befehl QUERY OPTION können Sie abfragen, ob diese Option aktiviert ist.

### Syntax

---

```
>>-TECUTF8event--+Yes+-----<<  
'-No--'
```

### Parameter

---

Yes

Gibt an, dass der IBM Spectrum Protect-Server das TEC-Ereignis in UTF-8 verschlüsselt, bevor das Ereignis an den TEC-Server ausgegeben wird.

No

Gibt an, dass der IBM Spectrum Protect-Server das TEC-Ereignis nicht in UTF-8 verschlüsselt. Das Ereignis wird im ASCII-Format an den TEC-Server ausgegeben.

## Beispiele

---

```
tecutf8event yes
```

## THROUGHPUTDATATHRESHOLD

---

Die Option THROUGHPUTDATATHRESHOLD gibt eine Durchsatzschwelle an, die eine Clientsitzung erreichen muss, damit sie nicht abgebrochen wird, wenn die Zeitschwelle erreicht wird.

Diese Option wird zusammen mit der Serveroption THROUGHPUTTIMETHRESHOLD verwendet, die den Wert für die Zeitschwelle plus die Zeit für das Warten auf Datenträger definiert. Die Zeitschwelle beginnt, wenn der Client beginnt, Daten zum Speichern an den Server zu senden (im Gegensatz zu Konfigurations- oder Sitzungsverwaltungsdaten).

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

## Syntax

---

```
>>-THROUGHPUTDatathreshold-- Kilobyte_pro_Sekunde-----<<
```

## Parameter

---

Kilobyte pro Sekunde

Gibt den Durchsatz an, den Clientsitzungen erreichen müssen, um ihren Abbruch zu vermeiden, wenn die mit THROUGHPUTTIMETHRESHOLD angegebenen Minuten verstrichen sind. Diese Schwelle enthält nicht die Zeit, die auf das Laden der Datenträger gewartet wird. Der Wert 0 gibt an, dass die Clientsitzungen nicht auf unzureichenden Durchsatz überprüft werden. Der Durchsatz wird berechnet, indem gesendete und empfangene Byte addiert und durch die Länge der Sitzung dividiert werden. Die Länge enthält nicht die Zeit, die auf das Laden der Datenträger gewartet wird, und beginnt mit dem Zeitpunkt, zu dem ein Client Daten zum Speichern an den Server sendet. Der Standardwert ist 0. Der Mindestwert ist 0; der Maximalwert ist 99999999.

## Beispiele

---

Angaben, dass der Server 90 Minuten plus Datenträgerwartezeit warten soll, nachdem eine Sitzung mit dem Senden von Daten begonnen hat, bis überprüft wird, ob die Sitzung aufgrund zu geringen Durchsatzes abgebrochen werden soll. Erreicht eine Sitzung keine Übertragungsrate von 50 KB pro Sekunde, wird sie abgebrochen.

```
throughputtimethreshold 90  
Throughputdatathreshold 50
```

## THROUGHPUTTIMETHRESHOLD

---

Die Option THROUGHPUTTIMETHRESHOLD gibt die Zeitschwelle für eine Sitzung an, nach deren Ablauf die Sitzung aufgrund zu geringen Durchsatzes abgebrochen werden kann.

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

## Syntax

---

```
>>-THROUGHPUTTimethreshold--Minuten-----<<
```

## Parameter

---

Minuten


Gibt die Schwelle für das Überprüfen von Clientsitzungen und deren Abbruch an, wenn die Datendurchsatzschwelle nicht erreicht wird (siehe Serveroption THROUGHPUTDATATHRESHOLD). Diese Schwelle enthält nicht die Zeit, die auf das Laden der Datenträger gewartet wird. Die Zeitschwelle beginnt, wenn ein Client beginnt, Daten zum Speichern an den Server zu senden (im Gegensatz zu Konfigurations- oder Sitzungsverwaltungsdaten). Der Wert 0 gibt an, dass die Clientsitzungen nicht auf zu geringen Durchsatz überprüft werden. Der Standardwert ist 0. Der Mindestwert ist 0; der maximale Wert ist 99999999.

## Beispiele

---

Angeben, dass der Server 90 Minuten plus Datenträgerwartezeit warten soll, nachdem eine Sitzung mit dem Senden von Daten begonnen hat, bis überprüft wird, ob die Sitzung abgebrochen werden soll. Erreicht eine Sitzung keine Übertragungsrate von 50000 Byte pro Sekunde, wird sie abgebrochen.

```
throughputtimethreshold 90
Throughputdatathreshold 50
```

 Windows-Betriebssysteme

## TIMEFORMAT

---

Die Option TIMEFORMAT gibt das Format an, in dem Uhrzeitangaben vom Server angezeigt werden.

Der Wert für die Option TIMEFORMAT wird von dem in den länderspezifischen Angaben definierten Uhrzeitformat überschrieben, wenn die länderspezifischen Angaben beim Starten des Servers erfolgreich initialisiert wurden. Die länderspezifischen Angaben werden in der Option LANGUAGE angegeben.

## Syntax

---

```
>>-TIMEformat--Formatnummer-----<<
```

## Parameter

---

Formatnummer

Eine Zahl von 1 bis 4 auswählen, um das vom Server verwendete Uhrzeitformat anzugeben. Der Standardwert ist 1.

- |   |                        |
|---|------------------------|
| 1 | hh:mm:ss               |
| 2 | hh,mm,ss               |
| 3 | hh.mm.ss               |
| 4 | hh:mm:ss a.m oder p.m. |
| 5 | a.m oder p.m. hh:mm:ss |

## Beispiele

---

```
timeformat 4
```

## TXNGROUPMAX

---

Die Option TXNGROUPMAX gibt die Anzahl der Objekte an, die als Gruppe zwischen einem Client und dem Server zwischen Transaktions-COMMIT-Punkten übertragen werden. Der Mindestwert beträgt 4 Objekte und der Maximalwert beträgt 65000 Objekte. Der Standardwert ist 4096 Objekte. Bei den übertragenen Objekten handelt es sich um tatsächliche Dateien, Verzeichnisse oder beides. Der Server zählt jede Datei oder jedes Verzeichnis als ein Objekt.

Es ist möglich, die Leistung bei Clientsicherungsoperationen, Archivierungsoperationen, Zurückschreibungsoperationen und Abrufoperationen durch die Verwendung eines höheren Werts für diese Option zu beeinflussen:

1. Wird der Wert für die Option TXNGROUPMAX erheblich vergrößert, achten Sie auf mögliche Auswirkungen auf das Wiederherstellungsprotokoll. Ein größerer Wert für die Option TXNGROUPMAX kann zu einer erhöhten Auslastung des Wiederherstellungsprotokolls sowie zu einer längeren Zeit bis zu einer Transaktionsfestschreibung führen. Bei besonders schweren Auswirkungen können Probleme beim Betrieb des Servers auftreten.



2. Die Erhöhung des Wertes der Option TXNGROUPMAX kann den Durchsatz für Operationen verbessern, die Daten direkt auf Band speichern. Dies gilt besonders, wenn eine große Anzahl Objekte gespeichert wird. Ein höherer Wert der Option TXNGROUPMAX kann jedoch auch die Anzahl der Objekte erhöhen, die erneut gesendet werden müssen, wenn die Transaktion gestoppt wird, weil eine Eingabedatei während der Sicherung geändert wurde oder weil ein neuer Speicherdatenträger erforderlich war. Je größer der Wert der Option TXNGROUPMAX ist, desto mehr Daten müssen erneut gesendet werden.
3. Die Erhöhung des Werts für TXNGROUPMAX hat Auswirkungen auf die Flexibilität beim Stoppen der Operation, und der Client muss möglicherweise länger warten, bis die Transaktion abgeschlossen ist.

Sie können den Wert dieser Option für einzelne Clientknoten überschreiben. Siehe Parameter TXNGROUPMAX in REGISTER NODE (Knoten registrieren) und UPDATE NODE (Attribute eines Knotens aktualisieren).

Diese Option steht im Zusammenhang mit der Option TXNBYTELIMIT in der Clientoptionsdatei. TXNBYTELIMIT steuert die Anzahl Byte (im Gegensatz zur Anzahl Objekte), die zwischen Transaktions-COMMIT-Punkten übertragen werden. Bei Beendigung der Übertragung eines Objekts schreibt der Client die Transaktion fest, wenn die Anzahl der während der Transaktion übertragenen Byte den Wert von TXNBYTELIMIT erreicht oder überschreitet, unabhängig von der Anzahl der übertragenen Objekte.

## Syntax

---

```
>>-TXNGroupmax--Anzahl_der_Objekte-----<<
```

## Parameter

---

Anzahl\_der\_Objekte

Gibt eine Zahl von 4 bis 65000 für die maximale Anzahl Objekte pro Transaktion an. Der Standardwert ist 4096.

## Beispiele

---

```
txngroupmax 4096
```

# UNIQUETDPTEEVENTS

---

Die Option UNIQUETDPTEEVENTS generiert eine eindeutige Tivoli Enterprise Console (TEC)-Ereignisklasse für jede einzelne IBM Spectrum Protect-Nachricht, einschließlich Client-, Server- und IBM Spectrum Protect Data Protection-Clientnachrichten. Der Standardwert ist 'No'.

## Syntax

---

```
>>-UNIQUETDPteevents--+-Yes+-----<<
                        '-No--'
```

## Parameter

---

Yes

Gibt an, dass eindeutige IBM Spectrum Protect Data Protection-Nachrichten an den TEC-Ereignisserver gesendet werden. UNIQUETEEvents wird dynamisch auf YES gesetzt.

No

Gibt an, dass allgemeine Nachrichten an den TEC-Ereignisserver gesendet werden.

## Beispiele

---

```
uniquetdpteevents yes
```

# UNIQUETECEVENTS

---

Die Option UNIQUETECEVENTS generiert eine eindeutige Tivoli Enterprise Console (TEC)-Ereignisklasse für jede einzelne IBM Spectrum Protect-Nachricht. Der Standardwert ist 'No'.

## Syntax

---

```
>>-UNIQUETEEvents--+-Yes+-----<<
```

'-No--'

## Parameter

---

Yes

Gibt an, dass eindeutige Nachrichten an den TEC-Ereignisserver gesendet werden.

No

Gibt an, dass allgemeine Nachrichten an den TEC-Ereignisserver gesendet werden.

## Beispiele

---

```
uniquetecevents yes
```

## USEREXIT

---

Die Option USEREXIT gibt einen benutzerdefinierten Ausgang an, dem die Steuerung für die Verwaltung eines Ereignisses übergeben wird.

## Syntax

---

```
>>-USEREXIT---+-Yes---Modulname-----DLL-Name----->
                (1)           (2)
                '-No--'

>--Funktion-----><
                (3)
```

Anmerkungen:

1. *Modulname* ist nur unter AIX, HP-UX, Linux, Solaris und z/OS verfügbar.
2. *DLL-Name* ist nur unter Windows verfügbar.
3. *Funktion* ist nur unter Windows verfügbar.

## Parameter



---




Yes



Gibt an, dass das Ereignisprotokoll für den Benutzerausgangsempfänger automatisch beim Serverstart gestartet wird.

No



Gibt an, dass das Ereignisprotokoll für den Benutzerausgangsempfänger nicht automatisch beim Serverstart gestartet wird. Wurde dieser Parameter angegeben, muss das Ereignisprotokoll manuell durch Eingabe des Befehls BEGIN EVENTLOGGING gestartet werden.


  Modulname



   Gibt den Modulnamen des Benutzerausgangs an.

  Dies ist der Name einer gemeinsam benutzten Bibliothek, die den Ausgang enthält. Der Modulname kann entweder ein vollständig qualifizierter Pfadname oder nur der Modulname selbst sein. Handelt es sich nur um den Modulnamen, wird er aus dem aktuellen Verzeichnis geladen.

 DLL-Name

  Gibt den DLL-Namen an, der die Benutzerausgangsfunktion enthält.

 Funktion

  Gibt den Namen der Benutzerausgangsfunktion in der DLL an.

## Beispiele

---

```
userexit yes dllname.dll dllmodulename
```

```
userexit yes fevent.exit
```

## VERBCECK

---

Die Option VERBCHECK gibt an, dass der Server eine zusätzliche Fehlerprüfung für die Struktur der Befehle durchführt, die vom Client gesendet werden. Diese Option sollte nur aktiviert werden, wenn der Client nicht ordnungsgemäß gebildete Anforderungen an den Server sendet, die zum Absturz des Servers führen. Ist diese Option aktiviert, hat dies einen Protokollfehler an Stelle eines Serverabsturzes zur Folge.

## Syntax

---

```
>>-VERBCHECK-----<<
```

## Parameter

---

Keine.

## Beispiele

---

Zusätzliche Fehlerprüfung für Befehle aktivieren, die vom Client gesendet werden:

```
verbcheck
```

## VOLUMEHISTORY

---

Die Option VOLUMEHISTORY gibt den Namen von Dateien an, die automatisch aktualisiert werden sollen, wenn History-Informationen von sequenziellen Datenträgern des Servers sich ändern. Für diese Option gibt es keinen Standardwert.

Es können eine oder mehrere Optionen VOLUMEHISTORY in die Serveroptionsdatei eingeschlossen werden. Wird mit mehreren VOLUMEHISTORY-Optionen gearbeitet, aktualisiert der Server automatisch die Datenträger-History-Informationen in jeder angegebenen Datei und speichert eine Sicherungskopie.

## Syntax

---

```
>>-VOLUMEHistory--Dateiname-----<<
```

## Parameter

---

Dateiname

Gibt den Namen der Datei an, in der der Server eine Sicherungskopie der gesammelten Datenträger-History-Informationen speichern soll.

## Beispiele

---

```
volumehistory volhist.out
```



## Serverdienstprogramme

---

Verwenden Sie Serverdienstprogramme, um spezielle Tasks auf dem Server auszuführen, während der Server nicht aktiv ist.

-  Windows-BetriebssystemeDSMMAXSG (Blockgröße für das Schreiben von Daten erhöhen)  
Verwenden Sie das Dienstprogramm DSMMAXSG, um die maximale Übertragungslänge für Host Bus Adapter (HBAs) zu erhöhen. Damit wird die Blockgröße erhöht, die vom IBM Spectrum Protect-Server zum Schreiben von Daten auf bestimmte Typen von Bandlaufwerken und zum Abrufen von Daten von bestimmten Typen von Bandlaufwerken verwendet wird.
- DSMSERV (Server starten)  
Verwenden Sie dieses Dienstprogramm, um den IBM Spectrum Protect-Server zu starten.
-  AIX-Betriebssysteme  Linux-BetriebssystemeServerstartscript: rc.dsmserv  
Sie können das Script rc.dsmserv in Ihrem Systemstart verwenden, um eine Serverinstanz unter einer bestimmten Benutzer-ID automatisch zu starten.
-  Linux-BetriebssystemeServerstartscript: dsmserv.rc  
Sie können das Script dsmserv.rc verwenden, um eine Serverinstanz zu stoppen oder einen Server manuell oder automatisch zu starten.
- DSMSERV DISPLAY DBSPACE (Informationen zum Datenbankspeicherbereich anzeigen)  
Verwenden Sie dieses Dienstprogramm, um Informationen zum Speicherbereich anzuzeigen, der für die Datenbank definiert ist.

Die Ausgabe dieses Dienstprogramms entspricht der Ausgabe von QUERY DBSPACE, aber Sie können dieses Dienstprogramm verwenden, wenn der Server nicht aktiv ist.

- **DSMSERV DISPLAY LOG** (Informationen zum Wiederherstellungsprotokoll anzeigen)  
Mit diesem Dienstprogramm können Sie Informationen zu Wiederherstellungsprotokollen anzeigen, einschließlich der aktiven Protokolldatei, dem Spiegel für die aktive Protokolldatei, dem Übernahmeverzeichnis für das Archivprotokoll und dem Überlaufstandort für die Protokolle. Verwenden Sie dieses Dienstprogramm, wenn der Server nicht aktiv ist.
- **DSMSERV EXTEND DBSPACE** (Speicherbereich für die Datenbank vergrößern)  
Verwenden Sie dieses Dienstprogramm, um den Speicherbereich für die Datenbank zu vergrößern, indem Verzeichnisse für die Datenbank hinzugefügt werden. Dieses Dienstprogramm führt dieselbe Funktion wie der Befehl EXTEND DBSPACE aus, aber Sie können es verwenden, wenn der Server nicht aktiv ist.
- **DSMSERV FORMAT** (Datenbank und Protokoll formatieren)  
Verwenden Sie das Dienstprogramm DSMSERV FORMAT, um die Serverdatenbank und das Wiederherstellungsprotokoll zu initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls sind keine anderen Serveraktivitäten zulässig.
- **DSMSERV INSERTDB** (Serverdatenbank in eine leere Datenbank versetzen)  
Verwenden Sie das Dienstprogramm DSMSERV INSERTDB, um eine Serverdatenbank in eine neue Datenbank zu versetzen. Die Datenbank kann vom ursprünglichen Server extrahiert und in eine neue Datenbank auf dem neuen Server eingefügt werden, indem eine Netzverbindung zwischen den beiden Servern verwendet wird. Die Datenbank kann auch von Datenträgern eingefügt werden, die die extrahierte Datenbank enthalten.
- **DSMSERV LOADFORMAT** (Datenbank formatieren)  
Verwenden Sie das Dienstprogramm DSMSERV LOADFORMAT, wenn ein Upgrade von Version 5 durchgeführt wird. Das Dienstprogramm formatiert eine leere Datenbank als Vorbereitung zum Einfügen einer extrahierten Datenbank in die leere Datenbank.
- **DSMSERV REMOVEDB** (Datenbank entfernen)  
Verwenden Sie das Dienstprogramm DSMSERV REMOVEDB, um eine IBM Spectrum Protect-Serverdatenbank zu entfernen.
- **DSMSERV RESTORE DB** (Datenbank zurückschreiben)  
Mit diesem Dienstprogramm können Sie eine Datenbank mit Hilfe einer Datenbanksicherung zurückschreiben.
-  **Windows-Betriebssysteme DSMSERV UPDATE** (Registry-Einträge für eine Serverinstanz erstellen)  
Verwenden Sie dieses Dienstprogramm, um Registry-Einträge für eine IBM Spectrum Protect-Serverinstanz zu erstellen, wenn die Einträge versehentlich gelöscht wurden.
-  **AIX-Betriebssysteme**  **Linux-Betriebssysteme DSMULOG** (IBM Spectrum Protect-Servernachrichten in einer Benutzerprotokolldatei speichern)  
Verwenden Sie diesen Befehl, um Nachrichten der IBM Spectrum Protect-Server-Konsole in einer Benutzerprotokolldatei zu speichern. Sie können angeben, dass IBM Spectrum Protect Nachrichten in mehrere Benutzerprotokolldateien schreiben soll.

 Windows-Betriebssysteme

## DSMMAXSG (Blockgröße für das Schreiben von Daten erhöhen)

---

Verwenden Sie das Dienstprogramm DSMMAXSG, um die maximale Übertragungslänge für Host Bus Adapter (HBAs) zu erhöhen. Damit wird die Blockgröße erhöht, die vom IBM Spectrum Protect-Server zum Schreiben von Daten auf bestimmte Typen von Bandlaufwerken und zum Abrufen von Daten von bestimmten Typen von Bandlaufwerken verwendet wird.

Mit diesem Dienstprogramm beträgt die maximale Blockgröße, die angegeben werden kann, 256 KB. Abhängig von Ihrer Systemumgebung kann mit der Erhöhung der Blockgröße die Geschwindigkeit verbessert werden, mit der IBM Spectrum Protect Daten für Sicherungs- und Zurückschreibungsoperationen sowie für Archivierungs- und Abrufoperationen verarbeitet. Das Dienstprogramm hat jedoch keine Auswirkungen auf die Generierung von Sicherungsgruppen.

Sie können Bandlaufwerke verwenden, die nur an SCSI- oder Fibre-Channel-HBAs angeschlossen sind und die folgenden Einheitentypen haben:

- 3590
- 3592
- DLT
- ECARTRIDGE
- LTO

Das Dienstprogramm wird im Rahmen der Installation des IBM Spectrum Protect-Servers und des Speicheragenten automatisch ausgeführt. Wenn Sie jedoch nach der Installation eines Servers oder eines Speicheragenten einen neuen HBA auf Ihrem System installieren oder wenn Sie eine neue Version eines vorhandenen HBA-Einheitentreibers installieren, mit der der Wert der maximalen Übertragungsgröße zurückgesetzt wird, müssen Sie das Dienstprogramm manuell ausführen, um die Vorteile der größeren Blockgröße zu nutzen.

Wird dieses Dienstprogramm ausgeführt, wird ein Registrierungsschlüssel für jeden HBA-Treiber auf dem System geändert. Der Name des Schlüssels ist MaximumSGList.

Einschränkung: Werden Daten unter Verwendung der Blockgröße von 256 KB auf Band gesichert oder archiviert, kann das Band nicht unter Verwendung eines HBAs angehängt oder gelesen werden, der die Blockgröße von 256 KB nicht unterstützt. Verwenden Sie beispielsweise ein 256-KB-Windows-System zum Sichern von Clientdaten auf dem IBM Spectrum Protect-Server, können Sie die Daten nicht mit einem Windows-System zurückschreiben, das eine andere Übertragungslänge unterstützt. Soll das Band angehängt oder von dem Band gelesen werden, das unter Verwendung einer Übertragungslänge von 256 KB beschrieben wurde, müssen Sie einen HBA installieren, der 256-KB-Übertragungen unterstützt.

## Syntax

```
>>-dsmmaxsg-----><
```

## Beispiel: Die Blockgröße zum Schreiben von Daten erhöhen


Das Dienstprogramm DSMMAXSG ausführen, um die Blockgröße zu erhöhen, die von IBM Spectrum Protect verwendet wird.




```
dsmmaxsg
```

## DSMSERV (Server starten)

Verwenden Sie dieses Dienstprogramm, um den IBM Spectrum Protect-Server zu starten.

Einschränkungen:

- Geben Sie maximal 1022 Zeichen in der DSMSERV-Konsolenbefehlszeilenschnittstelle ein. Text, der 1022 Zeichen überschreitet, wird abgeschnitten.
-  Windows-Betriebssysteme Die folgenden Parameter schließen sich gegenseitig aus:
  - NOEXPIRE
  - RUNFILE
  - MAINTENANCE

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Syntax

```
>>-DSMSERV----->
      | (1) |
      |----- -u--Benutzername- |
>----->
      | (1) |
      |----- -i--Instanzverzeichnis- |
      (2) .- -k--Server1----- .
>----->
      |'- -k--Schlüsselname-' | (1) |
      |----- -noexpire- |
>----->
      | (3) | |'- -o--Optionsdatei-' |
      |-----NOEXPIRE- |
>-----><
      | (1) | |+-RUNFILE--Dateiname-+ |
      |----- -quiet- | | (4) |
      |----- -MAINTenance----- |
```

Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.
3. Dieser Parameter gilt nur für Windows-Server.
4. Dieser Parameter gilt nur für AIX-, Linux- und Windows-Server.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

## Parameter

-u Benutzername

Gibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server gestartet wird. Um den Server mit der Rootbenutzer-ID zu starten, müssen Sie den Parameter -u angeben und die Anweisungen in Server mit der Rootbenutzer-ID starten befolgen.

-i Instanzverzeichnis

Gibt ein Instanzverzeichnis an, das verwendet werden soll. Das Instanzverzeichnis wird das aktuelle Arbeitsverzeichnis des Servers.

-k Schlüsselname

Gibt den Namen des Windows-Registrierungsschlüssels an, aus dem Informationen zum Server abgerufen werden sollen. Der Standardwert ist Server1.

-noexpire

Gibt an, dass der Server keine verfallenen Dateien aus der Serverdatenbank entfernt. Die Dateien werden beim Start des Servers nicht aus dem Serverspeicher gelöscht.

NOEXPIRE

Gibt an, dass der Server keine verfallenen Dateien aus der Serverdatenbank entfernt. Die Dateien werden beim Start des Servers nicht aus dem Serverspeicher gelöscht.

-o Optionsdatei

Gibt eine Optionsdatei an, die verwendet werden soll.

-quiet

Gibt an, dass Nachrichten an die Konsole unterdrückt werden.

MAIN Tenance

Gibt an, dass der Server im Verwaltungsmodus gestartet wird und Zeitpläne für Verwaltungsbefehle, Clientzeitpläne, Clientsitzungen, Wiederherstellung des Speicherbereichs, Bestandsverfall und Speicherpoolumlagerung inaktiviert sind.

Tipp: Der Verwaltungsmodus ist die bevorzugte Methode für die Ausführung des Servers während der Ausführung von Verwaltungs- oder Rekonfigurationstasks. Wenn der Server im Verwaltungsmodus ausgeführt wird, werden Operationen, die Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, automatisch inaktiviert.

RUNFILE Dateiname

Gibt den Namen einer Textdatei an, die auf dem Server ausgeführt werden soll. Die Datei enthält eine Liste mit Serverbefehlen.

Achtung: Wenn der Parameter RUNFILE verwendet wird, hält der Server an, nachdem die Verarbeitung abgeschlossen wurde. Sie müssen den Server mit dem Dienstprogramm DSMSEV erneut starten.

## Beispiel: Den Server starten

---

Starten Sie den Server für den normalen Betrieb. Geben Sie den folgenden Befehl in einer einzigen Zeile aus:

```
LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K  
usr/bin/dsmserv
```

Stellen Sie sicher, dass Sie hinter `SHMPSIZE=64K` ein Leerzeichen einfügen. Wenn Sie den Server mit diesem Befehl starten, werden 64-KB-Speicherseiten für den Server aktiviert. Mithilfe dieser Einstellung kann die Serverleistung optimiert werden.

```
/opt/tivoli/tsm/server/bin/dsmserv
```

```
C:\Programme\Tivoli\TSM\bin\dsmserv -k server2
```

## Beispiel: Einen zusätzlichen Server starten

---

Einen zusätzlichen Server unter Verwendung des Registrierungsschlüssels SERVER2 starten.

```
dsmserv -k server2
```

## Beispiel: Das Beispielscript laden

---

Die Beispielscriptdatei laden, die mit dem Server zur Verfügung gestellt wird.

```
dsmserv runfile scripts.smp
```

## Beispiel: Den Server im Verwaltungsmodus starten

---

Starten Sie den Server im Verwaltungsmodus, bevor Sie Verwaltungs- oder Rekonfigurationstasks ausführen.

```
dsmserve maintenance
```

### Zugehörige Tasks:

Server im Verwaltungsmodus starten

 AIX-Betriebssysteme

## Serverstartscript: rc.dsmserve

---

Sie können das Script rc.dsmserve in Ihrem Systemstart verwenden, um eine Serverinstanz unter einer bestimmten Benutzer-ID automatisch zu starten.

### Syntax

---

```
>>-rc.dsmserve--+- -u--Benutzername+----->
                '- -U--Benutzername-'
>--+-----+-----><
    '- -i--Instanzverzeichnis-'
```

### Parameter

---

-u Benutzername

Gibt die Instanzbenutzer-ID an, für die die Umgebung konfiguriert ist. Der Server wird unter dieser Benutzer-ID ausgeführt.

-U Benutzername


Gibt die Instanzbenutzer-ID an, für die die Umgebung konfiguriert ist. Der Server wird unter der Benutzer-ID des Aufrufers des Befehls ausgeführt.

-i Instanzverzeichnis

Gibt ein Instanzverzeichnis an, das das Arbeitsverzeichnis des Servers wird.

### Zugehörige Tasks:

 AIX: Server automatisch starten

 Linux-Betriebssysteme

## Serverstartscript: dsmserve.rc

---

Sie können das Script dsmserve.rc verwenden, um eine Serverinstanz zu stoppen oder einen Server manuell oder automatisch zu starten.

### Voraussetzungen

---

Bevor Sie den Befehl DSMSEV.RC ausgeben, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass die Serverinstanz unter einer Benutzer-ID ohne Rootberechtigung mit dem Namen des Instanzeigners ausgeführt wird.
2. Kopieren Sie das Script dsmserve.rc in das Verzeichnis /etc/rc.d/init.d. Das Script dsmserve.rc befindet sich im Serverinstallationsverzeichnis, z. B. /opt/tivoli/tsm/server/bin.
3. Benennen Sie das Script um, sodass es mit dem Namen des Serverinstanzeigners übereinstimmt, z. B. tsminst1.
4. Wenn das Serverinstanzverzeichnis nicht Ausgangsverzeichnis/tsminst1 ist, suchen Sie in der Kopie des Scripts nach der folgenden Zeile:

```
instance_dir="${Instanzausgangsverzeichnis}/tsminst1"
```

Ändern Sie die Zeile so, dass sie auf Ihr Serverinstanzverzeichnis verweist, beispielsweise:

```
instance_dir="/tsminst1"
```

5. Suchen Sie in der Kopie des Scripts nach der folgenden Zeile:

```
# pidfile: /var/run/dsmserve_InstanceName.pid
```

Ändern Sie den Wert für den Instanznamen in den Namen des Serverinstanzeigners. Hat beispielsweise der Serverinstanzeigner den Namen `tsminst1`, aktualisieren Sie die Zeile wie folgt:

```
# pidfile: /var/run/dsmserve_tsminst1.pid
```

- Verwenden Sie Tools, wie z. B. das Dienstprogramm `CHKCONFIG`, um die Ausführungsebene zu konfigurieren, auf der der Server automatisch gestartet wird. Geben Sie einen Wert an, der einem Mehrbenutzermodus mit aktiviertem Netzbetrieb entspricht. Normalerweise ist die zu verwendende Ausführungsebene 3 oder 5, abhängig vom Betriebssystem und seiner Konfiguration. Ausführliche Informationen zu Ausführungsebenen finden Sie in der Dokumentation für Ihr Betriebssystem.

## Syntax

---

```
>>-dsmserve.rc--+-+-----+-----><
                +-start---+
                +-stop----+
                +-status---+
                '-restart-'
```

## Parameter

---


**start**  
Startet den Server.

**stop**  
Stoppt den Server.

**status**  
Zeigt den Status des Servers an. Lautet der Status `started` (gestartet), wird auch die Prozess-ID des Serverprozesses angezeigt.

**restart**  
Stoppt den Server und startet ihn erneut.

### Zugehörige Tasks:

 Linux: Server auf Linux-Systemen automatisch starten

## DSMSERV DISPLAY DBSPACE (Informationen zum Datenbankspeicherbereich anzeigen)

---

Verwenden Sie dieses Dienstprogramm, um Informationen zum Speicherbereich anzuzeigen, der für die Datenbank definiert ist. Die Ausgabe dieses Dienstprogramms entspricht der Ausgabe von `QUERY DBSPACE`, aber Sie können dieses Dienstprogramm verwenden, wenn der Server nicht aktiv ist.

## Syntax

---

```
>>-DSMSERV--+-+-----+----->
          | (1)           |
          |----- -u--Benutzername- |
          |----->

>+-+-----+----->
  | (1)           |
  |----- -i--Instanzverzeichnis- |
  |----->

  (2) .- -k--Server1----->
>-----+-----+----->
  '- -k--Schlüsselname-' '- -o--Optionsdatei-'



>+-+-----+-----+-----DISPlay DBSPace-----><
  '- -noexpire-' '- -quiet-'
```

Anmerkungen:

- Dieser Parameter gilt nur für AIX- und Linux-Server.
- Dieser Parameter gilt nur für Windows-Server.

## Parameter

---

 AIX-Betriebssysteme  Linux-Betriebssysteme-u Benutzername



Gibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird.

-i Instanzverzeichnis

Gibt ein Instanzverzeichnis an, das verwendet werden soll. Dies wird das aktuelle Arbeitsverzeichnis des Servers.

-k Schlüsselname

Gibt den Namen eines Windows-Registrierungsschlüssels an, der zum Speichern von Informationen zu diesem Server verwendet wird. Verwenden Sie diesen Parameter nur, wenn sich mehrere Server in demselben System befinden. Der Standardwert ist SERVER1.

-o Optionsdatei

Gibt eine Optionsdatei an, die verwendet werden soll.

-noexpire

Gibt an, dass beim Start die Verfallsverarbeitung unterdrückt ist.

-quiet

Gibt an, dass Nachrichten an die Konsole unterdrückt werden.

## Beispiel: Informationen zum Datenbankbereich anzeigen

Informationen zum Datenbankspeicherbereich anzeigen. Details zu den Informationen, die in der Ausgabe angezeigt werden, befinden sich in Feldbeschreibungen. Den folgenden Befehl ausgeben.

```
dsmserv display dbspace
```

| Position  | Gesamtspeicherbereich (MB) | Verwendeter Sp.-Bereich (MB) | Freier Sp.-Bereich (MB) |
|-----------|----------------------------|------------------------------|-------------------------|
| /tsmdb001 | 46.080,00                  | 20.993,12                    | 25.086,88               |
| /tsmdb002 | 46.080,00                  | 20.992,15                    | 25.087,85               |

| Position     | Gesamtspeicherbereich (MB) | Verwendeter Sp.-Bereich (MB) | Freier Sp.-Bereich (MB) |
|--------------|----------------------------|------------------------------|-------------------------|
| d:\tsm\db001 | 46.080,00                  | 20.993,12                    | 25.086,88               |
| d:\tsm\db002 | 46.080,00                  | 20.993,15                    | 25.087,85               |

## Feldbeschreibungen

Standort

Das Verzeichnis oder der Pfad zum Speichern der Datenbank.

Gesamtspeicherbereich (MB)

Die Gesamtzahl Megabyte an der Position.

Verwendeter Speicherbereich (MB)

Die Anzahl Megabyte, die an der Position verwendet werden.

Freier Speicherbereich (MB)

Der Speicherbereich, der im Dateisystem verbleibt, in dem sich der Pfad befindet.

Der Speicherbereich, der auf dem Laufwerk verbleibt, auf dem sich das Verzeichnis befindet.

## DSMSERV DISPLAY LOG (Informationen zum Wiederherstellungsprotokoll anzeigen)

Mit diesem Dienstprogramm können Sie Informationen zu Wiederherstellungsprotokollen anzeigen, einschließlich der aktiven Protokolldatei, dem Spiegel für die aktive Protokolldatei, dem Übernahmeverzeichnis für das Archivprotokoll und dem Überlaufstandort für die Protokolle. Verwenden Sie dieses Dienstprogramm, wenn der Server nicht aktiv ist.

## Syntax

```
>>-DSMSERV-----+----->
| (1) |
'----- -u--Benutzername-'
>>+-----+----->
```

```

| (1) |
|----- -i--Instanzverzeichnis-|











(2) .- -k--Server1-----
>-----+-----+-----+-----+-----+----->
| -k--Schlüsselname- | -o--Optionsdatei- |
>-----+-----+-----+-----+-----+-----><
| -noexpire- | -quiet- |

```

Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.

## Parameter



-   **-u Benutzername**  
  Gibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird.
-   **-i Instanzverzeichnis**  
  Gibt ein Instanzverzeichnis an, das verwendet werden soll. Dies wird das aktuelle Arbeitsverzeichnis des Servers.
-  **-k Schlüsselname**  
 Gibt den Namen des Windows-Registrierungsschlüssels an, aus dem Informationen zum Server abgerufen werden sollen. Verwenden Sie diesen Parameter nur, wenn sich mehrere Server in demselben System befinden. Der Standardwert ist SERVER1.
- o Optionsdatei**  
 Gibt eine Optionsdatei an, die verwendet werden soll.
- noexpire**  
 Gibt an, dass beim Start die Verfallsverarbeitung unterdrückt ist.
- quiet**  
 Gibt an, dass Nachrichten an die Konsole unterdrückt werden.

## Beispiele: Informationen zu Wiederherstellungsprotokollen anzeigen

Informationen zu den Wiederherstellungsprotokollen anzeigen. Details zu den Informationen, die in der Ausgabe angezeigt werden, befinden sich in Feldbeschreibungen.


```
dsmserve display log
```

```

 
    Gesamtspeicherbereich (MB): 38.912
    Verwendeter Speicherbereich (MB): 401,34
    Freier Speicherbereich (MB): 38.358,65
    Verzeichnis für aktive Protokolldateien: /activelog
    Verzeichnis für Archivprotokolle: /archivelog
    Spiegelprotokollverzeichnis: /mirrorlog
    Übernahmeverzeichnis für Archivprotokolle: /archfailoverlog

```

```


    Gesamtspeicherbereich (MB): 38.912
    Verwendeter Speicherbereich (MB): 401,34
    Freier Speicherbereich (MB): 38.358,65
    Verzeichnis für aktive Protokolldateien: h:\tsm\activelog
    Verzeichnis für Archivprotokolle: k:\tsm\archivelog
    Spiegelprotokollverzeichnis: i:\tsm\mirrorlog
    Übernahmeverzeichnis für Archivprotokolle: j:\tsm\archfailoverlog

```

## Feldbeschreibungen

**Gesamtspeicherbereich**

Gibt die maximale Größe der aktiven Protokolldatei an.

**Verwendeter Speicherbereich**

Gibt den Gesamtspeicherbereich (in Megabyte) für aktive Protokolldateien an, der gegenwärtig in der Datenbank verwendet wird.

**Freier Speicherbereich**

Gibt den Speicherbereich (in MB) für aktive Protokolldateien in der Datenbank an, der nicht von nicht festgeschriebenen Transaktionen verwendet wird.

Verzeichnis für aktive Protokolldateien

Gibt die Position an, an der aktive Protokolldateien gespeichert werden. Wird das Verzeichnis für aktive Protokolldateien geändert, versetzt der Server alle archivierten Protokolle in das Verzeichnis für Archivprotokolle und alle aktiven Protokolldateien in ein neues Verzeichnis für aktive Protokolldateien.

Spiegelprotokollverzeichnis

Gibt die Position an, an der der Spiegel der aktiven Protokolldatei aufbewahrt wird.

Übernahmeverzeichnis für Archivprotokolle

Gibt die Position an, an der der Server Archivprotokolle sichert, wenn die Protokolle nicht am Zielort für Archivprotokolle archiviert werden können.

## DSMSERV EXTEND DBSPACE (Speicherbereich für die Datenbank vergrößern)

Verwenden Sie dieses Dienstprogramm, um den Speicherbereich für die Datenbank zu vergrößern, indem Verzeichnisse für die Datenbank hinzugefügt werden. Dieses Dienstprogramm führt dieselbe Funktion wie der Befehl EXTEND DBSPACE aus, aber Sie können es verwenden, wenn der Server nicht aktiv ist.

Einschränkung: Die Neuverteilung von Daten und die Zurückforderung von Speicherbereich als Teil einer Operation zum Erweitern des Datenbankbereichs funktioniert nur mit DB2-Tabellenbereichen der Version 9.7 oder höher, die erstellt werden, wenn Sie einen neuen Server der Version 6.3 oder höher formatieren.



### Syntax



```
>>-DSMSERV-----+-----+----->
      | (1)
      |----- -u--Benutzername-'
>-----+-----+----->
      | (1)
      |----- -i--Instanzverzeichnis-'
      (2) .- -k--Server1-----
>-----+-----+-----EXTend DBSpace----->
      | - -k--Schlüsselname-'
      .-,-----
      V      | .-RECLAIMstorage--==--Yes-----
>-----DB-Verzeichnis+-----+-----<
      |-----RECLAIMstorage--==--+No--+-'
      |-----Yes-'
```



Anmerkungen:



1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.


### Parameter


  -u Benutzername

  Gibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird.

  -i Instanzverzeichnis

  Gibt ein Instanzverzeichnis an, das verwendet werden soll. Dies wird das aktuelle Arbeitsverzeichnis des Servers.


 -k Schlüsselname

 Gibt den Namen eines Windows-Registrierungsschlüssels an, der zum Speichern von Informationen zu diesem Server verwendet wird. Verwenden Sie diesen Parameter nur, wenn sich mehrere Server in demselben System befinden. Der Standardwert ist SERVER1.

DB-Verzeichnis (Erforderlich)

Gibt die Verzeichnisse für den Datenbankspeicher an. Die Verzeichnisse müssen leer sein und auf die Verzeichnisse muss durch die Benutzer-ID des Datenbankmanagers zugegriffen werden können. Ein Verzeichnisname muss ein vollständig qualifizierter Name sein und darf 175 Zeichen nicht überschreiten. Schließen Sie den Namen in Anführungszeichen ein, wenn er eingebettete

Leerzeichen, ein Gleichheitszeichen oder andere Sonderzeichen enthält. Wenn Sie eine Verzeichnisliste für den Datenbankspeicher angeben, beträgt die maximale Länge der Liste 1400 Zeichen.

 **Einschränkung:** Sie können keine Pfade mit allgemeiner Namenskonvention angeben.

**Tipp:** Geben Sie Verzeichnisse an, die dieselbe Größe wie vorhandene Verzeichnisse haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Sind ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse, reduzieren sie das Potenzial zum optimierten parallelen Vorabesezugriff und zur Verteilung der Datenbank.

#### RECLAIMstorage

Gibt an, ob Daten auf neu erstellte Datenbankverzeichnisse erneut verteilt werden und Speicherbereich aus den alten Speicherpfaden zurückgefordert wird, wenn Sie der Datenbank Speicherbereich hinzufügen. Dieser Parameter ist wahlfrei. Der Standardwert ist 'Yes'.

#### Yes

Gibt an, dass Daten erneut verteilt werden, sodass neue Verzeichnisse für die sofortige Verwendung verfügbar sind. **Wichtig:** Bei dem Neuverteilungsprozess werden erhebliche Systemressourcen verwendet. Planen Sie dies im Voraus ein. Außerdem kann der Server für eine Weile offline sein, bis der Prozess beendet ist.

#### No

Gibt an, dass Daten nicht auf Datenbankverzeichnisse erneut verteilt werden und Speicherbereich nicht zurückgefordert wird.

 **AIX-Betriebssysteme**  **Linux-Betriebssysteme**

## Beispiel: Speicherbereich für die Datenbank vergrößern

---

Ein Verzeichnis mit dem Namen stg1 im Verzeichnis tsm\_db für den Datenbankspeicherbereich hinzufügen und dann Daten erneut verteilen und Speicherbereich zurückfordern, indem der folgende Befehl ausgegeben wird:

```
dsmserve extend dbSPACE /tsm_db/stg1
```

 **Windows-Betriebssysteme**

## Beispiel: Speicherbereich für die Datenbank vergrößern

---

Laufwerk D zum Speicherbereich für die Datenbank hinzufügen und dann Daten erneut verteilen und Speicherbereich zurückfordern, indem der folgende Befehl ausgegeben wird:

```
dsmserve extend dbSPACE D:
```

#### Zugehörige Verweise:


EXTEND DBSPACE (Speicherbereich für die Datenbank erhöhen)


## DSMSERV FORMAT (Datenbank und Protokoll formatieren)

---

Verwenden Sie das Dienstprogramm DSMSERV FORMAT, um die Serverdatenbank und das Wiederherstellungsprotokoll zu initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls sind keine anderen Serveraktivitäten zulässig.

Die in diesem Dienstprogramm angegebenen Verzeichnisse sollten sich in einem schnellen und zuverlässigen Speicher befinden. Stellen Sie die Verzeichnisse nicht in Dateisysteme, für die nicht genügend Speicherplatz zur Verfügung stehen könnte. Werden bestimmte Verzeichnisse (beispielsweise das Verzeichnis für aktive Protokolldateien) nicht verfügbar oder voll, wird der Server gestoppt.

 **Einschränkung:** Wenn Sie eine Dateizuordnungstabelle (FAT oder FAT32) oder ein NTFS-Format (NTFS = New Technology File System) verwenden, können Sie das Stammverzeichnis dieses Systems nicht als Position eines Datenbankverzeichnisses oder Protokollverzeichnisses angeben. Stattdessen müssen Sie ein oder mehrere Unterverzeichnisse innerhalb des Stammverzeichnisses erstellen. Erstellen Sie dann die Datenbankverzeichnisse und Protokollverzeichnisse innerhalb der Unterverzeichnisse.

 **Wichtig:** Das Installationsprogramm erstellt eine Reihe von Registrierungsschlüsseln. Einer dieser Schlüssel zeigt auf das Verzeichnis, in dem ein Standardserver mit dem Namen SERVER1 erstellt wird. Soll ein zusätzlicher Server installiert werden, erstellen Sie ein Verzeichnis und verwenden Sie das Dienstprogramm DSMSERV FORMAT mit dem Parameter -k in diesem Verzeichnis. Dieses Verzeichnis wird der Standort des Servers. Das Register verfolgt die installierten Server.

Wenn ein Server anfänglich mit dem Dienstprogramm DSMSERV FORMAT oder mit dem Konfigurationsassistenten erstellt wird, werden eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien zum Speichern von Datenbankinformationen erstellt, die vom Datenbankmanager verwendet werden.

## Syntax

---

```



>>-DSMSERV-----+----->
      | (1) |
      |----- -u--Benutzername-'
>-----+----->
      | (1) |
      |----- -i--Instanzverzeichnis-'
      (2) .- -k--Server1-----
>-----+----->
      |----- -k--Schlüsselname-' |----- -o--Optionsdatei-'
>-----+-----+-----+-----+-----+-----+-----+----->
      |----- -noexpire-' |----- -quiet-'
      .-,'-----
      v |
>-----+-----+-----+-----+-----+-----+-----+----->
      |----- DBDir-----Verzeichnis-+-----+-----+-----+-----+-----+-----+----->
      |----- DBFile-----Datei-----'
      .-ACTIVELOGSsize-----16384-----
>-----+-----+-----+-----+-----+-----+-----+----->
      |----- ACTIVELOGSsize-----Megabyte-'
>-----+-----+-----+-----+-----+-----+-----+----->
      |----- ACTIVELOGDirectory-----Verzeichnis----->
>-----+-----+-----+-----+-----+-----+-----+----->
      |----- ARCHLogdirectory-----Verzeichnis----->
>-----+-----+-----+-----+-----+-----+-----+----->
      |----- ARCHFailoverlogdirectory-----Verzeichnis-'
>-----+-----+-----+-----+-----+-----+-----+----->
      |----- MIRRorlogdirectory-----Verzeichnis-'



```



#### Anmerkungen:



1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.


## Parameter


  -u Benutzername

  Gibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird. Dieser Parameter ist wahlfrei.

  -i Instanzverzeichnis

  Gibt ein Instanzverzeichnis an, das verwendet werden soll. Dieses Verzeichnis wird das aktuelle Arbeitsverzeichnis des Servers. Dieser Parameter ist wahlfrei.

 -k Schlüsselname

 Gibt den Namen eines Windows-Registrierungsschlüssels an, der zum Speichern von Informationen zu diesem Server verwendet wird. Verwenden Sie diesen Parameter nur, um zusätzliche Server auf demselben System zu installieren. Nachdem ein Server unter Verwendung dieses Parameters installiert wurde, müssen Sie den Server immer mit dem Wert dieses Parameters starten. Dieser Parameter ist wahlfrei. Der Standardwert ist SERVER1.  
Einschränkung: Zusätzliche Instanzen des IBM Spectrum Protect-Servers, die auf demselben System ausgeführt werden, konkurrieren um Ressourcen und haben Auswirkungen auf die Gesamtleistung jedes IBM Spectrum Protect-Servers.

-o Optionsdatei

Gibt eine Optionsdatei an, die verwendet werden soll. Dieser Parameter ist wahlfrei.

-noexpire

Gibt an, dass beim Start die Verfallsverarbeitung unterdrückt ist. Dieser Parameter ist wahlfrei.

-quiet

Gibt an, dass Nachrichten an die Konsole unterdrückt werden. Dieser Parameter ist wahlfrei.

DBDir

Gibt die relativen Pfadnamen eines oder mehrerer Verzeichnisse an, die zum Speichern von Datenbankobjekten verwendet werden. Verzeichnisnamen müssen ohne Leerzeichen durch Kommas voneinander getrennt werden. Sie können bis zu 128 Verzeichnisnamen angeben. Sie müssen entweder den Parameter DBDIR oder den Parameter DBFILE angeben.

Tipp: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zugrunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Sind ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse, reduzieren sie das Potenzial zum optimierten parallelen Vorabsezugriff und zur Verteilung der Datenbank.

DBFile

Gibt den Namen einer Datei an, die die relativen Pfadnamen eines oder mehrerer Verzeichnisse enthält, die zum Speichern von Datenbankobjekten verwendet werden. Jeder Verzeichnisname muss sich auf einer separaten Zeile in der Datei befinden. Sie können bis zu 128 Verzeichnisnamen angeben. Sie müssen entweder den Parameter DBDIR oder den Parameter DBFILE angeben.

#### ACTIVELOGSize

Gibt die Größe der aktiven Protokolldatei in Megabyte an. Dieser Parameter ist wahlfrei. Der Mindestwert ist 2048 MB (2 GB); der Maximalwert ist 524.288 MB (512 GB). Wenn eine ungerade Zahl angegeben wird, wird der Wert auf die nächste gerade Zahl aufgerundet. Der Standardwert ist 16384 MB.

Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option ACTIVELOGSIZE. Richtlinien für den Speicherbedarf befinden sich in der folgenden Tabelle:

Tabelle 1. Schätzung des Datenträger- und Dateispeicherbedarfs

| Wert der Option ACTIVELOGSize | Reservieren Sie diesen freien Speicherbereich im Verzeichnis für aktive Protokolldateien, zusätzlich zum Speicherbereich von ACTIVELOGSize |
|-------------------------------|--|
| 16 GB - 128 GB                | 5120 MB  |
| 129 GB - 256 GB               | 10240 MB   |
| 257 GB - 512 GB               | 20480 MB   |

#### ACTIVELOGDirectory (Erforderlich)

Gibt das Verzeichnis an, in das der Server aktive Protokolldateien schreibt und in dem der Server die Dateien speichert. Es gibt nur eine Position für aktive Protokolldateien. Der Name muss ein vollständig qualifizierter Verzeichnisname sein. Das Verzeichnis muss vorhanden sein, es muss leer sein, und auf das Verzeichnis muss durch die Benutzer-ID des Datenbankmanagers zugegriffen werden können. Die maximale Anzahl Zeichen beträgt 175.

#### ARCHLogdirectory (Erforderlich)

Gibt das Verzeichnis für die Archivprotokolldateien an. Der Name muss ein vollständig qualifizierter Verzeichnisname sein. Die maximale Anzahl Zeichen beträgt 175.

#### ARCHFailoverlogdirectory

Gibt das Verzeichnis an, das als alternative Speicherposition verwendet werden soll, wenn das ARCHLOGDIRECTORY-Verzeichnis voll ist. Dieser Parameter ist wahlfrei. Die maximale Anzahl Zeichen beträgt 175.

#### MIRRORlogdirectory

Gibt das Verzeichnis an, in dem der Server die aktive Protokolldatei spiegelt (die Dateien im ACTIVELOGDIRECTORY-Verzeichnis). Dieser Parameter ist wahlfrei. Das Verzeichnis muss ein vollständig qualifizierter Verzeichnisname sein. Die maximale Anzahl Zeichen beträgt 175.

## Beispiel: Eine Datenbank formatieren

#### AIX-Betriebssysteme Linux-Betriebssysteme

```
dsmserv format dbdir=/tsmdb001 activelogsiz=8192
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

#### Windows-Betriebssysteme

```
dsmserv -k server2 format dbdir=d:\tms\db001 activelogsiz=8192
activelogdirectory=e:\tms\activelog archlogdirectory=f:\tms\archlog
archfailoverlogdirectory=g:\tms\archfaillog mirrorlogdirectory=h:\tms\mirrorlog
```

## DSMSERV INSERTDB (Serverdatenbank in eine leere Datenbank versetzen)

Verwenden Sie das Dienstprogramm DSMSERV INSERTDB, um eine Serverdatenbank in eine neue Datenbank zu versetzen. Die Datenbank kann vom ursprünglichen Server extrahiert und in eine neue Datenbank auf dem neuen Server eingefügt werden, indem eine Netzverbindung zwischen den beiden Servern verwendet wird. Die Datenbank kann auch von Datenträgern eingefügt werden, die die extrahierte Datenbank enthalten.

Führen Sie vor der Verwendung des Dienstprogramms DSMSERV INSERTDB die Planungs- und Vorbereitungstasks aus, wie z. B. Sichern der Datenbank und Sichern der Konfigurationsdaten. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind, bevor Sie die Serverdatenbank versetzen.

### Voraussetzungen für das Einfügen mit Datenträgern

Bevor Sie das Dienstprogramm zum Einfügen der Serverdatenbank in eine leere Datenbank ausführen, stellen Sie sicher, dass Ihr System die folgenden Voraussetzungen erfüllt.

- Die Manifestdatei aus der Operation DSMUPGRD EXTRACTDB muss verfügbar sein.
- Wenn die Manifestdatei keine Einheitenkonfigurationsdaten enthält oder wenn Sie den Parameter CONFIGINFO=DEVCONFIG angeben, müssen die beiden folgenden Anweisungen zutreffen:

- Die Serveroptionsdatei muss einen Eintrag für die Einheitenkonfigurationsdatei enthalten.
- Die Einheitenkonfigurationsdatei muss Informationen zur Einheitenklasse enthalten, die in der Manifestdatei angegeben ist.
- Die Datenträger, die die extrahierte Datenbank enthalten, müssen für den Server der Version 8 verfügbar sein. Außerdem müssen die Berechtigungen einen Zugriff auf die Datenträger für die Benutzer-ID gewähren, die Eigner der Serverinstanz der Version 8 ist.

## Syntax

```
>>-DSMSERV-----+----->
      | (1)           |
      '----- -u--Benutzername-'

>+-----+----->
      | (1)           |
      '----- -i--Instanzverzeichnis-'

      (2) .- -k--Server1----- .
>+-----+-----+-----+----->
      ' -k--Schlüsselname-' ' -o--Optionsdatei-'

>+-----+-----+-----+-----+-----+-----+-----+----->
      '- -noexpire-' ' -quiet-'

>+-----+-----+-----+-----+-----+-----+-----+----->
      A: Von Datenträgern einfügen |----->
      '-| B: Im Netz einfügen |-----'

      .-PREview-----No----- .
>+-----+-----+-----+-----+-----+-----+-----+----->
      '-PREview-----+Yes+-'
      ' -No--'

A: Von Datenträgern einfügen

|+-----+-----+-----+-----+-----+-----+-----+----->
      '-DEVclass-----Einheitenklassenname-'

      .-CONFiginfo-----MANifest----- .
>+-----+-----+-----+-----+-----+-----+-----+-----|
      '-CONFiginfo-----+MANifest--+-'
      ' -DEVconfig-'



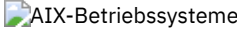
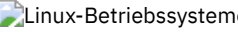


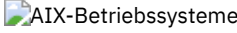
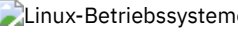

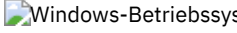
B: Im Netz einfügen

      .-SESSWait-----60----- .
|+-----+-----+-----+-----+-----+-----+-----+-----|
      '-SESSWait-----Minuten-'
```

Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.

## Parameter

-   **-u Benutzername**  
  Gibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird. Dieser Parameter ist wahlfrei.
-   **-i Instanzverzeichnis**  
  Gibt ein Instanzverzeichnis an, das verwendet werden soll. Dieses Verzeichnis wird das aktuelle Arbeitsverzeichnis des Servers. Dieser Parameter ist wahlfrei.
-  **-k Schlüsselname**  
 Gibt den Namen des Windows-Registrierungsschlüssels an, aus dem Informationen zum Server abgerufen werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist SERVER1.
- o Optionsdatei**  
 Gibt eine Optionsdatei an, die verwendet werden soll. Dieser Parameter ist wahlfrei.
- noexpire**  
 Gibt an, dass beim Start die Verfallsverarbeitung unterdrückt ist. Dieser Parameter ist wahlfrei.
- quiet**  
 Gibt an, dass Nachrichten an die Konsole unterdrückt werden. Dieser Parameter ist wahlfrei.
- DEVclass**

Gibt eine Einheitenklasse mit sequenziellem Zugriff an. Mit Ausnahme der Einheitenklasse DISK kann jede Einheitenklasse angegeben werden. Die Definition für die Einheitenklasse muss entweder in der Manifestdatei oder der Einheitenkonfigurationsdatei vorhanden sein.

Dieser Parameter ist wahlfrei und wird nur verwendet, wenn die Datenbank, die in die leere Datenbank der Version 8 eingefügt werden soll, auf Datenträger extrahiert wurde. Befindet sich die Datenbank auf Datenträgern und wird keine Einheitenklasse angegeben, wird die in der Manifestdatei angegebene Einheitenklasse verwendet.

Einschränkung: Sie können keine Einheitenklasse mit dem Einheitentyp NAS oder CENTERA verwenden.

#### MANifest

Gibt die Position der Manifestdatei an. Verwenden Sie einen vollständig qualifizierten Dateinamen oder stellen Sie die Datei in ein lokales Verzeichnis. Beispiel: `./manifest.txt`

Dieser Parameter ist erforderlich, wenn die Datenbank, die in die leere Datenbank der Version 8 eingefügt werden soll, auf Datenträger extrahiert wurde.

#### CONFiginfo

Gibt die Quelle der Einheitenkonfigurationsdaten an, die von der Operation DSMSEV INSERTDB verwendet wird. Der Standardwert für diesen Parameter ist MANIFEST. Gültige Werte sind:

##### MANifest

Gibt an, dass Einheitenkonfigurationsdaten aus der Manifestdatei gelesen werden. Wenn die Manifestdatei keine Einheitenkonfigurationsdaten enthält, wird statt dessen die Einheitenkonfigurationsdatei verwendet.

##### DEVConfig

Gibt an, dass Einheitenkonfigurationsdaten aus der Einheitenkonfigurationsdatei gelesen werden.

#### SESSWait

Gibt die Anzahl Minuten an, die der Server der Version 8 wartet, bis er vom ursprünglichen Server angesprochen wird. Der Standardwert ist 60 Minuten.

Verwenden Sie diesen Parameter nur, wenn die Daten, die in die leere Datenbank der Version 8 eingefügt werden, mit einer Netzverbindung vom Quellenserver übertragen werden.

#### PREview

Gibt an, ob die Einfügeoperation vorangezeigt werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

Verwenden Sie den Parameter PREVIEW=YES, um eine Datenbank zu testen. Wenn Sie diesen Parameter verwenden, schließt die Operation alle Schritte des Prozesses ein, mit Ausnahme der tatsächlichen Einfügung von Daten in die neue Datenbank. Mit der Voranzeige der Einfügeoperation können Sie schnell prüfen, ob die Quelldatenbank lesbar ist. Außerdem können Sie alle ungültigen Datenintegritätsbedingungen identifizieren, die verhindern können, dass eine Datenbank, für die ein Upgrade durchgeführt wurde, in der Produktion eingesetzt wird.

## DSMSERV LOADFORMAT (Datenbank formatieren)

Verwenden Sie das Dienstprogramm DSMSEV LOADFORMAT, wenn ein Upgrade von Version 5 durchgeführt wird. Das Dienstprogramm formatiert eine leere Datenbank als Vorbereitung zum Einfügen einer extrahierten Datenbank in die leere Datenbank.

### Syntax

```
>>-DSMSERV--+-+-----+----->
          | (1) |
          |----- -u--Benutzername-|
>+-----+----->
  | (1) |
  |----- -i--Instanzverzeichnis-|
  (2) .- -k--Server1----- .
>+-----+-----+-----+----->
  | -k--Schlüsselname-| | -o--Optionsdatei-|
>+-----+-----+-----+-----LOADFORMAT----->
  | -noexpire-| | -quiet-|
  .-,----- .
  v |
>+--DBDir-----Verzeichnis--+----->
  | -DBFile-----Datei-----|
  .-ACTIVELOGSize-----16384----- .
```



```



>+-----+----->
  '-ACTIVELOGSize-----Megabyte-'
>--ACTIVELOGDirectory-----Verzeichnis----->
>--ARCHLogdirectory-----Verzeichnis----->
>+-----+----->
  '-ARCHFailoverlogdirectory-----Verzeichnis-'
>+-----+-----<
  '-MIRRORlogdirectory-----Verzeichnis-'



```



Anmerkungen:



1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.


## Parameter


 AIX-Betriebssysteme  Linux-Betriebssysteme-u Benutzername

 AIX-Betriebssysteme  Linux-Betriebssysteme Gibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird. Dieser Parameter ist wahlfrei.

 AIX-Betriebssysteme  Linux-Betriebssysteme -i Instanzverzeichnis

 AIX-Betriebssysteme  Linux-Betriebssysteme Gibt ein Instanzverzeichnis an, das verwendet werden soll. Dieses Verzeichnis wird das aktuelle Arbeitsverzeichnis des Servers. Dieser Parameter ist wahlfrei.

 Windows-Betriebssysteme-k Schlüsselname

 Windows-Betriebssysteme Gibt den Namen eines Windows-Registrierungsschlüssels an, der zum Speichern von Informationen zu diesem Server verwendet wird. Verwenden Sie diesen Parameter nur, um zusätzliche Server auf demselben System zu installieren. Nachdem ein Server unter Verwendung dieses Parameters installiert wurde, müssen Sie den Server immer mit dem Wert dieses Parameters starten. Der Standardwert ist SERVER1.

-o Optionsdatei

Gibt eine Optionsdatei an, die verwendet werden soll. Dieser Parameter ist wahlfrei.

-noexpire

Gibt an, dass die Verfallsverarbeitung unterdrückt wird, wenn der Server gestartet wird. Dieser Parameter ist wahlfrei.

-quiet

Gibt an, dass Nachrichten an die Konsole unterdrückt werden. Dieser Parameter ist wahlfrei.

DBDir

Gibt die relativen Pfadnamen eines oder mehrerer Verzeichnisse an, die zum Speichern von Datenbankobjekten verwendet werden. Verzeichnisnamen müssen ohne Leerzeichen durch Kommas voneinander getrennt werden. Sie können bis zu 128 Verzeichnisnamen angeben. Sie müssen entweder den Parameter DBDIR oder den Parameter DBFILE angeben.

Tipp: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zugrunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Sind ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse, reduzieren sie das Potenzial zum optimierten parallelen Vorabesezugriff und zur Verteilung der Datenbank.

DBFile

Gibt den Namen einer Datei an, die die relativen Pfadnamen eines oder mehrerer Verzeichnisse enthält, die zum Speichern von Datenbankobjekten verwendet werden. Jeder Verzeichnisname muss sich auf einer separaten Zeile in der Datei befinden. Sie können bis zu 128 Verzeichnisnamen angeben. Sie müssen entweder den Parameter DBDIR oder den Parameter DBFILE angeben.

ACTIVELOGSize

Gibt die Größe der aktiven Protokolldatei in Megabyte an. Dieser Parameter ist wahlfrei. Der Mindestwert ist 2048 MB (2 GB); der Maximalwert ist 524.288 MB (512 GB). Wenn eine ungerade Zahl angegeben wird, wird der Wert auf die nächste gerade Zahl aufgerundet. Der Standardwert ist 16384 MB.

Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option ACTIVELOGSIZE. Richtlinien für den Speicherbedarf befinden sich in der folgenden Tabelle:



Tabelle 1. Schätzung des Datenträger- und Dateispeicherbedarfs



| Wert der Option<br>ACTIVELOGSize | Reservieren Sie diesen freien Speicherbereich im Verzeichnis für aktive Protokolldateien,<br>zusätzlich zum Speicherbereich von ACTIVELOGSize |
|----------------------------------|---|
| 16 GB - 128 GB                   | 5120 MB   |
| 129 GB - 256 GB                  | 10240 MB  |
| 257 GB - 512 GB                  | 20480 MB  |


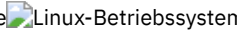
ACTIVELOGDirectory (Erforderlich)


Gibt das Verzeichnis an, in das der Server aktive Protokolldateien schreibt und in dem der Server die Dateien speichert. Es gibt nur eine Position für aktive Protokolldateien. Der Name muss ein vollständig qualifizierter Verzeichnisname sein. Das Verzeichnis

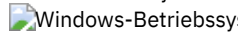


  Gibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird.

  -i Instanzverzeichnis

  Gibt ein Instanzverzeichnis an, das verwendet werden soll. Dies wird das aktuelle Arbeitsverzeichnis des Servers.

 -k Schlüsselname

 Gibt den Namen des Windows-Registrierungsschlüssels an, aus dem Informationen zum Server abgerufen werden sollen. Der Standardwert ist SERVER1.

-o Optionsdatei

Gibt eine Optionsdatei an, die verwendet werden soll.

-noexpire

Gibt an, dass beim Start die Verfallsverarbeitung unterdrückt ist.

-quiet

Gibt an, dass Nachrichten an die Konsole unterdrückt werden.

Datenbankname

Der Datenbankname, der bei der Installation eingegeben wurde. Wurde die Datenbank manuell formatiert, ist dies der Parameter für den Datenbanknamen im Dienstprogramm DSMSERV FORMAT oder DSMSERV LOADFORMAT. Dieser Datenbankname befindet sich auch in der Datei dsmserv.opt. Dieser Parameter ist erforderlich.

-force

Gibt an, ob die Datenbank entfernt wird, wenn offene Verbindungen vorhanden sind. Der Standardwert ist No. Dieser Parameter ist optional. Folgende Werte sind verfügbar:

Yes

Gibt an, dass die Datenbank entfernt wird, unabhängig davon, ob offene Verbindungen vorhanden sind.

No

Gibt an, dass die Datenbank nur entfernt wird, wenn alle Verbindungen geschlossen sind.

## Beispiel: Eine Datenbank entfernen

---

Die IBM Spectrum Protect-Serverdatenbank TSMDB1 und alle ihre Verweise entfernen.

```
dsmserv removedb TSMDB1
```

## Beispiel: Eine Datenbank mit dem Parameter 'force' entfernen

---

Die IBM Spectrum Protect-Serverdatenbank TSMDB1 und alle ihre Verweise entfernen, auch wenn offene Verbindungen vorhanden sind:

```
dsmserv removedb TSMDB1 force=yes
```

## DSMSERV RESTORE DB (Datenbank zurückschreiben)

---

Mit diesem Dienstprogramm können Sie eine Datenbank mit Hilfe einer Datenbanksicherung zurückschreiben.

Einschränkung: Sie können eine Serverdatenbank nicht zurückschreiben, wenn der Release-Level der Serverdatenbanksicherung von dem Release-Level des Servers abweicht, der zurückgeschrieben wird. Beispielsweise tritt ein Fehler auf, wenn Sie eine Datenbank der Version 7.1.3 zurückschreiben und Sie einen IBM Spectrum Protect-Server der Version 8.1 verwenden.

Die Zurückschreibungsoperation verwendet Datenbanksicherungen, die mit dem Befehl BACKUP DB erstellt wurden.

Wichtig: Geben Sie nach einer Zurückschreibungsoperation nach Zeitpunkt den Befehl AUDIT VOLUME aus, um alle DISK-Datenträger zu prüfen und alle Inkonsistenzen zwischen den Datenbankinformationen und den Speicherpooldatenträgern zu beseitigen. Überprüfen Sie vor dem Zurückschreiben der Datenbank die Datenträgerhistorydatei, um die Datenträger in Speicherpools mit sequenziellem Zugriff zu bestimmen, die seit dem Zeitpunkt, für den die Datenbank zurückgeschrieben wurde, gelöscht oder wiederverwendet wurden.

- **DSMSERV RESTORE DB (Datenbank mit dem neuesten Stand zurückschreiben)**  
Verwenden Sie das Dienstprogramm DSMSERV RESTORE DB, um unter bestimmten Bedingungen eine Datenbank mit ihrem aktuellen Status zurückzuschreiben.
- **DSMSERV RESTORE DB (Datenbank nach Zeitpunkt zurückschreiben)**  
Verwenden Sie diesen Befehl, um eine Datenbank nach Zeitpunkt zurückzuschreiben. Eine Datenträgerhistorydatei und eine Einheitenkonfigurationsdatei müssen verfügbar sein.

## DSMSERV RESTORE DB (Datenbank mit dem neuesten Stand zurückschreiben)

---

Verwenden Sie das Dienstprogramm DSMSEV RESTORE DB, um unter bestimmten Bedingungen eine Datenbank mit ihrem aktuellen Status zurückzuschreiben.

Folgende Bedingungen müssen erfüllt sein:

- Eine unbeschädigte Datenträgerhistorydatei ist verfügbar.
- Die Wiederherstellungsprotokolle sind verfügbar.
- Eine Einheitenkonfigurationsdatei mit den gültigen Einheitsdaten ist verfügbar.

Einschränkung: Sie können eine Serverdatenbank nicht zurückschreiben, wenn der Release-Level der Serverdatenbanksicherung von dem Release-Level des Servers abweicht, der zurückgeschrieben wird. Beispielsweise tritt ein Fehler auf, wenn Sie eine Datenbank der Version 7.1.3 zurückschreiben und Sie einen IBM Spectrum Protect-Server der Version 8.1 verwenden.

IBM Spectrum Protect fordert Datenträgerladevorgänge an, um die neueste Sicherungsserie zu laden, und verwendet dann die Wiederherstellungsprotokolle, um die Datenbank mit ihrem aktuellen Status zu aktualisieren.

Momentaufnahmesicherungen der Datenbank können nicht verwendet werden, um eine Datenbank mit ihrem aktuellen Status zurückzuschreiben.









## Syntax


```
>>DSMSERV-----+-----+----->
      | (1) |
      |----- -u--Benutzername-'
>+-----+-----+----->
      | (1) |
      |----- -i--Instanzverzeichnis-'
      (2) .- -k--Server1-----
>+-----+-----+-----+----->
      |----- -k--Schlüsselname-' |----- -o--Optionsdatei-'
>+-----+-----+-----RESTORE DB-----+----->
      | (1) |
      |----- -quiet-'
>+-----+-----+----->
      |----- -RECOVdir----Verzeichnis-'
>+-----+-----+----->
      |----- -ACTIVELOGDir----Verzeichnis-'
      .-PREview----No-----
>+-----+-----+-----+----->
      |----- -ON----Zielverzeichnisdatei-' |----- -PREview----+Yes--+'
      |----- -No--'
      .-RESTOREKeys----No-----
>+-----+-----+-----+----->
      |----- -RESTOREKeys----+No--+'
      |----- +-YES--+'
      |----- '-ONLY-'
>+-----+-----+-----+-----><
      |----- -PASSword----Kennwortname-'
```


Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.

## Parameter

-   -u Benutzername  
  Gibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird.
-   -i Instanzverzeichnis  
  Gibt ein Instanzverzeichnis an, das verwendet werden soll. Dieses Instanzverzeichnis wird das aktuelle Arbeitsverzeichnis des Servers.



 Windows-Betriebssysteme-k Schlüsselname

 Windows-Betriebssysteme Gibt den Namen des Windows-Registrierungsschlüssels an, aus dem Informationen zum Server abgerufen werden sollen. Der Standardwert ist SERVER1.

-o Optionsdatei

Gibt eine Optionsdatei an, die verwendet werden soll.

 AIX-Betriebssysteme  Linux-Betriebssysteme-quiet

 AIX-Betriebssysteme  Linux-Betriebssysteme Gibt an, dass Nachrichten an die Konsole unterdrückt werden.

RECOVdir



Gibt ein Verzeichnis an, in dem Wiederherstellungsprotokollinformationen von den Datenbanksicherungsdatenträgern gespeichert werden sollen. Dieses Verzeichnis muss über ausreichend Speicherplatz verfügen, um diese Transaktionswiederherstellungsinformationen zu speichern, und es muss ein leeres Verzeichnis sein. Wird dieser Parameter nicht angegeben, ist der Standardwert das Verzeichnis, das mit einem der folgenden Parameter im Dienstprogramm DSMSEV FORMAT oder DSMSEV LOADFORMAT angegeben ist:

- ARCHFAILOVERLOGDIRECTORY, falls angegeben
- ARCHLOGDIRECTORY, wenn ARCHFAILOVERLOGDIRECTORY nicht angegeben ist

ACTIVELOGDir

Gibt ein Verzeichnis an, in dem die Protokolldateien gespeichert werden sollen, die zum Verfolgen der aktiven Datenbankoperationen verwendet werden. Dieses Verzeichnis muss nur angegeben werden, wenn zu einem anderen Verzeichnis für aktive Protokolldateien als dem bereits konfigurierten Verzeichnis umgeschaltet werden soll.

On

Gibt eine Datei an, in der die Verzeichnisse aufgelistet sind, in die die Datenbank zurückgeschrieben wird. Geben Sie jedes Verzeichnis in einer separaten Zeile in der Datei an. Beispielsweise gibt der Parameter ON die Datei restorelist.txt an, die die folgende Liste enthält:  AIX-Betriebssysteme  Linux-Betriebssysteme

```
/tsmdb001  
/tsmdb002  
/tsmdb003
```

 Windows-Betriebssysteme

```
e: \tsm\db001  
f: \tsm\db002  
g: \tsm\db003
```

Wird dieser Parameter nicht angegeben, werden die Ursprungsverzeichnisse verwendet, die in der Datenbanksicherung aufgezeichnet wurden.

Tipp: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zugrunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Sind ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse, reduzieren sie das Potenzial zum optimierten parallelen Vorabesezugriff und zur Verteilung der Datenbank.

PReview

Gibt an, dass die Datenträgerhistorydateien geprüft und die Datenbanksicherungsdatenträger aus der Datenträgerhistorydatei ausgewertet werden.

1. Welche Gruppe von Datenbanksicherungsdatenträgern entspricht am besten den aktuellen Kriterien, die für die Zurückschreibungsverarbeitung angegeben sind? Die Datenträgerhistorydaten stellen ausführliche Informationen zur Sicherungsserien-ID, zur Operations-ID (Gesamtsicherung, Teilsicherung 1, Teilsicherung 2, usw.), zum Datum der Datenbanksicherung und zur Einheitenklasse bereit. Diese Informationen und die im Befehl DSMSEV RESTORE DB angegebenen Parameter bestimmen, was für die Ausführung der Zurückschreibung verwendet wird. Die Datenträgerhistorydatei wird geprüft, um die neueste Datenbanksicherung zu suchen und dann die Daten mit dieser Sicherung zurückzuschreiben.
2. Sind selbst beschreibende Daten für die ausgewählte Gruppe von Datenbanksicherungsdatenträgern verfügbar? Überprüfen Sie die Datenträgerhistorydaten auf diese Sicherungsserie. Beim Datenabgleich wird der Inhalt der selbst beschreibenden Daten mit den Angaben aus den Datenträgerhistoryeinträgen verglichen. Die Überprüfung schließt das Laden eines oder mehrerer Datenträger ein, die von der Datenträgerhistory angegeben werden. Anschließend werden die selbst beschreibenden Daten, die in den Datenbanksicherungsdatenträgern enthalten waren, mit den Angaben in der Datenträgerhistory für die Datenbanksicherung abgeglichen. Sind die Informationen aus der Datenträgerhistorydatei und die selbst beschreibenden Daten nicht konsistent, werden Nachrichten ausgegeben, um das Problem zu identifizieren. Beispiel: Es wurden nicht alle Werte angegeben bzw. es sind nicht alle Werte verfügbar oder es wurden keine selbst beschreibenden Daten gefunden.

Sind die Datenträgerhistorydaten und die selbst beschreibenden Daten aus der Datenbanksicherung konsistent, wird eine Nachricht ausgegeben, die angibt, dass die Datenbanksicherung für die Zurückschreibungsverarbeitung verwendet werden kann.


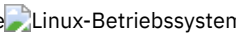
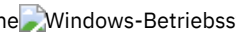
Sind die Datenträgerhistorydaten und die selbst beschreibenden Daten aus der Datenbanksicherung nicht konsistent oder wurden die selbst beschreibenden Daten für die Sicherung nicht gefunden, werden Fehlernachrichten ausgegeben, die angeben, was


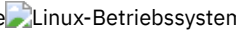

überprüft wurde und was nicht gefunden wurde.

Wird der Parameter PREVIEW nicht angegeben oder wird der Parameter auf NO gesetzt und sind die Datenträgerhistorydaten und die selbst beschreibenden Daten aus der Datenbanksicherung konsistent, wird die Zurückschreibung fortgesetzt.

Wird der Parameter PREVIEW nicht angegeben oder wird der Parameter auf NO gesetzt und schlagen der Datenabgleich und die Überprüfung fehl, wird die Datenbankzurückschreibung nicht ausgeführt. Stellen Sie weitere Datenträger zur Verfügung, auf die von der Datenträgerhistorydatei verwiesen wird, oder entfernen Sie die unvollständige Sicherungsserie oder Operation, damit der IBM Spectrum Protect-Server eine andere bevorzugte Serie oder Operation auswählt und die Verarbeitung fortsetzt.

Wird der Parameter PREVIEW auf YES gesetzt, werden von dem Prozess nur die Auswertung der Datenträgerhistorydatei sowie der Datenabgleich und die Validierung mit der ausgewählten Datenbanksicherung ausgeführt.

   RESTOREKeys

   Gibt an, ob der Masterverschlüsselungsschlüssel des Servers, der zum Verschlüsseln von Speicherpooldaten verwendet wird, zurückgeschrieben werden soll, wenn die Datenbank zurückgeschrieben wird. Dieser Parameter ist optional und gilt nur, wenn Sie verschlüsselte Containerspeicherpools in einer Cloudumgebung verwenden. Wenn der Masterschlüssel des Servers beim Zurückschreiben der Datenbank geschützt ist, ist der Standardwert YES. Wenn der Masterschlüssel des Servers beim Zurückschreiben der Datenbank nicht geschützt ist, ist der Standardwert NO. Sie können einen der folgenden Werte angeben:

No


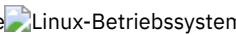
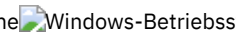
Gibt an, dass der Masterschlüssel des Servers beim Zurückschreiben der Datenbank nicht zurückgeschrieben wird.

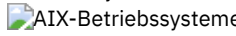
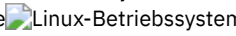
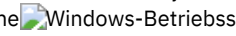
Yes

Gibt an, dass der Masterschlüssel des Servers beim Zurückschreiben der Datenbank zurückgeschrieben wird. Sie müssen ein Kennwort für diesen Parameter angeben.

Only

Gibt an, dass nur der Masterschlüssel des Servers zurückgeschrieben wird. Die Datenbank wird nicht zurückgeschrieben.

   PASSWORD

   Gibt das Kennwort an, das zum Schützen der Datenbanksicherung verwendet wird. Dieser Parameter gilt nur, wenn Sie verschlüsselte Containerspeicherpools in einer Cloudumgebung verwenden. Wenn Sie ein Kennwort für die Datenbanksicherung angeben, müssen Sie dasselbe Kennwort im Befehl RESTORE DB zum Zurückschreiben der Datenbank angeben. Sie müssen ein Kennwort verwenden, wenn Sie den Parameter RESTOREKEYS=YES oder RESTOREKEYS=ONLY angeben.

## Beispiel: Die Datenbank mit ihrem aktuellen Status zurückschreiben

---

Die Datenbank mit ihrem aktuellen Status unter Verwendung des bereits konfigurierten Verzeichnisses für aktive Protokolldatei zurückschreiben.

```
dsmserve restore db
```

## Beispiel: Masterschlüssel des Servers zurückschreiben, ohne die Datenbank zurückzuschreiben

---

Den folgenden Befehl ausgeben, um den Masterschlüssel des Servers zurückzuschreiben, ohne die Datenbank zurückzuschreiben:

```
dsmserve restore db restorekeys=only
```

## DSMSERV RESTORE DB (Datenbank nach Zeitpunkt zurückschreiben)

---

Verwenden Sie diesen Befehl, um eine Datenbank nach Zeitpunkt zurückzuschreiben. Eine Datenträgerhistorydatei und eine Einheitenkonfigurationsdatei müssen verfügbar sein.

Einschränkung: Sie können eine Serverdatenbank nicht zurückschreiben, wenn der Release-Level der Serverdatenbanksicherung von dem Release-Level des Servers abweicht, der zurückgeschrieben wird. Beispielsweise tritt ein Fehler auf, wenn Sie eine Datenbank der Version 7.1.3 zurückschreiben und Sie einen IBM Spectrum Protect-Server der Version 8.1 verwenden.

Sie können Gesamt- und Teilsicherungen der Datenbank oder Momentaufnahmesicherungen der Datenbank verwenden, um eine Datenbank nach Zeitpunkt zurückzuschreiben.

Tipp: Wenn Sie eine IBM Spectrum Protect-Serverdatenbank der Version 7 oder höher mit dem Stand eines bestimmten Zeitpunkts zurückschreiben, ist die bevorzugte Methode die Ausgabe des Befehls DSMSERV REMOVE DB vor der Ausgabe des Befehls DSMSERV RESTORE DB. Damit wird sichergestellt, dass das System einen ordnungsgemäßen Status aufweist. Das System löscht und entkatalogisiert die Datenbank im Hintergrund. Wenn Sie Daten mit dem Stand eines bestimmten Zeitpunkts zurückschreiben, werden alle erforderlichen Protokolle und das Datenbankimage von den Sicherungsdatenträgern abgerufen.















## Syntax

```
>>-DSMSERV----->
      | (1) |
      |----- -u--Benutzername-'
>----->
      | (1) |
      |----- -i--Instanzverzeichnis-'
      (2) .- -k--Server1-----
>----->
      |----- -k--Schlüsselname-' |----- -o--Optionsdatei-'
>-----+-----RESTORE DB--TODate----Datum----->
      | (1) |
      |----- -quiet-'
      .-TODate----23:59:59-. .-Source----DBBackup-----
>-----+-----+-----+----->
      |-----Zeit-----' |-----DBBackup----+'
      |-----DBSnapshot-'
>-----+-----+----->
      |-----RECOVdir----Verzeichnis-'
>-----+-----+----->
      |-----ACTIVELOGDir----Verzeichnis-'
      .-PREview----No-----
>-----+-----+-----+----->
      |-----ON----Zielverzeichnisdatei-' |-----PREview----+Yes+-'
      |-----No--'
      .-RESTOREKeys----No-----
>-----+-----+----->
      |-----RESTOREKeys----+No----+'
      |-----+YES--+'
      |-----ONLY-'
>-----+-----+-----><
      |-----PASSword----Kennwortname-'
```

Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.

## Parameter

-   **-u Benutzername**  
  Gibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird.
-   **-i Instanzverzeichnis**  
  Gibt ein Instanzverzeichnis an, das verwendet werden soll. Dies wird das aktuelle Arbeitsverzeichnis des Servers.
-  **-k Schlüsselname**  
 Gibt den Namen des Windows-Registrierungsschlüssels an, aus dem Informationen zum Server abgerufen werden sollen. Der Standardwert ist SERVER1.
- o Optionsdatei**  
Gibt eine Optionsdatei an, die verwendet werden soll.
-   **-quiet**  
  Gibt an, dass Nachrichten an die Konsole unterdrückt werden.
- TODate (Erforderlich)**  
Gibt das Datum an, auf das die Datenbank zurückgeschrieben werden soll. Die folgenden Werte sind gültig:
  - MM/TT/JJJJ**  
Gibt an, dass eine Datenbank unter Verwendung der letzten Sicherungsserie zurückgeschrieben werden soll, die vor diesem angegebenen Datum erstellt wurde.
  - TODAY**

Gibt an, dass eine Datenbank unter Verwendung der letzten Sicherungsserie zurückgeschrieben werden soll, die vor dem aktuellen Datum erstellt wurde.

TODAY-Tage oder -Tage

Gibt an, dass eine Datenbank unter Verwendung der letzten Sicherungsserie zurückgeschrieben werden soll, die die angegebene Anzahl Tage vor dem aktuellen Datum erstellt wurde.

TOTime

Gibt die Uhrzeit an, auf die die Datenbank zurückgeschrieben werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist das Ende des Tages (23:59:59). Gültige Werte:

HH:MM:SS

Gibt an, dass die Datenbank unter Verwendung der letzten Sicherungsserie zurückgeschrieben werden soll, die zu oder vor der angegebenen Zeit an dem Datum erstellt wurde, das im Parameter TODATE angegeben ist.

NOW

Gibt an, dass die Datenbank unter Verwendung einer Sicherungsserie zurückgeschrieben werden soll, die zu oder vor der aktuellen Zeit an dem Datum erstellt wurde, das im Parameter TODATE angegeben ist.

Wird beispielsweise das Dienstprogramm DSMSERV RESTORE DB um 9:00 mit TOTIME=NOW ausgegeben, wird die Datenbank unter Verwendung der letzten Sicherungsserie zurückgeschrieben, die um oder vor 9:00 an dem Datum erstellt wurde, das im Parameter TODATE angegeben ist.

NOW-Stunden:Minuten oder -Stunden:Minuten

Gibt an, dass die Datenbank unter Verwendung einer Sicherungsserie zurückgeschrieben werden soll, die zu oder vor der aktuellen Zeit minus einer angegebenen Anzahl Stunden und (wahlweise) Minuten an dem Datum erstellt wurde, das im Parameter TODATE angegeben ist.

Wird beispielsweise das Dienstprogramm DSMSERV RESTORE DB um 9:00 mit TOTIME=NOW-3:30 oder TOTIME+-3:30 ausgegeben, wird die Datenbank unter Verwendung der letzten Sicherungsserie zurückgeschrieben, die um oder vor 5:30 an dem Datum erstellt wurde, das im Parameter TODATE angegeben ist.

Source

Gibt an, ob die Datenbank unter Verwendung von Datenträgern mit Gesamt- und Teilsicherungen der Datenbank oder von Datenträgern mit Momentaufnahmesicherungen der Datenbank zurückgeschrieben wird. Dieser Parameter ist wahlfrei. Der Standardwert ist DBBackup. Die folgenden Werte sind gültig:

DBBackup

Gibt an, dass die Datenbank wie folgt zurückgeschrieben wird:

1. Die Datenträgerhistorydatei wird gelesen, um die erforderlichen Datenträger mit Gesamt- und Teilsicherungen der Datenbank zu lokalisieren.
2. Ladevorgänge werden angefordert und die Daten von den Datenträgern mit Gesamt- und Teilsicherungen der Datenbank nach Bedarf geladen, um den Datenbankdatenträger auf die angegebene Zeit zurückzuschreiben.

DBSnapshot

Gibt an, dass die Datenbank wie folgt zurückgeschrieben wird:

1. Die Datenträgerhistorydatei wird gelesen, um die erforderlichen Datenträger mit Momentaufnahmesicherungen der Datenbank zu lokalisieren.
2. Ladevorgänge werden angefordert und Daten von den Datenträgern mit Momentaufnahmesicherungen der Datenbank nach Bedarf geladen, um den Datenträger auf die angegebene Zeit zurückzuschreiben.

RECOVdir

Gibt ein Verzeichnis an, in dem Wiederherstellungsprotokollinformationen von den Datenbanksicherungsdatenträgern gespeichert werden sollen. Diese Protokollinformationen werden verwendet, um eine Transaktionskonsistenz der Serverdatenbank als Teil der Wiederherstellungsverarbeitung zu erreichen. Dieses Verzeichnis muss über ausreichend Speicherplatz verfügen, um diese Transaktionswiederherstellungsinformationen zu speichern, und es muss ein leeres Verzeichnis sein. Wird dieser Parameter nicht angegeben, ist der Standardwert das Verzeichnis, das mit einem der folgenden Parameter im Dienstprogramm DSMSERV FORMAT oder DSMSERV LOADFORMAT angegeben ist:



- ARCHFAILOVERLOGDIRECTORY, falls angegeben
- ARCHLOGDIRECTORY, wenn ARCHFAILOVERLOGDIRECTORY nicht angegeben ist

ACTIVELOGDir

Gibt ein Verzeichnis an, in dem die Protokolldateien gespeichert werden sollen, die zum Verfolgen der aktiven Datenbankoperationen verwendet werden. Geben Sie dieses Verzeichnis nur an, wenn zu einem anderen Verzeichnis für aktive Protokolldateien als dem bereits konfigurierten Verzeichnis umgeschaltet werden soll.

On



Gibt eine Datei an, in der die Verzeichnisse aufgelistet sind, in die die Datenbank zurückgeschrieben wird. Geben Sie jedes Verzeichnis in einer separaten Zeile in der Datei an. Beispielsweise gibt der Parameter ON die Datei restorelist.txt an, die die folgende Liste enthält:  AIX-Betriebssysteme  Linux-Betriebssysteme

```
/tsmdb001  
/tsmdb002  
/tsmdb003
```

 Windows-Betriebssysteme

```
e:\tsm\db001  
f:\tsm\db002  
g:\tsm\db003
```

Wird dieser Parameter nicht angegeben, werden die Ursprungsverzeichnisse verwendet, die in der Datenbanksicherung aufgezeichnet wurden.

Tipp: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zugrunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Sind ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse, reduzieren sie das Potenzial zum optimierten parallelen Vorabesezugriff und zur Verteilung der Datenbank.

#### PREVIEW

Gibt an, dass die Datenträgerhistorydateien geprüft und die Datenbanksicherungsdatenträger aus der Datenträgerhistorydatei ausgewertet werden.

1. Welche Gruppe von Datenbanksicherungsdatenträgern entspricht am besten den zeitpunktgesteuerten Kriterien, die für die Zurückschreibungsverarbeitung angegeben sind? Die Datenträgerhistorydaten stellen ausführliche Informationen zur Sicherungsserien-ID, zur Operations-ID (Gesamtsicherung, Teilsicherung 1, Teilsicherung 2, usw.), zum Datum der Datenbanksicherung und zur Einheitenklasse bereit. Diese Informationen und die im Befehl DSMSEV RESTORE DB angegebenen Parameter bestimmen, was für die Ausführung der Zurückschreibung verwendet wird. Die Datenträgerhistorydatei wird geprüft, um die beste Datenbanksicherung zu suchen, die den angegebenen zeitpunktgesteuerten Kriterien entspricht, und dann die Zurückschreibung mit dieser Sicherung auszuführen.
2. Sind selbst beschreibende Daten für die ausgewählte Gruppe von Datenbanksicherungsdatenträgern verfügbar? Überprüfen Sie die Datenträgerhistorydaten auf diese Sicherungsserie. Beim Datenabgleich wird der Inhalt der selbst beschreibenden Daten mit den Angaben aus den Datenträgerhistoryeinträgen verglichen. Die Überprüfung schließt das Laden eines oder mehrerer Datenträger ein, die von der Datenträgerhistory angegeben werden. Anschließend werden die selbst beschreibenden Daten, die in den Datenbanksicherungsdatenträgern enthalten waren, mit den Angaben in der Datenträgerhistory für die Datenbanksicherung abgeglichen. Sind die Informationen aus der Datenträgerhistorydatei und die selbst beschreibenden Daten nicht konsistent, werden Nachrichten ausgegeben, um das Problem zu identifizieren. Beispiel: Es wurden nicht alle Werte angegeben bzw. es sind nicht alle Werte verfügbar oder es wurden keine selbst beschreibenden Daten gefunden.




Sind die Datenträgerhistorydaten und die selbst beschreibenden Daten aus der Datenbanksicherung konsistent, wird eine Nachricht ausgegeben, die angibt, dass die Datenbanksicherung für die Zurückschreibungsverarbeitung verwendet werden kann.




Sind die Datenträgerhistorydaten und die selbst beschreibenden Daten aus der Datenbanksicherung nicht konsistent oder wurden die selbst beschreibenden Daten für die Sicherung nicht gefunden, werden Fehlermeldungen ausgegeben, die angeben, was überprüft wurde und was nicht gefunden wurde.

Wird der Parameter PREVIEW nicht angegeben oder wird der Parameter auf NO gesetzt und sind die Datenträgerhistorydaten und die selbst beschreibenden Daten aus der Datenbanksicherung konsistent, wird die Zurückschreibung fortgesetzt.

Wird der Parameter PREVIEW nicht angegeben oder wird der Parameter auf NO gesetzt und schlagen der Datenabgleich und die Überprüfung fehl, wird die Datenbankzurückschreibung nicht ausgeführt. Stellen Sie weitere Datenträger zur Verfügung, auf die von der Datenträgerhistorydatei verwiesen wird, oder entfernen Sie die unvollständige Sicherungsserie oder Operation, damit der IBM Spectrum Protect-Server eine andere bevorzugte Serie oder Operation auswählt und die Verarbeitung fortsetzt.

Wird der Parameter PREVIEW auf YES gesetzt, werden von dem Prozess nur die Auswertung der Datenträgerhistorydatei sowie der Datenabgleich und die Validierung mit der ausgewählten Datenbanksicherung ausgeführt.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme RESTOREKeys

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme Gibt an, ob der Masterverschlüsselungsschlüssel des Servers, der zum Verschlüsseln von Speicherpooldaten verwendet wird, zurückgeschrieben werden soll, wenn die Datenbank zurückgeschrieben wird. Dieser Parameter ist optional und gilt nur, wenn Sie verschlüsselte Containerspeicherpools in einer Cloudumgebung verwenden. Wenn der Masterschlüssel des Servers beim Zurückschreiben der Datenbank geschützt ist, ist der Standardwert YES. Wenn der Masterschlüssel des Servers beim Zurückschreiben der Datenbank nicht geschützt ist, ist der Standardwert NO. Sie können einen der folgenden Werte angeben:

No


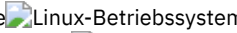
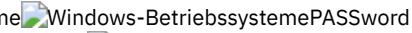
Gibt an, dass der Masterschlüssel des Servers beim Zurückschreiben der Datenbank nicht zurückgeschrieben wird.

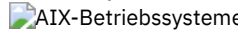
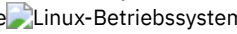
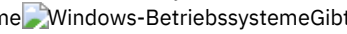
Yes

Gibt an, dass der Masterschlüssel des Servers beim Zurückschreiben der Datenbank zurückgeschrieben wird. Sie müssen ein Kennwort für diesen Parameter angeben.

Only

Gibt an, dass nur der Masterschlüssel des Servers zurückgeschrieben wird. Die Datenbank wird nicht zurückgeschrieben.

   PASSWORD

   Gibt das Kennwort an, das zum Schützen der Datenbanksicherung verwendet wird. Dieser Parameter gilt nur, wenn Sie verschlüsselte Containerspeicherpools in einer Cloudumgebung verwenden. Wenn Sie ein Kennwort für die Datenbanksicherung angeben, müssen Sie dasselbe Kennwort im Befehl RESTORE DB zum Zurückschreiben der Datenbank angeben. Sie müssen ein Kennwort verwenden, wenn Sie den Parameter RESTOREKEYS=YES oder RESTOREKEYS=ONLY angeben.

## Beispiel: Die Datenbank mit einer bestimmten Zeitangabe zurückschreiben

---

Die Datenbank mit ihrem Status am 12. Mai 2011 um 14:25 zurückschreiben.

```
dmserv restore db todate=05/12/2011 totime=14:45
```

## Beispiel: Masterschlüssel des Servers zurückschreiben, ohne die Datenbank zurückzuschreiben

---

Den folgenden Befehl ausgeben, um den Masterschlüssel des Servers zurückzuschreiben, ohne die Datenbank zurückzuschreiben:

```
dmserv restore db restorekeys=only
```



## DSMSERV UPDATE (Registry-Einträge für eine Serverinstanz erstellen)

---

Verwenden Sie dieses Dienstprogramm, um Registry-Einträge für eine IBM Spectrum Protect-Serverinstanz zu erstellen, wenn die Einträge versehentlich gelöscht wurden.

Führen Sie dieses Dienstprogramm im Instanzverzeichnis für die Datenbank aus (in dem Dateien, wie beispielsweise dmserv.dsk, für den Server gespeichert sind). Das Dienstprogramm erstellt die ursprünglichen Registry-Einträge für den Server erneut.

### Syntax

---

```
.. -k--Server1-----.  
>>-DSMSERV--+-+-----+---UPDATE-----><  
'- -k--Schlüsselname-'
```

### Parameter

---

-k Schlüsselname

Gibt den Namen des Windows-Registrierungsschlüssels an, in dem Informationen zum Server gespeichert werden sollen. Der Standardwert ist Server1.

## Beispiel: Registry-Einträge für eine Serverinstanz erneut erstellen

---

Führen Sie das Dienstprogramm aus, um Registry-Einträge für die Serverinstanz Server2 erneut zu erstellen.

```
"c:\Programme\Tivoli\TSM\server\bin\dmserv" -k server2 update
```

## DSMULOG (IBM Spectrum Protect-Servernachrichten in einer Benutzerprotokolldatei speichern)

---

Verwenden Sie diesen Befehl, um Nachrichten der IBM Spectrum Protect-Server-Konsole in einer Benutzerprotokolldatei zu speichern. Sie können angeben, dass IBM Spectrum Protect Nachrichten in mehrere Benutzerprotokolldateien schreiben soll.

Wichtig: Stellen Sie die Benutzerprotokolle nicht in das Dateisystem /usr oder /opt, da Speicherbeschränkungen in dem Dateisystem das Starten des Servers verhindern können.

## Syntax

---

```
      .-.-.-.-.-.
      |
      v
>>-DSMULOG---Protokolldateiname+-----><
```

## Parameter

---

Protokolldateiname (Erforderlich)

Gibt den Namen einer oder mehrerer Benutzerprotokolldateien an, in die IBM Spectrum Protect Serverkonsolnachrichten schreibt. Wenn Sie mehrere Dateinamen angeben, wird in jede Datei einen Tag lang geschrieben. Anschließend fährt der Server mit der nächsten Datei fort, um Protokollnachrichten zu speichern. Wenn in alle Dateien in der Liste geschrieben wurde, schreibt der Server wieder in die erste Datei und alle in dieser Datei enthaltenen Nachrichten werden überschrieben.

## Beispiel: Serverkonsolnachrichten auf täglicher Basis in einer Benutzerprotokolldatei speichern

---

Geben Sie die Benutzerprotokolldateien an, in denen Konsolnachrichten gespeichert werden sollen.

Wenn Sie in diesem Beispiel dieses Dienstprogramm am Freitag aufrufen, werden die Servernachrichten am Freitag in log1, am Samstag in log2 und am Sonntag in log3 gespeichert. Am Montag werden die Nachrichten in log1 gespeichert und die Nachrichten vom vorherigen Freitag werden überschrieben.

```
/opt/tivoli/tsm/server/bin/dsmserv -u tsminst1 -i
/tsmserv/tsminst1/tsminst1 2>&1 | dsmulog /tsmserv/tsminst1/tsminst1/log1
/tsmserv/tsminst1/tsminst1/log2
/tsmserv/tsminst1/tsminst1/log3 &
```




## Einheitendienstprogramme für den IBM Spectrum Protect-Server

---

Für Tasks, die sich auf das Konfigurieren von Speichereinheiten für den Server beziehen, können Sie Einheitendienstprogramme verwenden.

### Einheitendienstprogramme

---

-  AIX-Betriebssystemetsmdlst (Informationen zu Einheiten anzeigen)
-  Linux-Betriebssystemeautoconf (Einheiten automatisch konfigurieren)
-  Windows-Betriebssystemetsmdlst (Informationen zu Einheiten anzeigen)

 AIX-Betriebssysteme

## tsmdlst (Informationen zu Einheiten anzeigen)

---

Mit dem Dienstprogramm tsmdlst können Sie Einheitenamen und andere Informationen zu Datenträgerwechslern und Bandeneinheiten, die durch den IBM Spectrum Protect gesteuert werden, anzeigen.

Das Dienstprogramm tsmdlst ist Bestandteil des IBM Spectrum Protect-Einheitentreiberpakets, das für den Server und den Speicheragenten identisch ist. Sie müssen den IBM Spectrum Protect-Einheitentreiber installieren, um das Dienstprogramm tsmdlst für den Speicheragenten ausführen zu können.

Nach der Konfiguration von Einheiten können Sie das Dienstprogramm tsmdlst ausführen, um Einheitsdaten anzuzeigen. Das Dienstprogramm speichert diese Informationen in Dateien, die Sie abrufen können. Die Dateien haben den Namen lbinfo für Datenträgerwechsler und den Namen mtinfo für Bandeneinheiten. Nachdem eine Einheit hinzugefügt oder rekonfiguriert wurde, können Sie diese Dateien aktualisieren, indem Sie das Dienstprogramm tsmdlst erneut ausführen.

Das Dienstprogramm tsmdlst und die von ihm generierten Ausgabedateien befinden sich im Verzeichnis devices/bin, das standardmäßig /opt/tivoli/tsm/devices/bin lautet. Bevor Sie das Dienstprogramm tsmdlst ausführen, müssen Sie sicherstellen, dass entweder der IBM Spectrum Protect-Server gestoppt wurde oder alle Aktivitäten der Einheiten gestoppt wurden. Wird eine Einheit gerade vom IBM Spectrum Protect-Server verwendet, wenn das Dienstprogramm tsmdlst ausgeführt wird, erhalten Sie einen Fehler, der angibt, dass die Einheit aktiv ist.

## Optionen

---

/t

Zeigt Tracenachrichten für das Dienstprogramm tsmdlst an.

/?

Zeigt Nutzungsinformationen zum Dienstprogramm tsmdlst und zu seinen Parametern an.

 Linux-Betriebssysteme

## Beispiel: Informationen zu allen Einheiten anzeigen

---

Informationen zu allen Einheiten anzeigen, die durch den IBM Spectrum Protect-Einheitentreiber konfiguriert wurden:

tsmdlst

| TSM Device Name | Vendor | Product ID | Firmware | World Wide Name | Serial Number |
|-----------------|--------|------------|----------|-----------------|---------------|
| /dev/lb4        | ATL    | P3000      | 0100     | N/A             | 1651639999    |

| TSM Device Name | Vendor  | Product ID | Firmware | World Wide Name         | Serial Number  |
|-----------------|---------|------------|----------|-------------------------|----------------|
| /dev/mt0        | QUANTUM | DLT-S4     | 2A2A     | 50:0e:09:e0:00:16:ca:47 | QD0619AMD00052 |
| /dev/mt1        | QUANTUM | DLT-S4     | 2A2A     | 50:0e:09:e0:00:16:cd:e5 | QD0624AMD00184 |
| /dev/mt22       | QUANTUM | DLT7000    | 0100     | N/A                     | 1651639000     |
| /dev/mt23       | QUANTUM | DLT7000    | 0100     | N/A                     | 1651639002     |

 Linux-Betriebssysteme

## autoconf (Einheiten automatisch konfigurieren)

---

Verwenden Sie das Dienstprogramm autoconf, um Einheiten für die Verwendung mit dem IBM Spectrum Protect-Server zu konfigurieren.

Das Dienstprogramm autoconf führt die folgenden Tasks aus:

- Lädt den Treiber in den Kernel
- Erstellt die erforderlichen Dateien für den IBM Spectrum Protect-Einheitentreiber
- Erstellt Einheitendatendateien für Speicherarchive und Bandeinheiten

Das Dienstprogramm autoconf ist im Paket für den Einheitentreiber enthalten und wird im Verzeichnis /opt/tivoli/tsm/devices/bin installiert.

## Optionen

---

-a

Fügt den IBM Spectrum Protect-Einheitendateien Lese- und Schreibberechtigung hinzu, um allen Benutzern den Zugriff auf die Einheiten zu ermöglichen. Geben Sie diesen Wert an, um Einheiten zu konfigurieren, wenn der IBM Spectrum Protect-Server von einem Benutzer ohne Rootberechtigung gestartet wird.

-g

Fügt den IBM Spectrum Protect-Einheitendateien Lese- und Schreibberechtigung hinzu, um jedem Benutzer in derselben Gruppe die Verwendung der Einheiten als Rootbenutzer zu ermöglichen.

-t

Aktiviert die Tracefunktion für das Dienstprogramm autoconf.

-?

Zeigt Informationen zum Dienstprogramm autoconf und zu seinen Parametern an.

## Beispiel: Einheiten mit dem Dienstprogramm 'autoconf' konfigurieren

---

Führen Sie das Dienstprogramm autoconf aus, um IBM Spectrum Protect-Einheiten zu konfigurieren:

```
> /opt/tivoli/tsm/devices/bin/autoconf
```

 Linux-Betriebssysteme

## Beispiel: Einheiten mithilfe des Dienstprogramms 'autoconf' für einen Server konfigurieren, der von einer Benutzer-ID ohne Rootberechtigung gestartet wird

---

Führen Sie autoconf aus, um IBM Spectrum Protect-Einheiten zu konfigurieren. Verwenden Sie die Option a, da der Server von einer Benutzer-ID gestartet wird, die nicht der Rootbenutzer ist.

```
> /opt/tivoli/tsm/devices/bin/autoconf -a
```

```
Added the read and write permissions for all users to /dev/sg4.  
Added the read and write permissions for all users to /dev/sg5.
```

```

Added the read and write permissions for all users to /dev/sg6.
Added the read and write permissions for all users to /dev/sg7.
Added the read and write permissions for all users to /dev/sg8.
Added the read and write permissions for all users to /dev/sg9.
Added the read and write permissions for all users to /dev/sg10.
Added the read and write permissions for all users to /dev/sg11.
Added the read and write permissions for all users to /dev/sg12.
Added the read and write permissions for all users to /dev/sg13.
Added the read and write permissions for all users to /dev/sg14.
Added the read and write permissions for all users to /dev/sg15.
Added the read and write permissions for all users to /dev/sg16.
Added the read and write permissions for all users to /dev/sg17.
Added the read and write permissions for all users to /dev/sg18.
Added the read and write permissions for all users to /dev/sg19.
Added the read and write permissions for all users to /dev/sg20.
Added the read and write permissions for all users to /dev/sg21.
Added the read and write permissions for all users to /dev/sg22.
Added the read and write permissions for all users to /dev/sg23.
Added the read and write permissions for all users to /dev/sg24.
Added the read and write permissions for all users to /dev/sg25.
Added the read and write permissions for all users to /dev/sg26.
Added the read and write permissions for all users to /dev/sg27.
Added the read and write permissions for all users to /dev/sg28.
Added the read and write permissions for all users to /dev/sg29.

```

#### Tape Drives:

```

=====
Index Minor Host CHN ID LUN Type Vendor_ID Device_Serial_Number Product_ID Rev.
000 004 003 000 004 000 001 IBM 1068000439 ULTRIUM-HH5 C5X1
001 007 003 000 008 001 001 HP 01UbWSD-04 Ultrium 2-SCSI R210
002 008 003 000 008 002 001 HP 01UbWSD-05 Ultrium 2-SCSI R210
003 010 003 000 008 004 001 HP 01UbWSD-07 Ultrium 3-SCSI R210
004 012 003 000 008 006 001 HP 01UbWSD-01 Ultrium 3-SCSI R210
005 013 003 000 008 007 001 HP 01UbWSD-02 Ultrium 3-SCSI R210
006 014 003 000 008 008 001 HP 01UbWSD-08 Ultrium 3-SCSI R210
007 015 003 000 008 009 001 HP 01UbWSD-09 Ultrium 3-SCSI R210
008 016 003 000 008 010 001 HP 01UbWSD-0a Ultrium 3-SCSI R210
009 017 003 000 008 011 001 HP 01UbWSD-0b Ultrium 3-SCSI R210
010 018 003 000 008 012 001 HP 01UbWSD-0c Ultrium 3-SCSI R210
011 019 003 000 008 013 001 HP 01UbWSD-0d Ultrium 3-SCSI R210
012 020 003 000 005 000 001 IBM 1068000913 ULTRIUM-HH5 C5X1
013 022 003 000 009 001 001 QUANTUM 01UbWSD-0f SDLT320 R210
014 023 003 000 009 002 001 QUANTUM 01UbWSD-0g SDLT320 R210
015 024 003 000 009 003 001 QUANTUM 01UbWSD-0h SDLT320 R210
016 025 003 000 009 004 001 QUANTUM 01UbWSD-0i SDLT320 R210
017 026 003 000 006 000 001 IBM 1068001573 ULTRIUM-HH4 B5Q1
018 027 003 000 007 000 001 IBM 1068001545 ULTRIUM-HH4 B5Q1
019 028 003 000 010 000 001 HP HU19477PAE Ultrium 5-SCSI I65W

```

#### Medium Changer Devices:

```

=====
Index Minor Host CHN ID LUN Type Vendor_ID Device_Serial_Number Product_ID Rev.
000 005 003 000 004 001 008 NEC 2Y11BB0023 LL-2B01 0004
001 006 003 000 008 000 008 HP 01UbWSD-03 VLS 1.00
002 009 003 000 008 003 008 HP 01UbWSD-06 ThinStor AutoLdr T133
003 011 003 000 008 005 008 HP 01UbWSD-00 ESL E-Series 2.00
004 021 003 000 009 000 008 HP 01UbWSD-0e MSL6000 Series 0430
005 029 003 000 010 001 008 HP 3615-0101 MSL G3 Series 1120

```

 Windows-Betriebssysteme

## tsmdlst (Informationen zu Einheiten anzeigen)

Mit dem Dienstprogramm tsmdlst können Sie Einheitennamen und andere Informationen zu Datenträgerwechslern und Bandeinheiten auf dem System anzeigen.

### Optionen

Nach der Konfiguration von Einheiten können Sie das Dienstprogramm tsmdlst ausführen, um Einheitsdaten anzuzeigen. Das Dienstprogramm befindet sich im Einheitenverzeichnis 'server', das standardmäßig \Programme\Tivoli\TSM\server lautet.

/computer=Computername

Gibt den Namen des Computers an, für den Einheiten aufgelistet werden. Der Standardwert ist das lokale System.

/detail

Zeigt Details zu Einheiten in der Liste an. Standardmäßig wird eine Zusammenfassung angezeigt.

`/all`  
 Zeigt Informationen zu allen Einheitentypen an. Standardmäßig sind nur Bandlaufwerke und Bandarchive in den Ergebnissen enthalten.

`/nogenerictapecheck`  
 Überspringt den Schritt zum Öffnen erkannter Laufwerke, um zu bestimmen, ob sie für den IBM Spectrum Protect-Einheitentyp GENERICTAPE unterstützt werden.

`/nohbackcheck`  
 Überspringt den Schritt für die HBA-API-Erkennung. Damit kann die Verarbeitung beschleunigt werden. Diese Option kann hilfreich sein, wenn das Debugging erforderlich ist.

`/trace`  
 Wird für Diagnosezwecke verwendet. Speichert Traceausgabe in der Datei `tsmdlst_trace.txt`.

`/?`  
 Zeigt Nutzungsinformationen zum Dienstprogramm `tsmdlst` und zu seinen Parametern an.

`/xinquiry`  
 Stellt eine alternative Methode zum Abrufen der Seriennummer und des weltweiten Namens bereit. Diese Option wird nur für Einheiten verwendet, die vom IBM® Bandedeinheitentreiber unterstützt werden. Die folgenden Parameter gelten speziell für die Option `/xinquiry`:

`/processAll`  
 Gibt an, dass der Prozess so lange ausgeführt wird, bis alle Einheiten verarbeitet wurden.

`/maxRetries=#`  
 Gibt die maximale Anzahl Versuche an, jedes Laufwerk zu öffnen. Diese Option erfordert die Option `/processAll`.

`/genpathfile`  
 Verwenden Sie diese Option, um eine Liste mit Einheiten und Seriennummern zu generieren. Informationen für die Optionen `/genmacropathsync` und `/genmacropathoffline` werden in die Datei `tsmdlst_pathfile.txt` geschrieben.

`/includelib`  
 Wenn dieser Parameter mit der Option `/genpathfile` angegeben wird, schließt die Liste der Einheiten zusätzlich zu Laufwerken auch Speicherarchive ein.

`/genmacropathsync`  
 Generiert ein Makro, um IBM Spectrum Protect-Pfade für den Speicheragenten auf der Basis der Seriennummer zu synchronisieren. Ein Laufwerk muss eine für IBM Spectrum Protect definierte Seriennummer haben, damit diese Option funktioniert.

`/genmacropathoffline`  
 Generiert ein Makro, um IBM Spectrum Protect-Pfade für den Speicheragenten auf der Basis der Zugänglichkeit eines Laufwerks in den Online- oder Offline-Status zu aktualisieren. Auf ein Laufwerk kann zugegriffen werden, wenn ein Betriebssystemaufruf zum Öffnen zu einem der folgenden Ergebnisse führt: `ERROR_SUCCESS`, `ERROR_BUSY` oder `ERROR_ACCESS_DENIED`. Diese Option kann nur für Einheiten verwendet werden, die den IBM Einheitentreiber verwenden. Ein symbolischer Name, wie z. B. `\\.\tape0`, ist zum Öffnen einer Einheit erforderlich.  
 Die folgenden Optionen werden nur mit den Optionen `/genmacropathsync` und `/genmacropathoffline` verwendet:

`/server=Servername`  
 Gibt den Namen des Servers an, den der Speicheragent verwendet.

`/stagent=Name des Speicheragenten`  
 Gibt den Namen des Speicheragenten an.

`/tcps=Adresse`  
 Gibt die IBM Spectrum Protect-Serveradresse an.

`/tcpport=Port`  
 Gibt den IBM Spectrum Protect-Server-Port an. Der Standardwert ist 1500.

`/id=ID`  
 Gibt die IBM Spectrum Protect-Administrator-ID an.

`/pass=Kennwort`  
 Gibt das IBM Spectrum Protect-Administratorkennwort an.

`/devicetype=Laufwerktyp`  
 Gibt den Einheitentyp des Laufwerks an, beispielsweise `LTO`. Bei dieser Option muss die Groß-/Kleinschreibung beachtet werden. Die Option ist optional.

`/libraryname=Speicherarchivname`  
 Filtert den Speicherarchivnamen des Laufwerks, z. B. `LTO3584`. Bei dieser Option muss die Groß-/Kleinschreibung beachtet werden. Die Option ist optional.

`/execmacropathsync`  
 Gibt das Makro zum Synchronisieren des Pfads an den IBM Spectrum Protect-Server aus.

`/execmacropathoffline`  
 Gibt das Makro zum Aktualisieren des Pfads in den Online- oder Offline-Status an den IBM Spectrum Protect-Server aus.

`/addpaths`

Fügt Anweisungen DEFINE und UPDATE PATH hinzu. Diese Option wird mit der Option /genmacropathsync verwendet.  
 /verbose  
 Listet Laufwerk- und Pfadinformationen, die vom IBM Spectrum Protect-Server zurückgegeben werden, und den Inhalt der Pfaddatei auf.  
 /encodednames  
 Wird ein Pfad auf online=no gesetzt, werden Zeitmarke, Fehler und Einheit als aktualisierter Einheitenname verschlüsselt.

## Beispiel: Informationen zu Einheiten anzeigen

Informationen zu Bandeinheiten und Bandarchiven für das lokale System WANTON anzeigen, indem das Dienstprogramm tsmdblst ausgeführt wird:

```
tsmdblst
```

Der angezeigte Einheitenname ist der Aliasname, der im Befehl DEFINE PATH und im Befehl UPDATE PATH verwendet werden kann. Der Aliasname ist nicht der tatsächliche Einheitenname.

```
Computer Name:      WANTON
OS Version:        6.2
OS Build #:        9200
TSM Device Driver: TSMScsi - Not Running
```

4 HBAs were detected.

| Manufacturer       | Model   | Driver     | Version   | Firmware | NodeWWN          | Description                          |
|--------------------|---------|------------|-----------|----------|------------------|--------------------------------------|
| QLogic Corporation | QLE2562 | ql2300.sys | 9.1.11.28 | 7.03.00  | 20000024FF25F846 | QLogic QLE2562 Fibre Channel Adapter |
| QLogic Corporation | QLE2562 | ql2300.sys | 9.1.11.28 | 7.03.00  | 20000024FF25F847 | QLogic QLE2562 Fibre Channel Adapter |
| QLogic Corporation | QLE2562 | ql2300.sys | 9.1.11.28 | 7.03.00  | 20000024FF25F7FE | QLogic QLE2562 Fibre Channel Adapter |
| QLogic Corporation | QLE2562 | ql2300.sys | 9.1.11.28 | 7.03.00  | 20000024FF25F7FF | QLogic QLE2562 Fibre Channel Adapter |

| TSM Name Identifier | ID   | LUN | Bus | Port | SSN              | WWN              | TSM Type | Driver | Device |
|---------------------|------|-----|-----|------|------------------|------------------|----------|--------|--------|
| mt0.0.0.7           | 0    | 0   | 0   | 7    | 000001327176     | 5005076300566011 | 3592     | IBM    | IBM    |
| 03592E06            | 2883 |     |     |      |                  |                  |          |        |        |
| lb0.1.0.7           | 0    | 1   | 0   | 7    | 0000013400480405 | 5005076300566011 | LIBRARY  | IBM    | IBM    |
| 03584L22            | E01q |     |     |      |                  |                  |          |        |        |
| mt1.0.0.7           | 1    | 0   | 0   | 7    | 000001327147     | 5005076300566012 | 3592     | IBM    | IBM    |
| 03592E06            | 2883 |     |     |      |                  |                  |          |        |        |
| mt2.0.0.7           | 2    | 0   | 0   | 7    | 000001327349     | 5005076300566013 | 3592     | IBM    | IBM    |
| 03592E06            | 2883 |     |     |      |                  |                  |          |        |        |
| mt3.0.0.7           | 3    | 0   | 0   | 7    | 000001327140     | 5005076300566014 | 3592     | IBM    | IBM    |
| 03592E06            | 2883 |     |     |      |                  |                  |          |        |        |
| mt4.0.0.7           | 4    | 0   | 0   | 7    | 1068000254       | 500507630F51FA05 | LTO      | IBM    | IBM    |
| ULT3580-TD5         | D8D4 |     |     |      |                  |                  |          |        |        |
| lb4.1.0.7           | 4    | 1   | 0   | 7    | 0000078216780402 | 500507630F51FA05 | LIBRARY  | IBM    | IBM    |
| 03584L32            | C460 |     |     |      |                  |                  |          |        |        |
| mt5.0.0.7           | 5    | 0   | 0   | 7    | 1068000039       | 500507630F51FA06 | LTO      | IBM    | IBM    |
| ULT3580-TD5         | D8D4 |     |     |      |                  |                  |          |        |        |
| mt6.0.0.7           | 6    | 0   | 0   | 7    | 1068000047       | 500507630F51FA07 | LTO      | IBM    | IBM    |
| ULT3580-TD5         | D8D4 |     |     |      |                  |                  |          |        |        |
| mt7.0.0.7           | 7    | 0   | 0   | 7    | 1068000017       | 500507630F51FA08 | LTO      | IBM    | IBM    |
| ULT3580-TD5         | D8D4 |     |     |      |                  |                  |          |        |        |

## Server-Scripts und Makros für die Automatisierung

Sie können allgemeine Verwaltungstasks automatisieren, indem Sie IBM Spectrum Protect-Server-Scripts und Makros des Verwaltungsclients erstellen. Server-Scripts werden in der Serverdatenbank gespeichert und können für die Ausführung mit einem Befehl für Verwaltungszeitpläne geplant werden. Makros des Verwaltungsclients werden als Dateien auf dem Verwaltungscient gespeichert. Makros können nicht serverübergreifend verteilt und nicht auf dem Server geplant werden.

- **Server-Scripts**  
 Sie können allgemeine Verwaltungstasks mithilfe von Scripts, die in der Serverdatenbank gespeichert sind, automatisieren. Sie können die Verarbeitung eines Scripts mithilfe des Verwaltungsbefehlsschedulers auf dem Server planen.

- Makros des Verwaltungsclients  
Ein Makro ist eine Datei, die mindestens einen Verwaltungsclientbefehl enthält. Sie können ein Makro vom Verwaltungsclient aus nur im Stapelmodus oder im interaktiven Modus ausführen. Makros werden als Datei auf dem Verwaltungsclient gespeichert. Sie werden nicht über Server verteilt und können nicht auf dem Server geplant werden.

## Server-Scripts

---

Sie können allgemeine Verwaltungstasks mithilfe von Scripts, die in der Serverdatenbank gespeichert sind, automatisieren. Sie können die Verarbeitung eines Scripts mithilfe des Verwaltungsbefehlschedulers auf dem Server planen.

IBM Spectrum Protect-Scripts weisen die folgende Funktionalität und Anweisungen auf:

- Befehlsparametersubstitution
- Befehle SELECT, die Sie bei der Verarbeitung des Scripts angeben
- Steuerung der Befehlsausführung, wie beispielsweise die Verarbeitungsoptionen PARALLEL und SERIAL
- Ablaufanweisungen mit bedingter Logik. Diese Logikablaufanweisungen umfassen die folgenden Anweisungen:
  - Die Klausel IF; diese Klausel legt fest, wie die Verarbeitung auf der Basis des aktuellen Rückkehrcodewerts fortgesetzt wird.
  - Die Anweisung EXIT; diese Anweisung beendet die Scriptverarbeitung.
  - Die Anweisungen GOTO und LABEL; diese Anweisungen steuern den Logikablauf so, dass die Verarbeitung bei der Zeile fortgesetzt wird, die mit der angegebenen Kennzeichnung beginnt
- Kommentarzeilen

Beispielscripts werden in der Datei scripts.smp bereitgestellt. Die Beispielscripts verfügen über eine beispielhafte Ausführungsreihenfolge zur Zeitplanung von Verwaltungsbefehlen.

Wenn einer der Befehle in dem Script nicht erfolgreich verarbeitet wird, werden die übrigen Befehle nicht verarbeitet.

- Server-Script definieren  
Sie können ein Server-Script zeilenweise definieren, eine Datei erstellen, die Befehlszeilen enthält, oder ein vorhandenes Script kopieren.
- Script aktualisieren  
Sie können ein Script aktualisieren, um eine Befehlszeile zu ändern oder einem Script eine Befehlszeile hinzuzufügen.
- Server-Script zum Erstellen eines anderen Server-Scripts abfragen  
Sie können weitere Server-Scripts durch Abfragen eines Scripts unter Angabe der Parameter FORMAT=RAW und OUTPUTFILE erstellen. Die Ausgabe der Abfrage kann als Eingabe für ein neues Script verwendet werden, so dass das neue Script nicht zeilenweise erstellt werden muss.
- Server-Script ausführen  
Um ein Script zu verarbeiten, verwenden Sie den Befehl RUN. Sie können ein Script, das Substitutionsvariablen enthält, ausführen, indem Sie die Substitutionsvariablen im Befehl RUN angeben.

## Server-Script definieren

---

Sie können ein Server-Script zeilenweise definieren, eine Datei erstellen, die Befehlszeilen enthält, oder ein vorhandenes Script kopieren.

### Informationen zu diesem Vorgang

---

Einschränkung: Sie können die Ausgabe eines Befehls in einem Server-Script nicht umleiten. Führen Sie stattdessen das Script aus und geben Sie dann die Befehlsumleitung an. Um beispielsweise die Ausgabe von script1 in das Verzeichnis c:\temp\test.out umzuleiten, führen Sie das Script aus und geben Sie die Befehlsumleitung wie in dem folgenden Beispiel gezeigt an:

```
run script1 > c:\temp\test.out
```

### Vorgehensweise

---

1. Definieren Sie ein Script mit dem Befehl DEFINE SCRIPT. Anfänglich kann mit diesem Befehl die erste Zeile des Scripts definiert werden. Beispiel:

```
define script qaixc "select node_name from nodes where platform='aix'"
desc='AIX-Clients anzeigen'
```

In diesem Beispiel wird das Script als QAIXC definiert. Wenn das Script ausgeführt wird, werden alle AIX-Clients angezeigt.

2. Definieren Sie mit dem Befehl UPDATE SCRIPT weitere Zeilen in dem Script. Wenn beispielsweise ein Befehl QUERY SESSION hinzugefügt werden soll, geben Sie Folgendes ein:

```
update script qaixc "query session *"
```



3. Optional: Sie können einen Parameter WAIT im Befehl DEFINE CLIENTACTION angeben. Mithilfe dieses Parameters können Sie festlegen, dass die Clientaktion abgeschlossen sein muss, bevor der nächste Schritt im Befehlsscript oder Makro verarbeitet wird.
  4. Optional: Mit dem Befehl ISSUE MESSAGE können Sie feststellen, wo innerhalb eines Befehls in einem Script ein Problem vorliegt.
- Befehle parallel oder seriell ausführen  
Sie können Befehle in einem Script seriell, parallel oder seriell und parallel ausführen. Geben Sie dazu den Scriptbefehl SERIAL oder PARALLEL im Parameter COMMAND\_LINE der Befehle DEFINE und UPDATE SCRIPT an. Demzufolge ist es möglich, mehrere Befehle parallel auszuführen und zu warten, bis sie beendet sind, bevor der nächste Befehl ausgeführt wird.
  - Befehle über mehrere Befehlszeilen fortsetzen  
Lange Befehle können über mehrere Befehlszeilen fortgesetzt werden, indem ein Fortsetzungszeichen (-) als letztes Zeichen in einer Zeile eines fortzusetzenden Befehls angegeben wird.
  - Substitutionsvariablen in ein Script einschließen  
Sie können Substitutionsvariablen in ein Script einschließen. Substitutionsvariablen werden durch das Zeichen \$ angegeben, gefolgt von einer Ziffer, die die Position des Parameters bei der Verarbeitung des Scripts angibt.
  - Logikablaufanweisungen in ein Script einschließen  
Sie können Ablaufanweisungen mit bedingter Logik verwenden, die auf Rückkehrcodes basieren, die bei der vorherigen Befehlsverarbeitung ausgegeben wurden. Mithilfe dieser Logikanweisungen können Sie Ihre Scripts gemäß dem Ergebnis bestimmter Befehle verarbeiten. Die Anweisungen IF, EXIT und GOTO (LABEL) können verwendet werden.
  - Befehle SELECT in einem Script verwenden  
Ein IBM Spectrum Protect-Script besteht aus mindestens einem Befehl und wird als Objekt in der Datenbank gespeichert. Sie können ein Script definieren, das einen oder mehrere Befehle SELECT enthält.

## Befehle parallel oder seriell ausführen

---

Sie können Befehle in einem Script seriell, parallel oder seriell und parallel ausführen. Geben Sie dazu den Scriptbefehl SERIAL oder PARALLEL im Parameter COMMAND\_LINE der Befehle DEFINE und UPDATE SCRIPT an. Demzufolge ist es möglich, mehrere Befehle parallel auszuführen und zu warten, bis sie beendet sind, bevor der nächste Befehl ausgeführt wird.

### Informationen zu diesem Vorgang

---

Durch die serielle Ausführung von Befehlen in einem Script wird sichergestellt, dass alle vorhergehenden Befehle abgeschlossen sind, bevor der nächste Befehl ausgeführt wird, und dass alle nachfolgenden Befehle seriell ausgeführt werden. Wenn ein Script gestartet wird, werden alle Befehle so lange seriell ausgeführt, bis ein Befehl PARALLEL gefunden wird. Mehrere Befehle, die parallel ausgeführt werden und auf gemeinsame Ressourcen, wie beispielsweise Bandlaufwerke, zugreifen, können seriell ausgeführt werden.

Scriptrückkehrcodes vor und nach der Ausführung eines Befehls PARALLEL ändern sich nicht. Wenn ein Befehl SERIAL gefunden wird, wird der Scriptrückkehrcode auf den maximalen Rückkehrcode aller vorhergehenden Befehle gesetzt, die parallel ausgeführt wurden.

Wenn Sie Serverbefehle verwenden, die den Parameter WAIT im Anschluss an einen Befehl PARALLEL unterstützen, ist das Verhalten wie folgt:

- Wenn Sie den Standardwert WAIT=NO angeben oder verwenden, wartet das Script nicht auf den Abschluss des Befehls, wenn ein nachfolgender Befehl SERIAL gefunden wird. Der Rückkehrcode von diesem Befehl spiegelt die Verarbeitung nur bis zu dem Punkt wider, an dem der Befehl einen Hintergrundprozess startet. Der abschließende Rückkehrcode des Befehls ist für das Script nicht verfügbar.
- Wenn Sie WAIT=YES angeben, wartet das Script auf den Abschluss des Befehls, wenn ein nachfolgender Befehl SERIAL gefunden wird. Der Rückkehrcode von diesem Befehl spiegelt die Verarbeitung für den gesamten Befehl wider.

In den meisten Fällen können Sie WAIT=YES in Befehlen verwenden, die parallel ausgeführt werden.

Einschränkung: Wenn mit dem Befehl ein Hintergrundprozess gestartet wird, für den nicht der Parameter WAIT angegeben ist, wird der Befehl als abgeschlossen betrachtet, nachdem der Hintergrundthread gestartet wurde. Daher kann der Befehl nur in Parallelverarbeitung ausgeführt werden.

Das folgende Beispiel zeigt die Verwendung des Befehls PARALLEL zum Sichern, Umlagern und Wiederherstellen von Speicherpools.

```
/*mehrere Befehle parallel ausführen und auf deren Beendigung warten, bevor fortgefahren wird*/
PARALLEL
/*vier Speicherpools gleichzeitig sichern*/
BACKUP STGPOOL PRIMPOOL1 COPYPOOL1 WAIT=YES
BACKUP STGPOOL PRIMPOOL2 COPYPOOL2 WAIT=YES
BACKUP STGPOOL PRIMPOOL3 COPYPOOL3 WAIT=YES
BACKUP STGPOOL PRIMPOOL4 COPYPOOL4 WAIT=YES
/*warten, bis alle vorherigen Befehle beendet sind*/
SERIAL
/*nach Beendigung der Sicherungen die Speicherpools gleichzeitig umlagern*/
PARALLEL
MIGRATE STGPOOL PRIMPOOL1 DURATION=90 WAIT=YES
```

```

MIGRATE STGPOOL PRIMPOOL2 DURATION=90 WAIT=YES
MIGRATE STGPOOL PRIMPOOL3 DURATION=90 WAIT=YES
MIGRATE STGPOOL PRIMPOOL4 DURATION=90 WAIT=YES
/*warten, bis alle vorherigen Befehle beendet sind*/
SERIAL
/*nach Beendigung der Umlagerung die Speicherpools gleichzeitig wiederherstellen*/
PARALLEL
RECLAIM STGPOOL PRIMPOOL1 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL2 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL3 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL4 DURATION=120 WAIT=YES

```

#### Zugehörige Verweise:

DEFINE SCRIPT (Server-Script definieren)  
 UPDATE SCRIPT (Server-Script aktualisieren)

## Befehle über mehrere Befehlszeilen fortsetzen

---

Lange Befehle können über mehrere Befehlszeilen fortgesetzt werden, indem ein Fortsetzungszeichen (-) als letztes Zeichen in einer Zeile eines fortzusetzenden Befehls angegeben wird.

### Informationen zu diesem Vorgang

---

Im folgenden Beispiel wird eine SQL-Anweisung über mehrere Befehlszeilen fortgesetzt:

```

/*-----*/
/* Beispiel einer Fortsetzung */
SELECT-
* FROM-
NODE WHERE-
PLATFORM='win32'

```

Wenn dieser Befehl verarbeitet wird, wird der folgende Befehl ausgeführt:

```
select * from nodes where platform='win32'
```

## Substitutionsvariablen in ein Script einschließen

---

Sie können Substitutionsvariablen in ein Script einschließen. Substitutionsvariablen werden durch das Zeichen \$ angegeben, gefolgt von einer Ziffer, die die Position des Parameters bei der Verarbeitung des Scripts angibt.

### Informationen zu diesem Vorgang

---

In dem folgenden Beispielscript SQLSAMPLE sind die Substitutionsvariablen \$1 und \$2 angegeben:

```

/*-----*/
/* Beispiel einer Substitution */
/* -----*/
SELECT-
$1 FROM-
NODES WHERE-
PLATFORM='$2'

```

Wenn Sie das Script ausführen, müssen Sie zwei Werte angeben, einen Wert für \$1 und einen Wert für \$2. Beispiel:

```
run sqlsample node_name aix
```

Der folgende Befehl wird verarbeitet, wenn das Script SQLSAMPLE ausgeführt wird:

```
select node_name from nodes where platform='aix'
```

## Logikablaufanweisungen in ein Script einschließen

---

Sie können Ablaufanweisungen mit bedingter Logik verwenden, die auf Rückkehrcodes basieren, die bei der vorherigen Befehlsverarbeitung ausgegeben wurden. Mithilfe dieser Logikanweisungen können Sie Ihre Scripts gemäß dem Ergebnis bestimmter Befehle verarbeiten. Die Anweisungen IF, EXIT und GOTO (LABEL) können verwendet werden.

Bei der Verarbeitung der Befehle in einem Script wird der Rückkehrcode für eine mögliche Auswertung gesichert, bevor der nächste Befehl verarbeitet wird. Der Rückkehrcode kann eine der drei folgenden Bewertungsstufen haben: OK, WARNING oder ERROR. Eine Liste

der gültigen Rückkehrcodes und Bewertungsstufen finden Sie in Rückkehrcodes für die Verwendung in Scripts.

- **Klausel IF angeben**  
Mit der Klausel IF am Anfang einer Befehlszeile kann bestimmt werden, wie die Verarbeitung des Scripts auf der Basis des aktuellen Rückkehrcodewertes fortgesetzt wird. In der Klausel IF wird ein symbolischer Wert oder eine Bewertung für einen Rückkehrcode angegeben.
- **Anweisung EXIT angeben**  
Verwenden Sie die Anweisung EXIT, um die Scriptverarbeitung zu beenden.
- **Anweisung GOTO angeben**  
Die Anweisung GOTO wird zusammen mit einer Kennzeichnungsanweisung verwendet. Die Kennzeichnungsanweisung ist das Ziel der Anweisung GOTO. Die Anweisung GOTO führt die Scriptverarbeitung zu der Zeile mit der Kennzeichnungsanweisung, damit die Verarbeitung an diesem Punkt wiederaufgenommen wird.

## Klausel IF angeben

---

Mit der Klausel IF am Anfang einer Befehlszeile kann bestimmt werden, wie die Verarbeitung des Scripts auf der Basis des aktuellen Rückkehrcodewertes fortgesetzt wird. In der Klausel IF wird ein symbolischer Wert oder eine Bewertung für einen Rückkehrcode angegeben.

### Informationen zu diesem Vorgang

---

Der Server setzt den Rückkehrcode am Anfang des Scripts anfänglich auf RC\_OK. Der Rückkehrcode wird durch jeden verarbeiteten Befehl aktualisiert. Entspricht der aktuelle Rückkehrcode aus dem verarbeiteten Befehl einem der Rückkehrcodes oder einer der Bewertungen in der Klausel IF, wird der Rest der Zeile verarbeitet. Entspricht der aktuelle Rückkehrcode keinem der aufgelisteten Werte, wird die Zeile übersprungen.

Mit dem folgenden Beispielscript wird der Speicherpool BACKUPPOOL nur dann gesichert, wenn momentan keine Sitzungen auf den Server zugreifen. Die Sicherung wird nur dann fortgesetzt, wenn der Rückkehrcode RC\_NOTFOUND empfangen wird:

```
/* Speicherpools sichern, wenn keine Clients auf den Server zugreifen */
select * from sessions
/* Keine Sitzungen vorhanden, wenn rc_notfound empfangen wird */
if(rc_notfound) backup stg backuppool copypool
```

Mit dem folgenden Beispielscript wird der Speicherpool BACKUPPOOL gesichert, wenn ein Rückkehrcode mit der Bewertung WARNING empfangen wird:

```
/* Speicherpools sichern, wenn keine Clients auf den Server zugreifen */
select * from sessions
/* Keine Sitzungen vorhanden, wenn rc_notfound empfangen wird */
if(warning) backup stg backuppool copypool
```

## Anweisung EXIT angeben

---

Verwenden Sie die Anweisung EXIT, um die Scriptverarbeitung zu beenden.

### Informationen zu diesem Vorgang

---

Im folgenden Beispiel wird mit der Klausel IF in Verbindung mit RC\_OK festgestellt, ob Clients auf den Server zugreifen. Der Empfang des Rückkehrcodes RC\_OK gibt an, dass Clientsitzungen auf den Server zugreifen. Das Script wird mit der Anweisung EXIT fortgesetzt und die Sicherung wird nicht gestartet.

```
/* Speicherpools sichern, wenn keine Clients auf den Server zugreifen */
select * from sessions
/* Sitzungen vorhanden, wenn rc_ok empfangen wird */
if(rc_ok) exit
backup stg backuppool copypool
```

## Anweisung GOTO angeben

---

Die Anweisung GOTO wird zusammen mit einer Kennzeichnungsanweisung verwendet. Die Kennzeichnungsanweisung ist das Ziel der Anweisung GOTO. Die Anweisung GOTO führt die Scriptverarbeitung zu der Zeile mit der Kennzeichnungsanweisung, damit die Verarbeitung an diesem Punkt wiederaufgenommen wird.

### Informationen zu diesem Vorgang

---

Hinter der Kennzeichnungsanweisung steht immer ein Doppelpunkt (:); hinter dem Doppelpunkt muss keine Angabe stehen. Das folgende Beispiel zeigt, wie mit der Anweisung GOTO ein Speicherpool nur dann gesichert wird, wenn momentan keine Sitzungen auf den Server zugreifen. In diesem Beispiel zeigt der Rückkehrcode RC\_OK an, dass Clients auf den Server zugreifen. Die Anweisung GOTO überträgt die Verarbeitung an die Kennzeichnung done:, die die Anweisung EXIT enthält, mit der die Scriptverarbeitung beendet wird:

```
/* Speicherpools sichern, wenn keine Clients auf den Server zugreifen */
select * from sessions
/* Sitzungen vorhanden, wenn rc_ok empfangen wird */
if(rc_ok) goto done
backup stg backuppool copypool
done:exit
```

## Befehle SELECT in einem Script verwenden

---

Ein IBM Spectrum Protect-Script besteht aus mindestens einem Befehl und wird als Objekt in der Datenbank gespeichert. Sie können ein Script definieren, das einen oder mehrere Befehle SELECT enthält.

## Informationen zu diesem Vorgang

---

Ein Script kann über einen Verwaltungsclient oder über die Serverkonsole ausgeführt werden. Außerdem kann es einem Zeitplan für Verwaltungsbefehle hinzugefügt werden, damit es automatisch ausgeführt wird. Ausführliche Informationen befinden sich in Server-Scripts.

IBM Spectrum Protect wird mit einer Datei ausgeliefert, die eine Reihe von Beispielscripts enthält. Die Datei scripts.smp befindet sich im Serververzeichnis. Um die Scripts zu erstellen und als Objekte in Ihrer Serverdatenbank zu speichern, geben Sie den Befehl DSMSERV RUNFILE während der Installation aus:

```
> dsmserv runfile scripts.smp
```

Sie können die Datei auch als Makro über einen Verwaltungsbefehlszeilenclient ausführen:

```
macro scripts.smp
```

Die Datei mit den Beispielscripts enthält Befehle. Diese Befehle löschen zuerst alle Scripts mit denselben Namen wie die zu definierenden Scripts und definieren anschließend die Scripts. Die meisten Beispiele erstellen Befehle SELECT, andere sichern beispielsweise Speicherpools. Sie können die Datei mit den Beispielscripts auch kopieren und ändern, um eigene Scripts zu erstellen.

Nachfolgend sind einige Beispiele aus der Datei mit den Beispielscripts aufgeführt:

```
def script q_inactive_days '/* -----*/'
upd script q_inactive_days '/* Scriptname: Q_INACTIVE */'
upd script q_inactive_days '/* Beschreibung: Knoten anzeigen, die für eine */'
upd script q_inactive_days '/* bestimmte Anzahl Tage nicht auf den */'
upd script q_inactive_days '/* Sicherungsserver zugegriffen haben */'
upd script q_inactive_days '/* Parameter 1: Tage */'
upd script q_inactive_days '/* Beispiel: run q_inactive_days 5 */'
upd script q_inactive_days '/* -----*/'
upd script q_inactive_days "select node_name,lastacc_time from nodes where -"
upd script q_inactive_days " cast((current_timestamp-lastacc_time)days as -"
upd script q_inactive_days " decimal) >= $1 "

/* Nachrichten mit Wertigkeit X oder Y im Aktivitätenprotokoll anzeigen */

def script q_msg_sev desc='Nachr. mit Wertigk. X oder Y im Akt.-Prot. anz. '
upd script q_msg_sev '/* -----*/'
upd script q_msg_sev '/* Scriptname: Q_MSG_S EV */'
upd script q_msg_sev '/* Beschreibung: Nachrichten im Aktivitätenproto- */'
upd script q_msg_sev '/* koll mit einer der angegebenen */'
upd script q_msg_sev '/* Wertigkeiten anzeigen. */'
upd script q_msg_sev '/* Parameter 1: Wertigkeit 1 */'
upd script q_msg_sev '/* Parameter 2: Wertigkeit 2 */'
upd script q_msg_sev '/* Dabei ist Wertigkeit I, W, E, S oder D */'
upd script q_msg_sev '/* Beispiel: run q_msg_sev S E */'
upd script q_msg_sev '/* -----*/'
upd script q_msg_sev "select date_time,msgno,message from actlog -"
upd script q_msg_sev " where severity=upper('$1') or severity=upper('$2')"
```

## Script aktualisieren

---

Sie können ein Script aktualisieren, um eine Befehlszeile zu ändern oder einem Script eine Befehlszeile hinzuzufügen.

- **Neuen Befehl anfügen**  
Um einem vorhandenen Script eine Befehlszeile anzufügen, den Befehl UPDATE SCRIPT mit dem Parameter LINE= ausgeben. Der angefügten Befehlszeile wird eine um fünf größere Zeilennummer als der letzten Befehlszeile in der Befehlszeilenfolge zugeordnet. Wenn ein Script beispielsweise mit der Zeile 010 endet, wird der angefügten Befehlszeile die Zeilennummer 015 zugeordnet.
- **Vorhandenen Befehl ersetzen**  
Sie können eine vorhandene Befehlszeile ändern, indem Sie den Parameter LINE= angeben.
- **Befehl und Zeilennummer hinzufügen**  
Sie können ein vorhandenes Script ändern, indem Sie neue Zeilen hinzufügen.
- **Befehl aus einem Server-Script löschen**  
Aus einem Script kann eine einzelne Befehlszeile gelöscht werden. Wenn eine Zeilennummer angegeben wird, wird nur die entsprechende Befehlszeile aus dem Script gelöscht.

## Neuen Befehl anfügen

---

Um einem vorhandenen Script eine Befehlszeile anzufügen, den Befehl UPDATE SCRIPT mit dem Parameter LINE= ausgeben. Der angefügten Befehlszeile wird eine um fünf größere Zeilennummer als der letzten Befehlszeile in der Befehlszeilenfolge zugeordnet. Wenn ein Script beispielsweise mit der Zeile 010 endet, wird der angefügten Befehlszeile die Zeilennummer 015 zugeordnet.

### Informationen zu diesem Vorgang

---

Das folgende Beispiel zeigt das Script QSTATUS. Das Script hat die Zeilen 001, 005 und 010:

```
001 /* Dies ist das Script QSTATUS */
005  QUERY STATUS
010  QUERY PROCESS
```

Um den Befehl QUERY SESSION am Ende des Scripts anzufügen, geben Sie den folgenden Befehl aus:

```
update script qstatus "query session"
```

Dem Befehl QUERY SESSION wird die Befehlszeilennummer 015 zugeordnet; das aktualisierte Script sieht wie folgt aus:

```
001 /* Dies ist das Script QSTATUS */
005  QUERY STATUS
010  QUERY PROCESS
015  QUERY SESSION
```

## Vorhandenen Befehl ersetzen

---

Sie können eine vorhandene Befehlszeile ändern, indem Sie den Parameter LINE= angeben.

### Informationen zu diesem Vorgang

---

Zeilennummer 010 in dem Script QSTATUS enthält einen Befehl QUERY PROCESS. Um den Befehl QUERY PROCESS durch den Befehl QUERY STGPOOL zu ersetzen, geben Sie den Parameter LINE= wie folgt an:

```
update script qstatus "query stgpool" line=10
```

Das Script QSTATUS wird aktualisiert und enthält dann die folgenden Zeilen:

```
001 /* Dies ist das Script QSTATUS */
005  QUERY STATUS
010  QUERY STGPOOL
015  QUERY SESSION
```

## Befehl und Zeilennummer hinzufügen

---

Sie können ein vorhandenes Script ändern, indem Sie neue Zeilen hinzufügen.

### Informationen zu diesem Vorgang

---

Um dem Script QSTATUS den Befehl QUERY NODE OPEN als neue Zeile 007 hinzuzufügen, geben Sie den folgenden Befehl aus:

```
update script qstatus "query node" line=7
```

Das Script QSTATUS wird aktualisiert und enthält dann die folgenden Zeilen:

```
001 /* Dies ist das Script QSTATUS */
005 QUERY STATUS
007 QUERY NODE
010 QUERY STGPOOL
015 QUERY SESSION
```

## Befehl aus einem Server-Script löschen

---

Aus einem Script kann eine einzelne Befehlszeile gelöscht werden. Wenn eine Zeilennummer angegeben wird, wird nur die entsprechende Befehlszeile aus dem Script gelöscht.

### Informationen zu diesem Vorgang

---

Um beispielsweise die Befehlszeile 007 aus dem Script QSTATUS zu löschen, geben Sie den folgenden Befehl aus:

```
delete script qstatus line=7
```

## Server-Script zum Erstellen eines anderen Server-Scripts abfragen

---

Sie können weitere Server-Scripts durch Abfragen eines Scripts unter Angabe der Parameter FORMAT=RAW und OUTPUTFILE erstellen. Die Ausgabe der Abfrage kann als Eingabe für ein neues Script verwendet werden, so dass das neue Script nicht zeilenweise erstellt werden muss.

### Informationen zu diesem Vorgang

---

Das folgende Beispiel zeigt, wie das Script SRTL2 abgefragt und die Ausgabe in newscript.script übertragen wird:

```
query script srtl2 format=raw outputfile=newscript.script
```

Sie können die Datei newscript.script dann mit einem auf Ihrem System verfügbaren Editor editieren. Um ein neues Script mithilfe der editierten Ausgabe Ihrer Abfrage zu erstellen, geben Sie Folgendes aus:

```
define script srtnew file=newscript.script
```

## Server-Script ausführen

---

Um ein Script zu verarbeiten, verwenden Sie den Befehl RUN. Sie können ein Script, das Substitutionsvariablen enthält, ausführen, indem Sie die Substitutionsvariablen im Befehl RUN angeben.

### Informationen zu diesem Vorgang

---

Um ein Script zu stoppen, das gerade ausgeführt wird, muss ein Administrator den Server anhalten. Sie können ein Script nach seinem Start nicht mit einem IBM Spectrum Protect-Befehl abbrechen.

### Vorgehensweise

---

- Rufen Sie eine Voranzeige der Befehle in einem Script auf, um das Script vor seiner Ausführung auszuwerten. Um die Voranzeige des Scripts aufzurufen, ohne die Befehle auszuführen, geben Sie den Befehl RUN mit dem Parameter PREVIEW=YES ein. Wenn das Script Substitutionsvariablen enthält, werden die Befehle mit den ersetzten Variablen angezeigt.
- Führen Sie ein Script, das keine Variablen enthält, durch Eingabe des folgenden Befehls aus: `run qaixc`; dabei ist `qaixc` der Name des Scripts.
- Führen Sie ein Script, das Substitutionsvariablen enthält, durch Angabe der Variablenwerte im Befehl aus. Inhalt des Scripts:

```
/*-----*/
/* Fortsetzungs- und Substitutionsbeispiel */
/* -----*/
SELECT-
$1 FROM-
NODES WHERE-
PLATFORM='$2'
```

Um dieses Script auszuführen, geben Sie den folgenden Befehl ein:

```
run qaixc Knotenname aix
```

Dabei ist `Knotenname` der Wert für die Variable `$1` und `aix` der Wert für die Variable `$2`.

**Zugehörige Verweise:**  
RUN (Server-Script ausführen)

## Makros des Verwaltungsclients

---

Ein Makro ist eine Datei, die mindestens einen Verwaltungsclientbefehl enthält. Sie können ein Makro vom Verwaltungsclient aus nur im Stapelmodus oder im interaktiven Modus ausführen. Makros werden als Datei auf dem Verwaltungsclient gespeichert. Sie werden nicht über Server verteilt und können nicht auf dem Server geplant werden.

Makros können die folgenden Elemente enthalten:

- Serververwaltungsbefehle
- Kommentare
- Fortsetzungszeichen
- Variablen

Der Name für ein Makro muss die Namenskonventionen des Verwaltungsclients erfüllen, der unter Ihrem Betriebssystem ausgeführt wird.

Verwenden Sie in einem Makro, das mehrere Befehle enthält, die Befehle COMMIT und ROLLBACK, um die Befehlsverarbeitung innerhalb des Makros zu steuern.

Sie können den Befehl MACRO in eine Makrodatei einschließen, um weitere Makros aufzurufen (bis zu 10 Ebenen sind möglich). Ein über die Befehlszeile des Verwaltungsclients aufgerufenes Makro wird als Makro höherer Ebene bezeichnet. Alle Makros, die innerhalb des Makros höherer Ebene aufgerufen werden, werden als *verschachtelte* Makros bezeichnet.

- Befehle in ein Makro schreiben  
Fügen sie einem Makro Verwaltungsbefehle hinzu. Der Verwaltungsclient ignoriert alle in Ihren Makros enthaltenen Leerzeilen. Ein Befehl, der (mit einem Fortsetzungszeichen) fortgesetzt wird, wird jedoch durch eine Leerzeile beendet.
- Kommentare in ein Makro schreiben  
Fügen Sie Ihrer Makrodatei Kommentare hinzu, um den Zweck oder die in der Datei enthaltenen Befehle zu beschreiben.
- Fortsetzungszeichen in ein Makro einschließen  
Sie können Fortsetzungszeichen in einer Makrodatei verwenden, wenn ein Befehl ausgeführt werden soll, der länger als die Anzeigen- oder Fensterbreite ist.
- Substitutionsvariablen in ein Makro einschließen  
Sie können Substitutionsvariablen in einem Makro verwenden, sodass Sie bei der Ausführung des Makros Werte für Elemente wie beispielsweise Befehlsparameter angeben können. Bei der Verwendung von Substitutionsvariablen kann ein Makro wiederholt zur Ausführung derselben Task für verschiedene Objekte oder mit unterschiedlichen Parameterwerten verwendet werden.
- Makro ausführen  
Verwenden Sie den Befehl MACRO, wenn ein Makro ausgeführt werden soll. Sie können den Befehl MACRO im Stapelmodus oder im interaktiven Modus eingeben.
- Befehlsverarbeitung in einem Makro  
Wenn Sie einen Befehl MACRO ausgeben, verarbeitet der Server nacheinander alle Befehle in der Makrodatei, einschließlich der Befehle, die in verschachtelten Makros enthalten sind. Der Server schreibt alle Befehle in einem Makro fest, nachdem die Verarbeitung der Makros höherer Ebene erfolgreich abgeschlossen wurde.

## Befehle in ein Makro schreiben

---

Fügen sie einem Makro Verwaltungsbefehle hinzu. Der Verwaltungsclient ignoriert alle in Ihren Makros enthaltenen Leerzeilen. Ein Befehl, der (mit einem Fortsetzungszeichen) fortgesetzt wird, wird jedoch durch eine Leerzeile beendet.

## Informationen zu diesem Vorgang

---

Das folgende Beispiel zeigt ein Makro mit dem Namen REG.MAC, das einen neuen Administrator registriert und ihm Berechtigungen erteilt:

```
register admin pease mypasswd -  
  contact='david pease, x1234'  
grant authority pease -  
  classes=policy,storage -  
  jdomains=domain1,domain2 -  
  stgpools=stgpool1,stgpool2
```

Dieses Beispiel verwendet Fortsetzungszeichen in der Makrodatei. Weitere Informationen zu Fortsetzungszeichen befinden sich in Fortsetzungszeichen in ein Makro einschließen.

Nach der Erstellung einer Makrodatei können die darin enthaltenen Informationen aktualisiert werden, um sie erneut verwenden zu können. Sie können die Makrodatei auch kopieren. Nachdem Sie eine Kopie des Makros erstellt haben, können Sie die Kopie ändern und ausführen.

## Kommentare in ein Makro schreiben

---

Fügen Sie Ihrer Makrodatei Kommentare hinzu, um den Zweck oder die in der Datei enthaltenen Befehle zu beschreiben.

### Informationen zu diesem Vorgang

---

Gehen Sie wie folgt vor, um einen Kommentar zu schreiben:

- Schreiben Sie einen Schrägstrich und einen Stern (/\*), um den Anfang des Kommentars anzugeben.
- Schreiben Sie den Kommentar.
- Schreiben Sie einen Stern und einen Schrägstrich (\*//), um das Ende des Kommentars anzugeben.

Ein Kommentar kann auf einer eigenen Zeile oder auf einer Zeile stehen, die einen Befehl oder einen Teil eines Befehls enthält.

Um beispielsweise den Zweck eines Makros mithilfe eines Kommentars zu erläutern, geben Sie die folgende Zeile ein:

```
/* auth.mac - neue Knoten registrieren */
```

Ein Kommentar kann auch verwendet werden, um einen Befehl oder einen Teil eines Befehls zu erläutern:

```
domain=domain1 /*Knoten domain1 zuordnen */
```

Kommentare dürfen nicht verschachtelt werden und können sich nicht über mehrere Zeilen erstrecken. Jede Zeile eines Kommentars muss die Kommentarbegrenzer enthalten.

## Fortsetzungszeichen in ein Makro einschließen

---

Sie können Fortsetzungszeichen in einer Makrodatei verwenden, wenn ein Befehl ausgeführt werden soll, der länger als die Anzeigen- oder Fensterbreite ist.

### Informationen zu diesem Vorgang

---

Ohne Fortsetzungszeichen können bis zu 256 Zeichen eingegeben werden. Mit Fortsetzungszeichen können bis zu 1500 Zeichen eingegeben werden. Im Befehl MACRO werden Werte der Substitutionsvariablen bei der Anzahl Zeichen berücksichtigt.

Geben Sie als Fortsetzungszeichen einen Bindestrich oder einen umgekehrten Schrägstrich am Ende der fortzusetzenden Zeile ein. Mit Fortsetzungszeichen können Sie die folgenden Zeilen eines Makros fortsetzen.

### Beispiele

---

- Befehl fortsetzen; Beispiel:

```
register admin pease mypasswd -  
contact="david, ext1234"
```

- Eine Liste mit Werten durch einen Bindestrich oder einen umgekehrten Schrägstrich fortsetzen; dabei darf nach dem letzten Komma der Zeile, die auf der ersten Zeile begonnen wurde, kein Leerzeichen verwendet werden. Danach die restlichen Teile der Liste in die nächste Zeile eingeben, wobei die Zeile nicht mit Leerzeichen begonnen werden darf. In dem folgenden Beispiel wird eine Liste mit Speicherpoolnamen über mehrere Zeilen fortgesetzt:

```
stgpools=stg1, stg2, stg3, -  
stg4, stg5, stg6
```

- Um eine Zeichenfolge aus Werten, die in Hochkommas oder Anführungszeichen eingeschlossen ist, fortzusetzen, schließen Sie den ersten Teil der Zeichenfolge in Hochkommas bzw. Anführungszeichen ein und geben Sie am Ende der Zeile einen Bindestrich oder einen umgekehrten Schrägstrich ein. Geben Sie dann den Rest der Zeichenfolge in die nächste Zeile ein. Schließen Sie den Rest der Zeichenfolge analog zum ersten Teil der Zeichenfolge in Hochkommas bzw. Anführungszeichen ein. Das folgende Beispiel zeigt eine Zeichenfolge, die über mehrere Zeilen fortgesetzt wird:

```
contact="david pease, bldg. 100, room 2b, san jose, "-  
"ext. 1234, alternate contact-norm pass, ext 2345"
```

Die beiden Zeichenfolgen werden ohne Zwischenleerschritte verkettet. Zum Fortsetzen einer in Hochkommas oder Anführungszeichen eingeschlossenen Zeichenfolge aus Werten über mehrere Zeilen darf nur diese Methode verwendet werden.



## Substitutionsvariablen in ein Makro einschließen

---

Sie können Substitutionsvariablen in einem Makro verwenden, sodass Sie bei der Ausführung des Makros Werte für Elemente wie beispielsweise Befehlsparameter angeben können. Bei der Verwendung von Substitutionsvariablen kann ein Makro wiederholt zur Ausführung derselben Task für verschiedene Objekte oder mit unterschiedlichen Parameterwerten verwendet werden.

### Informationen zu diesem Vorgang

---

Eine Substitutionsvariable besteht aus einem Prozentzeichen (%), gefolgt von einer eindeutigen Zahl, die die Substitutionsvariable angibt. Wenn Sie die Datei mit dem Befehl MACRO ausführen, müssen Sie für die Variablen Werte angeben.

Einschränkungen:

- Wenn Ihr System das Prozentzeichen als Platzhalterzeichen verwendet, interpretiert der Verwaltungsclient einen Mustererkennungsausdruck in einem Makro, bei dem auf das Prozentzeichen direkt eine Ziffer folgt, als Substitutionsvariable.
- Eine Substitutionsvariable kann nicht zwischen Anführungszeichen gesetzt werden. Ein Wert, den Sie als Substitution für die Variable angeben, kann jedoch eine Zeichenfolge in Anführungszeichen sein.

### Beispiel

---

Erstellen Sie ein Makro mit dem Namen AUTH.MAC zum Registrieren neuer Knoten. Das Makro enthält vier Substitutionsvariablen für Parameter in dem Befehl:

```
/* neue Knoten registrieren */
register node %1 %2 -          /* Benutzer-ID, Kennwort           */
contact=%3 -                 /* 'Name, Telefonnummer'     */
domain=%4                    /* Maßnahmendomäne           */
```

Wenn Sie das Makro ausführen, müssen Sie die Werte eingeben, die zur Verarbeitung des Befehls an den Server übergeben werden sollen.

Um beispielsweise das Makro zum Registrieren des Knotens mit dem Namen DAVID und dem Kennwort DAVIDPW zu verwenden, einen Namen und eine Telefonnummer als Kontaktinformationen einzuschließen und den Knoten der Maßnahmendomäne DOMAIN1 zuzuordnen, geben Sie den folgenden Befehl ein:

```
macro auth.mac david davidpw "david pease, x1234" domain1
```

## Makro ausführen

---

Verwenden Sie den Befehl MACRO, wenn ein Makro ausgeführt werden soll. Sie können den Befehl MACRO im Stapelmodus oder im interaktiven Modus eingeben.

### Informationen zu diesem Vorgang

---

Wenn das Makro keine Substitutionsvariablen enthält, führen Sie das Makro aus, indem Sie den Befehl MACRO zusammen mit dem Namen der Makrodatei eingeben. Beispiel:

```
macro reg.mac
```

Wenn das Makro Substitutionsvariablen enthält, geben Sie die bereitzustellenden Werte hinter dem Makronamen ein. Jeder Wert wird durch ein Leerzeichen begrenzt. Beispiel:

```
macro auth.mac pease mypasswd "david pease, x1234" domain1
```

Wenn weniger Werte eingegeben werden als Substitutionsvariablen im Makro vorhanden sind, ersetzt der Verwaltungsclient die restlichen Variablen durch Nullzeichenfolgen.

Wenn ein oder mehrere Werte zwischen Werten übergangen werden sollen, geben Sie für jeden übergangenen Wert eine Nullzeichenfolge ("" ) ein. Wenn beispielsweise die Kontaktinformationen aus dem vorhergehenden Beispiel übergangen werden sollen, folgendes eingeben:

```
macro auth.mac pease mypasswd "" domain1
```

**Zugehörige Verweise:**  
MACRO (Makro aufrufen)

## Befehlsverarbeitung in einem Makro

---

Wenn Sie einen Befehl MACRO ausgeben, verarbeitet der Server nacheinander alle Befehle in der Makrodatei, einschließlich der Befehle, die in verschachtelten Makros enthalten sind. Der Server schreibt alle Befehle in einem Makro fest, nachdem die Verarbeitung der Makros höherer Ebene erfolgreich abgeschlossen wurde.

Wenn in einem der Befehle in dem Makro oder in einem der verschachtelten Makros ein Fehler auftritt, stoppt der Server die Verarbeitung und macht alle Änderungen rückgängig, die durch alle vorhergehenden Befehle vorgenommen wurden.

Wenn Sie bei der Eingabe des Befehls DSMADMC die Option ITEMCOMMIT angeben, schreibt der Server jeden Befehl in einem Script oder einem Makro einzeln fest, nachdem die Verarbeitung für den jeweiligen Befehl erfolgreich abgeschlossen wurde. Wenn ein Fehler auftritt, setzt der Server die Verarbeitung fort und macht nur die Änderungen rückgängig, die durch den fehlgeschlagenen Befehl verursacht wurden.

Mit dem Befehl COMMIT können Sie präzise steuern, wann Befehle festgeschrieben werden. Wenn ein Fehler auftritt, während der Server die Befehle in einem Makro verarbeitet, beendet der Server die Verarbeitung des Makros und macht alle nicht festgeschriebenen Änderungen rückgängig. Nicht festgeschriebene Änderungen sind Befehle, die seit dem letzten Befehl COMMIT verarbeitet wurden. Stellen Sie sicher, dass Ihre Verwaltungsclientsitzung nicht mit der Option ITEMCOMMIT ausgeführt wird, wenn die Befehlsverarbeitung mit dem Befehl COMMIT gesteuert werden soll.

Sie können ein Makro vor seiner Implementierung mit dem Befehl ROLLBACK testen. Sie können die Befehle (mit Ausnahme des Befehls COMMIT), die ausgegeben werden sollen, in das Makro eingeben und ROLLBACK als letzten Befehl eingeben. Dann können Sie das Makro ausführen, um zu prüfen, ob alle Befehle erfolgreich verarbeitet werden. Alle Änderungen an der Datenbank, die durch die Befehle vorgenommen wurden, werden mit dem Befehl ROLLBACK rückgängig gemacht. Sie dürfen nicht vergessen, den Befehl ROLLBACK zu entfernen, bevor Sie das Makro zur Verwendung freigeben. Stellen Sie außerdem sicher, dass die Verwaltungsclientsitzung nicht mit der Option ITEMCOMMIT ausgeführt wird, wenn die Befehlsverarbeitung mit dem Befehl ROLLBACK gesteuert werden soll.

Tipp: Befehle, die Hintergrundprozesse starten, können nicht rückgängig gemacht werden.

Wenn eine Serie von Befehlen verwendet wird, die über die Befehlszeile erfolgreich ausgeführt werden, jedoch fehlschlagen, wenn sie in einem Makro ausgegeben werden, bestehen möglicherweise Abhängigkeiten zwischen den Befehlen. Es ist möglich, dass ein innerhalb eines Makros ausgegebener Befehl erst erfolgreich ausgeführt werden kann, wenn ein vorhergehender Befehl, der innerhalb desselben Makros ausgeführt wird, festgeschrieben wurde. Jede der beiden folgenden Aktionen ermöglicht die erfolgreiche Verarbeitung dieser Befehle innerhalb eines Makros:

- Fügen Sie einen Befehl COMMIT vor dem Befehl ein, der von einem vorherigen Befehl abhängig ist. Wenn beispielsweise COMMAND C von COMMAND B abhängig ist, würden Sie einen Befehl COMMIT vor COMMAND C einfügen.

```
command a
command b
commit
command c/
```

- Starten Sie die Verwaltungsclientsitzung unter Verwendung der Option ITEMCOMMIT. Diese Option hat zur Folge, dass jeder Befehl in einem Makro festgeschrieben wird, bevor der nächste Befehl verarbeitet wird.

#### Zugehörige Verweise:

COMMIT (Festschreiben von Befehlen in einem Makro steuern)

ROLLBACK (Nicht festgeschriebene Änderungen in einem Makro rückgängig machen)

## Rückkehrcodes für die Verwendung in IBM Spectrum Protect-Scripts

Sie können IBM Spectrum Protect-Scripts schreiben, die Rückkehrcodes verwenden, um den Fortschritt der Scriptverarbeitung zu bestimmen. Die Rückkehrcodes können eine von drei Wertigkeiten haben: OK, WARNING, ERROR.

IBM Spectrum Protect-Scripts verwenden den symbolischen Rückkehrcode für die Verarbeitung, nicht den numerischen Wert. Der Verwaltungsclient zeigt die numerischen Werte an, wenn ein Befehl ausgeführt wird. Die Rückkehrcodes werden in der folgenden Tabelle angezeigt.

Tabelle 1. Rückkehrcodes

| Rückkehrcode | Wertigkeit | Numerischer Wert | Beschreibung   |
|--------------|------------|------------------|--|
| RC_OK        | OK         | 0                | Der Befehl wurde erfolgreich ausgeführt.   |
| RC_UNKNOWN   | ERROR      | 2                | Der Befehl wird nicht gefunden; kein bekannter Befehl.                                 |
| RC_SYNTAX    | ERROR      | 3                | Der Befehl ist gültig, aber ein oder mehrere Parameter wurden nicht korrekt angegeben. |

| <b>Rückkehrcode</b> | <b>Wertigkeit</b> | <b>Numerischer Wert</b> | <b>Beschreibung</b>  |
|---------------------|-------------------|-------------------------|--|
| RC_ERROR            | ERROR             | 4                       | Ein interner Serverfehler hat die erfolgreiche Ausführung des Befehls verhindert.  |
| RC_NOMEMORY         | ERROR             | 5                       | Der Befehl konnte nicht ausgeführt werden, da auf dem Server nicht genügend Speicher vorhanden ist.  |
| RC_NOLOG            | ERROR             | 6                       | Der Befehl konnte nicht ausgeführt werden, da auf dem Server nicht genügend Speicherbereich für das Wiederherstellungsprotokoll vorhanden ist. |
| RC_NODB             | ERROR             | 7                       | Der Befehl konnte nicht ausgeführt werden, da auf dem Server nicht genügend Datenbankbereich vorhanden ist.                                    |
| RC_NOSTORAGE        | ERROR             | 8                       | Der Befehl konnte nicht ausgeführt werden, da auf dem Server nicht genügend Speicherbereich vorhanden ist.                                     |
| RC_NOAUTH           | ERROR             | 9                       | Der Befehl ist fehlgeschlagen, da der Administrator nicht berechtigt ist, den Befehl auszugeben.   |
| RC_EXISTS           | ERROR             | 10                      | Der Befehl ist fehlgeschlagen, da das angegebene Objekt bereits auf dem Server vorhanden ist.  |
| RC_NOTFOUND         | WARNING           | 11                      | Wird von einem Befehl QUERY oder SQL SELECT zurückgegeben, wenn keine Objekte gefunden werden, die den Spezifikationen entsprechen.            |
| RC_INUSE            | ERROR             | 12                      | Der Befehl ist fehlgeschlagen, da das Objekt, mit dem gearbeitet werden sollte, im Gebrauch war.   |
| RC_ISREFERENCED     | ERROR             | 13                      | Der Befehl ist fehlgeschlagen, da das Objekt, mit dem gearbeitet werden sollte, noch von einem anderen Serverkonstrukt referenziert wird.      |
| RC_NOTAVAILABLE     | ERROR             | 14                      | Der Befehl ist fehlgeschlagen, da das Objekt, mit dem gearbeitet werden sollte, nicht verfügbar ist.   |
| RC_IOERROR          | ERROR             | 15                      | Der Befehl ist fehlgeschlagen, da ein E/A-Fehler auf dem Server festgestellt wurde.  |
| RC_NOTXN            | ERROR             | 16                      | Der Befehl ist fehlgeschlagen, da eine Datenbanktransaktion auf dem Server fehlgeschlagen ist.   |
| RC_NOLOCK           | ERROR             | 17                      | Der Befehl ist fehlgeschlagen, da ein Sperrenkonflikt in der Serverdatenbank festgestellt wurde.   |
| RC_NOTHREAD         | ERROR             | 19                      | Der Befehl konnte nicht ausgeführt werden, da auf dem Server nicht genügend Speicher vorhanden ist.  |
| RC_LICENSE          | ERROR             | 20                      | Der Befehl ist fehlgeschlagen, da der Server die Lizenzierung nicht einhält.   |
| RC_INVDEST          | ERROR             | 21                      | Der Befehl ist fehlgeschlagen, da ein Zielwert ungültig war.   |
| RC_IFILEOPEN        | ERROR             | 22                      | Der Befehl ist fehlgeschlagen, da eine erforderliche Eingabedatei nicht geöffnet werden konnte.  |
| RC_OFILEOPEN        | ERROR             | 23                      | Der Befehl ist fehlgeschlagen, da er eine erforderliche Ausgabedatei nicht öffnen konnte.  |
| RC_OFILEWRITE       | ERROR             | 24                      | Der Befehl ist fehlgeschlagen, da er nicht erfolgreich in eine erforderliche Ausgabedatei schreiben konnte.                                    |
| RC_INVADMIN         | ERROR             | 25                      | Der Befehl ist fehlgeschlagen, da der Administrator nicht definiert war.   |
| RC_SQLERROR         | ERROR             | 26                      | Ein SQL-Fehler wurde während der Abfrage einer Anweisung SELECT festgestellt.  |

| Rückkehrcode    | Wertigkeit | Numerischer Wert | Beschreibung   |
|-----------------|------------|------------------|--|
| RC_INVALIDUSE   | ERROR      | 27               | Der Befehl ist fehlgeschlagen, da er nicht korrekt verwendet wurde.  |
| RC_NOTABLE      | ERROR      | 28               | Der Befehl ist aufgrund eines unbekanntes SQL-Tabellennamens fehlgeschlagen.   |
| RC_FS_NOTCAP    | ERROR      | 29               | Der Befehl ist aufgrund nicht kompatibler Typen des Dateibereichsnamens fehlgeschlagen.                                    |
| RC_INVALIDADDR  | ERROR      | 30               | Der Befehl ist aufgrund einer falschen Adresse der höheren Ebene oder Adresse der unteren Ebene fehlgeschlagen.            |
| RC_INVALIDCG    | ERROR      | 31               | Der Befehl ist fehlgeschlagen, da die Verwaltungsklasse keine Archivierungskopiengruppe hat.                               |
| RC_OVERSIZE_VOL | ERROR      | 32               | Der Befehl ist fehlgeschlagen, da die Datenträgergröße den maximal zulässigen Wert überschreitet.                          |
| RC_DEFVOL_FAIL  | ERROR      | 33               | Der Befehl ist fehlgeschlagen, da Datenträger nicht in Speicherpools mit RECLAMATIONTYPE=SNAPLOCK definiert werden können. |
| RC_DELVOL_FAIL  | ERROR      | 34               | Der Befehl ist fehlgeschlagen, da Datenträger nicht in Speicherpools mit RECLAMATIONTYPE=SNAPLOCK gelöscht werden können.  |
| RC_CANCELED     | WARNING    | 35               | Der Befehl wurde abgebrochen.  |
| RC_INVPOLICY    | ERROR      | 36               | Der Befehl ist fehlgeschlagen, da die Maßnahmendomäne eine ungültige Definition enthält.                                   |
| RC_INVALIDPW    | ERROR      | 37               | Der Befehl ist aufgrund eines ungültigen Kennworts fehlgeschlagen.   |
| RC_UNSUPP_PARM  | WARNING    | 38               | Der Befehl ist fehlgeschlagen, da der Befehl oder der Parameter nicht unterstützt wird.                                    |

**Zugehörige Verweise:**

DEFINE SCRIPT (IBM Spectrum Protect-Prozedur definieren)  
UPDATE SCRIPT (IBM Spectrum Protect-Prozedur aktualisieren)  
RUN (IBM Spectrum Protect-Prozedur ausführen)

## Serverdokumentation in PDF-Dateien

Vorgefertigte PDF-Dateien für die IBM Spectrum Protect-Dokumentation sind zum Herunterladen verfügbar.

Tipp: Ab Version 7.1.3 ist das *Administratorhandbuch* veraltet. Verwenden Sie die Handbücher für Speicherlösungen, um eine Plattenspeicherlösung für einen einzelnen Standort und eine Plattenspeicherlösung für mehrere Standorte zu implementieren und zu verwalten. Prozeduren für die Ausführung von Systemverwaltungstasks sind in den folgenden Abschnitten verfügbar:

- Speicherumgebung konfigurieren und verwalten
- IBM Spectrum Protect-Datenschutzlösungen

Verwenden Sie für die Ausführung der folgenden Tasks die PDF-Dateien in den folgenden Links.

| Task  | Komponenten   | Links                             |
|---|---|-----------------------------------|
| Informationen zu Produktkonzepten und -lösungen lesen | <ul style="list-style-type: none"> <li>• Server</li> <li>• Operations Center</li> </ul> | Einführung in Datenschutzlösungen |

| Task                                  | Komponenten   | Links   |
|---------------------------------------|---|---|
| Best-Practice-Lösung implementieren   | <ul style="list-style-type: none"> <li>• Server</li> <li>• Operations Center</li> </ul> | <ul style="list-style-type: none"> <li>• Plattenspeicherlösung für einen einzelnen Standort</li> <li>• Plattenspeicherlösung für mehrere Standorte</li> <li>• Bandspeicherlösung</li> </ul> |
| Komponenten installieren              | <ul style="list-style-type: none"> <li>• Server</li> <li>• Operations Center</li> </ul> | <ul style="list-style-type: none"> <li>• AIX</li> <li>• Linux</li> <li>• Windows</li> </ul>   |
| Upgrade für Komponenten durchführen   | <ul style="list-style-type: none"> <li>• Server</li> </ul>                              | <ul style="list-style-type: none"> <li>• AIX</li> <li>• Linux</li> <li>• Windows</li> </ul>   |
| Befehle und Optionen verwenden        | <ul style="list-style-type: none"> <li>• Server</li> </ul>                              | <ul style="list-style-type: none"> <li>• AIX</li> <li>• Linux</li> <li>• Windows</li> </ul>   |
| Nachrichten und Fehlercodes verwenden | <ul style="list-style-type: none"> <li>• Server</li> </ul>                              | Alle Betriebssysteme  |

## IBM Spectrum Protect-Clients für Sichern/Archivieren

Verwenden Sie den IBM Spectrum Protect-Client für Sichern/Archivieren, um Kopien von Dateien und Verzeichnissen auf Ihrer Workstation oder Ihrem Dateiserver zu sichern und die Kopien auf dem IBM Spectrum Protect-Server zu speichern. Sie können diese Kopien wiederherstellen, wenn die Originale beschädigt sind oder verloren gehen. Abhängig von den Gründen für das Sichern von Daten können Sie die Daten entweder sichern oder archivieren.

Dieses Release enthält keine aktualisierte Version der Clientkomponente für Sichern/Archivieren. Die Dokumentation für den Client für Sichern/Archivieren finden Sie unter frühere Releases.

## Anwendungsprogrammierschnittstelle

Die Anwendungsprogrammierschnittstelle (API) von IBM Spectrum Protect ist in dem Paket mit dem IBM Spectrum Protect-Client für Sichern/Archivieren enthalten. Mit der API können Sie Geschäftsanwendungen wie z. B. Datenbanken in der IBM Spectrum Protect-Umgebung schützen.

Dieses Release enthält keine aktualisierte Version der API-Komponente. Die API-Dokumentation finden Sie unter frühere Releases.

## Leistung

Viele Faktoren beeinflussen die Leistung des Servers und der Clients, einschließlich Betriebssysteme, Systemhardware, Netzkonfigurationen, Speichereinheitentypen sowie Größe und Anzahl der Clientdateien. Die Interaktionen zwischen diesen Faktoren können eine komplexe Leistungsoptimierung zur Folge haben.

Dieses Release enthält keine aktualisierte Version der Leistungskomponente. Die Leistungsdokumentation finden Sie unter Version 8.1.0.


## Fehlerbehebung

Fehlerbehebungsprozeduren für die Problemdiagnose und Problemlösung sind verfügbar.

Dieses Release enthält keine aktualisierte Version der Fehlerbehebungskomponente. Die Dokumentation für die Fehlerbehebung finden Sie unter Version 8.1.0.

## Nachrichten, Rückkehrcodes und Fehlercodes

Erläuterungen und vorgeschlagene Aktionen sind für Nachrichten verfügbar, die von IBM Spectrum Protect-Komponenten ausgegeben werden.

- Einführung in Nachrichten
- ANS-Nachrichten 0000-9999
- API-Rückkehrcodes
- Rückkehrcodes für IBM Global Security Kit  
Der Server und Client verwenden das IBM Global Security Kit (GSKit) für die SSL-Verarbeitung (SSL - Secure Sockets Layer) zwischen dem Server und dem Client für Sichern/Archivieren. Einige Nachrichten, die für die SSL-Verarbeitung ausgegeben werden, enthalten GSKit-Rückkehrcodes.
- ANE: Auf dem Server protokollierte Clientereignisse
- ANR: Allgemeine und plattformspezifische Servernachrichten
- E/A-Fehlercodebeschreibungen in Servernachrichten
- Einheitenfehlercodes im AIX-Systemfehlerprotokoll
-  Fehlerbehebung (Version 8.1.0 ist die neueste Veröffentlichung)

## Einführung in Nachrichten

Nachrichten, Fehlercodes und Rückkehrcodes werden von den IBM Spectrum Protect-Servern und -Clients ausgegeben.

Nachrichten und Codes können an der Serverkonsole, im Verwaltungsclient, an der Datenstation des Bedieners, in der grafischen Benutzerschnittstelle des Verwaltungsclients, im Client für Sichern/Archivieren oder im Client für hierarchische Speicherverwaltung (HSM-Client) angezeigt werden.


IBM Spectrum Protect stellt ein Aktivitätenprotokoll zur Verfügung, das dem Administrator helfen soll, Serveraktivitäten zu verfolgen und das System zu überwachen. Das Aktivitätenprotokoll enthält Nachrichten, die vom Server generiert wurden, und ist in der Datenbank gespeichert. Der Server löscht automatisch Nachrichten aus dem Aktivitätenprotokoll, die die angegebene Aufbewahrungszeit überschritten haben. Alle Nachrichten, die an die Serverkonsole gesendet wurden, werden im Aktivitätenprotokoll gespeichert. Beispiele für die Arten von Nachrichten, die im Aktivitätenprotokoll gespeichert werden, sind:

- Start oder Ende von Clientsitzungen
- Start oder Ende von Umlagerungen
- Verfall gesicherter Dateien im Serverspeicher
- Alle Ausgaben, die von Hintergrundprozessen generiert werden

Einige Nachrichten haben keine Erläuterungen und werden nicht veröffentlicht. Der Client kann Statistiken an den Server senden, um Informationen zu einer Sicherungs- oder Zurückschreibungsoperation zur Verfügung zu stellen. Diese Statistiken sind Informationsnachrichten, die für die verschiedenen Ereignisprotokollempfänger aktiviert oder inaktiviert werden können. Diese Nachrichten werden nicht veröffentlicht.

- Format der IBM Spectrum Protect-Server- und -Clientnachrichten
- Rückkehrcodenachrichten interpretieren

### Zugehörige Tasks:

-  Aktivitätenprotokoll verwenden (Version 7.1.1)

## Format der IBM Spectrum Protect-Server- und -Clientnachrichten

IBM Spectrum Protect-Server- und -Clientnachrichten bestehen aus den folgenden Elementen:

- Einem Präfix mit drei Buchstaben. Nachrichten haben verschiedene Präfixe, mit denen Sie die IBM Spectrum Protect-Komponente identifizieren können, die die Nachricht ausgibt. Alle Nachrichten für eine Komponente haben normalerweise dasselbe Präfix. Manchmal gibt eine Komponente Nachrichten mit zwei oder drei verschiedenen Präfixen aus.

Beispielsweise geben Clients für Sichern/Archivieren Nachrichten mit dem Präfix ANS aus. Ereignisse des Clients für Sichern/Archivieren, die auf dem Server protokolliert werden, haben das Präfix ANE. Allgemeine und plattformspezifische Nachrichten des Servers haben das Präfix ANR.

- Einer numerischen Nachricht-ID.
- Einem Bewertungscode mit einem Buchstaben. Die folgenden Codes geben die Bewertung der Aktion an, die die Nachricht generiert hat:

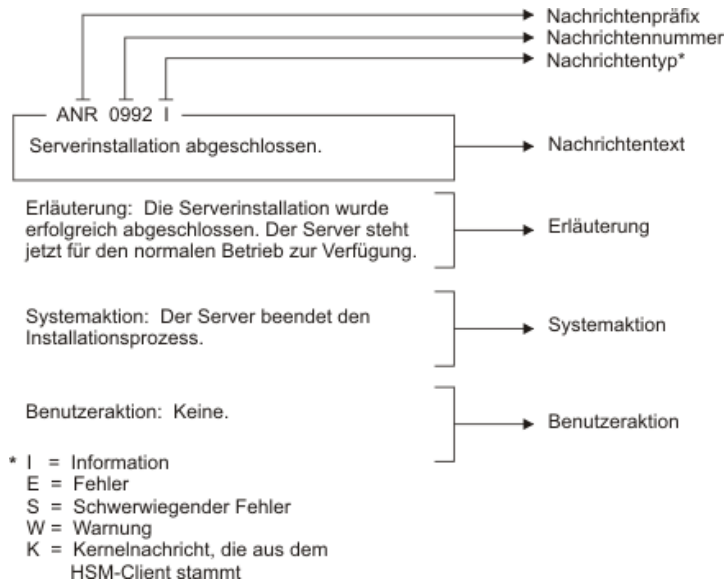
| Code | Bewertung     | Bedeutung   |
|------|---------------|---|
| S    | Schwerwiegend | Das Produkt oder eine Produktfunktion kann nicht fortgesetzt werden. Eine Benutzeraktion ist erforderlich.                                  |
| E    | Fehler        | Bei der Verarbeitung ist ein Fehler aufgetreten. Die Verarbeitung wird möglicherweise gestoppt. Eine Benutzeraktion kann erforderlich sein. |

| Code | Bewertung   | Bedeutung  |
|------|-------------|--|
| W    | Warnung     | Die Verarbeitung wird fortgesetzt, aber es können zu einem späteren Zeitpunkt aufgrund der Warnung Probleme auftreten. |
| I    | Information | Die Verarbeitung wird fortgesetzt. Es ist keine Benutzeraktion erforderlich.   |

- Nachrichtentext, der angezeigt und in Nachrichtenprotokolle geschrieben wird.
- Erläuterung, Systemaktion und Benutzeraktion. In diesen Texten wird der Nachrichtentext näher erläutert. Die Texte sind in den Nachrichtenhandbüchern des Produkts und in der Befehlszeilenhilfe verfügbar.

Die folgende Abbildung zeigt eine typische IBM Spectrum Protect-Servernachricht.

Die Beschriftungen geben jedes Element der Nachricht an.



Nachrichtenvariablen im Nachrichtentext werden kursiv angezeigt.

## Rückkehrcodenachrichten interpretieren

Viele verschiedene Befehle können denselben *Rückkehrcode* generieren. Die folgenden Beispiele zeigen zwei verschiedene Befehle, die ausgegeben wurden und denselben Rückkehrcode zur Folge haben; daher muss die *beschreibende Nachricht* für den Befehl gelesen werden.

In diesen Beispielen haben zwei verschiedene Befehle denselben Rückkehrcode zur Folge, aber sie geben auch beschreibende Nachrichten zurück, die für jeden Befehl eindeutig sind. Die beiden Befehle sind `q event standard dddd` und `def vol cstg05 primary`. Beide haben eine generische Nachricht mit diesem Rückkehrcode zur Folge:

ANS5102I: Rückkehrcode 11.

Der erste Befehl gibt jedoch auch eine beschreibende Nachricht zurück:

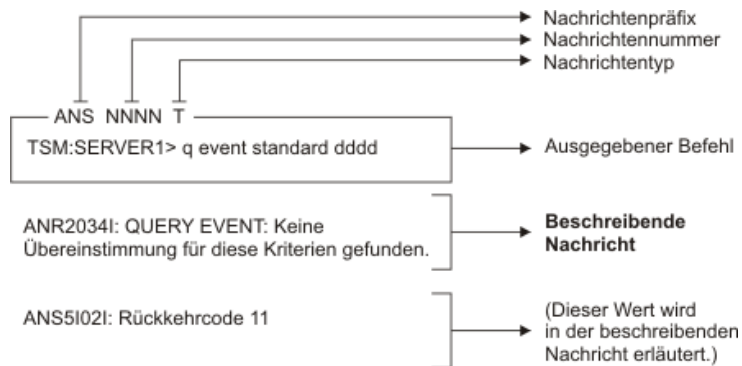
ANR2034I: QUERY EVENT: Keine Übereinstimmung für diese Abfrage gefunden.

Der zweite Befehl gibt ebenfalls eine eindeutige beschreibende Nachricht zurück:

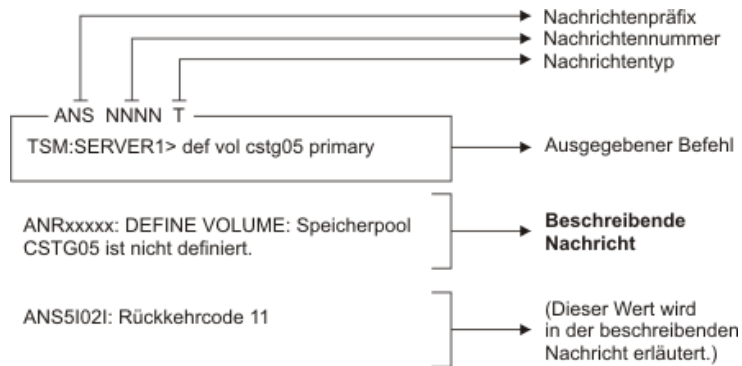
ANRxxxx: DEFINE VOLUME: Speicherpool CSTG05 ist nicht definiert.

- Erstes Beispiel für den Befehl QUERY EVENT
- Zweites Beispiel für den Befehl DEFINE VOLUME

## Erstes Beispiel für den Befehl QUERY EVENT



## Zweites Beispiel für den Befehl DEFINE VOLUME



## ANE-Nachrichten

ANE-Nachrichten werden vom Server ausgegeben. Alle Nachrichten mit dem Präfix ANE sind Clientereignisse, die auf dem Server protokolliert werden.

- Liste der ANE-Nachrichten

## ANR-Nachrichten

ANR-Nachrichten werden vom Server ausgegeben. Einige ANR-Nachrichten gelten für alle Betriebssysteme, andere gelten nur für ein einzelnes Betriebssystem.

- Liste der ANR-Nachrichten

## ANS-Nachrichten 0000-9999

Dieses Release enthält keine aktualisierten Nachrichten mit dem Präfix ANS. Die Dokumentation für die Nachrichten mit dem Präfix ANS finden Sie unter andere Releases von IBM Spectrum Protect.

## API-Rückkehrcodes

Dieses Release enthält keine aktualisierten Rückkehrcodes der Anwendungsprogrammierschnittstelle (API). Die Dokumentation für API-Rückkehrcodes finden Sie unter andere Releases von IBM Spectrum Protect.

## Beschreibungen der E/A-Codes in Servernachrichten

IBM Spectrum Protect-Nachrichten können Ein-/Ausgabecodes (E/A-Codes) enthalten. Die Codes können Operationscodes, Beendigungscodes, ASC-Codes (ASC = Additional Sense Codes) und ASCQ-Codes (ASCQ = Additional Sense Code Qualifier) sein.

Codebeschreibungen für E/A-Fehlernachrichten des IBM Spectrum Protect-Servers werden für alle unterstützten Betriebssysteme bereitgestellt.

### Code



## Beschreibung

OP

Fehlgeschlagene E/A-Operation. Diese Werte können angezeigt werden:

- READ
- WRITE
- FSR (Speicherbereichssatz weiterleiten)
- RSR (Speicherbereichssatz zurücknehmen)
- FSF (Speicherbereichsdatei weiterleiten)
- RSF (Speicherbereichsdatei zurücknehmen)
- WEOF (Dateiendemarkierung schreiben)
- OFFL (Band zurückspulen und entnehmen)
- FLUSH (Flushoperation ausführen)
- GET\_MEDIUM\_INFO (Datenträgerinformationen abrufen)
- LOCATE (lokalisieren)
- QRYLBP (Schutz logischer Blöcke abfragen)
- RDBLKID (Block-ID lesen)
- SETLBP (Schutz logischer Blöcke definieren)
- SETMODE (Modus definieren)
- REW (zurückspulen)
- SPACEEOD (Datenende des Speicherbereichs)
- TESTREADY (Testlaufwerk bereit)

CC

E/A-Beendigungscode. Dieser Wert wird von dem Einheitentreiber an den Server zurückgegeben, wenn ein Fehler auftritt. Eine Liste der BeendigungsCodes finden Sie in Übersicht über die Werte der BeendigungsCodes und Operationscodes. Informationen zu Bandarchivsystemaufrufen und Fehlerbeschreibungen für die Speicherarchiv-E/A-Steuerungsanforderungen finden Sie in Technote S7002972.

KEY

Byte 2 der Prüfbyte des Fehlers. Nachfolgend sind einige Definitionen aufgelistet:

- 0 = keine weiteren Prüfbyte verfügbar
- 1 = behobener Fehler
- 2 = nicht bereit
- 3 = Datenträgerfehler
- 4 = Hardwarefehler
- 5 = falsche Anforderung
- 6 = Einheitenabruf (zum Beispiel Zurücksetzen eines SCSI-Busses)
- 7 = Datenschutz
- 8 = Leerprüfung
- 9 = lieferantenspezifisch
- A = Kopieroperation abgebrochen
- B = abgebrochener Befehl
- C = veraltet
- D = Datenträgerüberlauf
- E = fehlende Übereinstimmung
- F = reserviert

ASC/ASCQ

ASC- und ASCQ-Codes sind die Byte 12 und 13 der Prüfbyte. Das mit der Einheit zur Verfügung gestellte Referenzhandbuch zum Laufwerk oder Kassettenarchiv enthält Tabellen, die die Werte der Felder KEY, ASC und ASCQ erläutern. Der Abschnitt Beschreibungen der ASC- und ASCQ-Standardcodes stellt weitere Informationen zu den Standardwerten der ASC- und ASCQ-Codes bereit.

Fehlercodes des Betriebssystems

Wenn ein Befehl fehlschlägt, gibt das Betriebssystem eine Fehlernummer zurück. Um die Bedeutung der Fehlercodes zu bestimmen, führen Sie die folgende Aktion aus:

- Rufen Sie auf den Plattformen AIX, HP-UX und Solaris die Datei `errno.h` im Verzeichnis `/usr/include/sys` auf. Diese Datei stellt Definitionen der Fehlercodes bereit.
- Rufen Sie auf Linux-Plattformen die Dateien `errno-base.h` und `errno.h` im Verzeichnis `/usr/include/asm-generic` auf. Diese Dateien stellen Definitionen für Codes bereit.
- Wenden Sie sich auf Windows-Plattformen zwecks Unterstützung bei den Fehlernachrichten an den Microsoft Support.
- Übersicht über die Werte der BeendigungsCodes und Operationscodes  
IBM Spectrum Protect-Nachrichten können BeendigungsCodes von den Einheitentribern enthalten.

- Beschreibungen der ASC- und ASCQ-Standardcodes  
ASC- und ASCQ-Standardcodes werden beschrieben.

## Übersicht über die Werte der Beendigungs- und Operationscodes

IBM Spectrum Protect-Nachrichten können Beendigungs- und Operationscodes von den Einheitentreibern enthalten.

- Beendigungs- und Operationscodes für Einheitentreiber: Allgemeine Codes  
IBM Spectrum Protect-Einheitentreiber stellen Beendigungs- und Operationscodes bereit, die für alle Einheitenklassen gelten.
- Beendigungs- und Operationscodes für Einheitentreiber: Datenträgerwechsler  
IBM Spectrum Protect-Einheitentreiber stellen Beendigungs- und Operationscodes bereit, die für bestimmte Datenträgerwechseleinheiten gelten.
- Beendigungs- und Operationscodes für Einheitentreiber: Bandlaufwerke  
IBM Spectrum Protect-Einheitentreiber stellen Beendigungs- und Operationscodes bereit, die für bestimmte Bandlaufwerke gelten.

## Beendigungs- und Operationscodes für Einheitentreiber: Allgemeine Codes

IBM Spectrum Protect-Einheitentreiber stellen Beendigungs- und Operationscodes bereit, die für alle Einheitenklassen gelten.

Die folgende Tabelle enthält allgemeine Beendigungs- und Operationscodewerte für IBM Spectrum Protect-Einheitentreiber. Jeder Eintrag stellt eine Beschreibung für die E/A-Fehlernachricht und die empfohlene Aktion zur Verfügung. Wiederholen Sie nach der Ausführung der empfohlenen Aktion die fehlgeschlagene Operation.

Tabelle 1. Beendigungs- und Operationscodewerte, die auf alle Einheitenklassen zutreffen

| Dezimal | Hexadezimal | Beschreibung  | Empfohlene Aktion   |
|---------|-------------|---|---|
| 200     | X'CB'       | Die Einheit hat eine Fehlerbedingung angezeigt, Prüfdaten waren jedoch nicht verfügbar. | Die fehlgeschlagene Operation wiederholen.  |
| 201     | X'CC'       | Der Einheitentreiber ist fehlgeschlagen.  | Den IBM Spectrum Protect Support verständigen.  |
| 202     | X'CA'       | Die Einheit EEPROM ist fehlgeschlagen.  | Die Einheit testen. Bei Bedarf die Einheit warten.  |
| 203     | X'CB'       | Manueller Eingriff ist erforderlich.  | Den Fehler an der Einheit beheben. Bei dem Problem kann es sich um ein steckengebliebenes Band, verschmutzte Plattenköpfe oder einen eingeklemmten Plattenzugriffssarm handeln.   |
| 204     | X'CC'       | Das System wurde nach einem E/A-Fehler wiederhergestellt; nur zu Informationszwecken.   | Keine Aktion erforderlich.  |
| 205     | X'CD'       | Der SCSI-Adapter ist fehlgeschlagen.  | Auf lose Kabel, verbogene Kontaktstifte, falsche Kabel, falsche SCSI-Adapter, nicht ordnungsgemäße Abschlüsse oder falsche Abschlussstecker überprüfen.   |
| 206     | X'CE'       | Ein allgemeiner SCSI-Fehler ist aufgetreten.  | Auf lose Kabel, verbogene Kontaktstifte, falsche Kabel, falsche SCSI-Adapter, nicht ordnungsgemäße Abschlüsse oder falsche Abschlussstecker überprüfen.   |
| 207     | X'CF'       | Die Einheit kann die angeforderte Aktion nicht ausführen.                               | Sicherstellen, dass die Einheit eingeschaltet und bereit ist. Stellen Sie sicher, dass das Laufwerk mit dem Befehl DEFINE DRIVE korrekt definiert wurde. Stellen Sie sicher, dass die Einheitenklasse mit dem Befehl DEFINE DEVCLASS korrekt definiert wurde. |
| 208     | X'D0'       | Der Befehl wurde gestoppt.  | Den IBM Spectrum Protect Support verständigen.  |
| 209     | X'D1'       | Im Mikrocode der Einheit wurde ein Fehler gefunden.                                     | Die Mikrocodeversion des Laufwerks überprüfen. Den Hersteller des Laufwerks benachrichtigen und die neueste Version anfordern.  |

| Dezimal | Hexadezimal | Beschreibung  | Empfohlene Aktion  |
|---------|-------------|---|--|
| 210     | X'D2'       | Die Einheit wurde aufgrund des Einschaltens, der SCSI-Buszurücksetzung oder des manuellen Ladens/Entladens von Bändern zurückgesetzt. | Die fehlgeschlagene Operation wiederholen.   |
| 211     | X'D3'       | Der SCSI-Bus ist aktiv.   | Sicherstellen, dass die SCSI-IDs der korrekten Einheit richtig zugeordnet wurden und auf die Einheit nicht durch einen anderen Prozess zugegriffen wird. |
| 212     | X'D4'       | Persistente Reservierung wird auf dieser Einheit nicht unterstützt.   | Keine Aktion erforderlich.   |
| 213     | X'D5'       | Eine Operation für persistente Reservierung ist fehlgeschlagen.   | Die Einheit zurücksetzen und die Operation wiederholen. Bleibt der Fehler bestehen, den IBM Spectrum Protect Support verständigen.                       |

## Beendigungscode für Einheitentreiber: Datenträgerwechsler

IBM Spectrum Protect-Einheitentreiber stellen Beendigungscode bereit, die für bestimmte Datenträgerwechseleinheiten gelten.

Die folgende Tabelle enthält Beendigungscodewerte für IBM Spectrum Protect-Einheitentreiber für Datenträgerwechsler. Jeder Eintrag stellt eine Beschreibung für die E/A-Fehlernachricht und die empfohlene Aktion zur Verfügung. Wiederholen Sie nach der Ausführung der empfohlenen Aktion die fehlgeschlagene Operation.

Tabelle 1. Beendigungscodewerte für Datenträgerwechsler

| Dezimal | Hexadezimal | Beschreibung                                | Empfohlene Aktion  |
|---------|-------------|---|--|
| 300     | X'12C'      | Kassetten-Eingangs/Ausgangsfehler           | Den Eingang/Ausgang auf einen eingeklemmten Datenträger überprüfen.  |
| 301     | X'12D'      | Kassettenladefehler                         | Das Laufwerk auf eingeklemmte Datenträger überprüfen. Unter AIX den errpt zum Überprüfen auf Hardwarefehler anzeigen.                  |
| 302     | X'12E'      | Kassette in fehlerhaftem Laufwerk           | Das Laufwerk auf eingeklemmte Datenträger überprüfen. Unter AIX den errpt zum Überprüfen auf Hardwarefehler anzeigen.                  |
| 303     | X'12F'      | Karussell nicht geladen                     | Sicherstellen, dass das Karussell korrekt positioniert und die Tür geschlossen ist.  |
| 304     | X'130'      | Wechslerfehler                              | Unter AIX den errpt zum Überprüfen auf Hardwarefehler anzeigen.  |
| 305     | X'131'      | Laufwerkfehler                              | Sicherstellen, dass die Köpfe sauber sind. Unter AIX den errpt zum Überprüfen auf Hardwarefehler anzeigen.                             |
| 306     | X'132'      | Laufwerk- oder Datenträgerfehler            | Sicherstellen, dass die Köpfe sauber sind. Unter AIX den errpt zum Überprüfen auf Hardwarefehler anzeigen.                             |
| 307     | X'133'      | Eingangs-/Ausgangsfehler                    | Die Bandarchivschnittstelle auf Hardwarefehler überprüfen. Sind keine Fehler vorhanden, den IBM Spectrum Protect Support verständigen. |
| 308     | X'134'      | Eingangs-/Ausgangsanschluss nicht vorhanden | Die Bandarchivschnittstelle auf Hardwarefehler überprüfen. Sind keine Fehler vorhanden, den IBM Spectrum Protect Support verständigen. |

| Dezimal | Hexadezimal | Beschreibung   | Empfohlene Aktion  |
|---------|-------------|--|--|
| 309     | X'135'      | Kassettenarchivprüffehler  | Sicherstellen, dass keine Datenträger eingeklemmt sind. Es ist möglich, dass die Kassettenarchivprüfung aufgrund von Hardwarefehlern fehlschlägt. Unter AIX den errpt zum Überprüfen auf Hardwarefehler anzeigen.                            |
| 310     | X'136'      | Kassettenarchiv voll   | Auf eingeklemmte Datenträger überprüfen. Sicherstellen, dass die Datenträger nicht neu angeordnet werden. Ist das Kassettenarchiv nicht voll, den Befehl AUDIT LIBRARY starten.  |
| 311     | X'137'      | Datenträgerexport  | Die Bandarchivschnittstelle auf Hardwarefehler überprüfen. Sind keine Fehler vorhanden, den IBM Spectrum Protect Support verständigen.   |
| 312     | jX'138'     | Schachtfehler  | Sicherstellen, dass in dem Schacht nichts eingeklemmt ist.   |
| 313     | X'139'      | Schacht- oder Datenträgerfehler  | Sicherstellen, dass der Datenträger in dem Schacht nicht eingeklemmt ist und die Datenträger nicht neu angeordnet werden. Bleibt der Fehler bestehen, den Befehl AUDIT LIBRARY starten.  |
| 314     | X'13A'      | Quellenschacht oder -laufwerk waren bei Versuch leer, Datenträger zu versetzen | Sicherstellen, dass die Datenträger nicht neu angeordnet werden. Bleibt der Fehler bestehen, den Befehl AUDIT LIBRARY starten.   |
| 315     | X'13B'      | Zielschacht oder -laufwerk waren bei Versuch leer, Datenträger zu versetzen    | Sicherstellen, dass die Datenträger nicht neu angeordnet werden und dass kein Datenträger in dem Laufwerk eingeklemmt ist. Bleibt der Fehler bestehen, den Befehl AUDIT LIBRARY starten.   |
| 316     | X'13C'      | Reinigungskassette installiert   | Den IBM Spectrum Protect Support verständigen.   |
| 317     | X'13D'      | Datenträger nicht ausgegeben   | Sicherstellen, dass die Datenträger nicht neu angeordnet werden und dass kein Datenträger in dem Laufwerk eingeklemmt ist. Bleibt der Fehler bestehen, den Befehl AUDIT LIBRARY starten.   |
| 318     | X'13E'      | E/A-Anschluss nicht konfiguriert   | Den IBM Spectrum Protect Support verständigen.   |
| 319     | X'13F'      | Erster Zielort ist leer  | Sicherstellen, dass die Datenträger nicht neu angeordnet werden. Bleibt der Fehler bestehen, den Befehl AUDIT LIBRARY starten.   |
| 320     | X'140'      | Keine Informationen zum Datenträgerbestand                                     | Den Befehl AUDIT LIBRARY starten.  |
| 321     | X'141'      | Abweichung beim Lesen des Elementstatus  | Stellen Sie sicher, dass die Hostbusadaptertreiber und die Firmware über aktuelle Versionen verfügen. Die Bandarchivschnittstelle auf Hardwarefehler überprüfen. Sind keine Fehler vorhanden, den IBM Spectrum Protect Support verständigen. |
| 322     | X'142'      | Bereichsinitialisierung fehlgeschlagen   | Die Bandarchivschnittstelle auf Hardwarefehler überprüfen. Sind keine Fehler vorhanden, den IBM Spectrum Protect Support verständigen.   |

## Beendigungscodes für Einheitentreiber: Bandlaufwerke

IBM Spectrum Protect-Einheitentreiber stellen Beendigungscodes bereit, die für bestimmte Bandlaufwerke gelten.

Die folgende Tabelle enthält Beendigungscodewerte für IBM Spectrum Protect-Einheitentreiber für Bandlaufwerke. Jeder Eintrag stellt eine Beschreibung für die E/A-Fehlernachricht und die empfohlene Aktion zur Verfügung. Wiederholen Sie nach der Ausführung der empfohlenen Aktion die fehlgeschlagene Operation.

Tabelle 1. Beendigungscodewerte für Bandlaufwerke

| Dezimal | Hexadezimal | Beschreibung   | Empfohlene Aktion  |
|---------|-------------|--|--|
| 400     | X'190'      | Physisches Ende des Datenträgers erkannt                 | Sicherstellen, dass die Köpfe im Laufwerk sauber sind.   |
| 401     | X'191'      | Datenende erkannt  | Den IBM Spectrum Protect Support verständigen.   |
| 402     | X'192'      | Datenträger beschädigt                                   | Sicherstellen, dass die Köpfe sauber sind. Stellen Sie sicher, dass der Datenträger nicht physisch beschädigt ist und nicht das Ende des Lebenszyklus erreicht hat, das vom Hersteller des Datenträgers angegeben wurde. |
| 403     | X'193'      | Datenträgerfehler  | Sicherstellen, dass die Köpfe sauber sind. Stellen Sie sicher, dass der Datenträger nicht physisch beschädigt ist und nicht das Ende des Lebenszyklus erreicht hat, das vom Hersteller des Datenträgers angegeben wurde. |
| 404     | X'194'      | Datenträgerinkompatibilität                              | Sicherstellen, dass die korrekte Länge und der korrekte Typ des Datenträgers verwendet wird.   |
| 406     | X'196'      | Angeforderter Sektor ist ungültig                        | Interner Serverfehler. Den IBM Spectrum Protect Support verständigen.  |
| 407     | X'197'      | Schreibgeschützt   | Sicherstellen, dass der Datenträger nicht schreibgeschützt ist.  |
| 408     | X'198'      | Datenträger und Laufwerk reinigen                        | Die Laufwerkköpfe mit einer Reinigungskassette reinigen.   |
| 409     | X'199'      | Datenträgerfehler  | Sicherstellen, dass die Köpfe sauber sind. Stellen Sie sicher, dass der Datenträger nicht physisch beschädigt ist und nicht das Ende des Lebenszyklus erreicht hat, das vom Hersteller des Datenträgers angegeben wurde. |
| 410     | X'19A'      | Reinigung beendet  | Die fehlgeschlagene Operation wiederholen.   |
| 411     | X'19B'      | Logisches Datenträgerende festgestellt                   | Den IBM Spectrum Protect Support verständigen.   |
| 412     | X'19C'      | Datenträger in Laufwerk nicht vorhanden                  | Sicherstellen, dass der Datenträger im Laufwerk korrekt positioniert ist. Bleibt der Fehler bestehen, den Befehl AUDIT LIBRARY starten.  |
| 413     | X'19D'      | Anfang des Datenträgers festgestellt                     | Den IBM Spectrum Protect Support verständigen.   |
| 414     | X'19E'      | Fehler beim Löschen                                      | Die Laufwerkköpfe reinigen.  |
| 415     | X'19F'      | Versuch, beschriebenen WORM-Datenträger zu überschreiben | Interner Serverfehler. Den IBM Spectrum Protect Support verständigen.  |
| 416     | X'1A0'      | Block mit falscher Länge gelesen.                        | Sicherstellen, dass die Köpfe sauber sind. Unter AIX den errpt zum Überprüfen auf Hardwarefehler anzeigen.   |
| 417     | X'1A1'      | Nur zum Lesen öffnen                                     | Den IBM Spectrum Protect Support verständigen.   |
| 418     | X'1A2'      | Nur zum Schreiben öffnen                                 | Den IBM Spectrum Protect Support verständigen.   |
| 419     | X'1A2'      | Durchsuchen des Datenträgers fehlgeschlagen              | Das Laufwerk und den Datenträger reinigen.   |

| Dezimal | Hexadezimal | Beschreibung  | Empfohlene Aktion  |
|---------|-------------|---|--|
| 420     | X'1A4'      | Kein logischer Schreibzugriff   | Sicherstellen, dass die Köpfe sauber sind. Die Fehlerprotokolle des Betriebssystems auf Hardwarefehler überprüfen. Sicherstellen, dass der Schreibschutzschalter auf 'Off' gesetzt ist. Die SAN-Bandbeschleunigung inaktivieren oder CHECKTAPEPOS auf OFF oder TSMonly setzen. |
| 422     | X'1A6'      | Reinigung ist erforderlich  | Das Bandlaufwerk reinigen.   |
| 423     | X'1A7'      | Datenträgerfehler   | Die Fehlerprotokolle des Betriebssystems auf Hardwarefehler überprüfen. Überprüfen, ob fehlerhafte Datenträger vorhanden sind.   |
| 424     | X'1A8'      | Mit der Verschlüsselung zusammenhängender Fehler ist aufgetreten              | Überprüfen Sie Ihre Verschlüsselungseinstellung für Ihre Einheitenklasse und Ihr Bandlaufwerk.   |
| 425     | X'1A9'      | Mit der Entschlüsselung zusammenhängender Fehler ist aufgetreten              | Überprüfen Sie Ihre Verschlüsselungseinstellung für Ihre Einheitenklasse und Ihr Bandlaufwerk.   |
| 425     | X'1AA'      | Ein externer mit der Verschlüsselung zusammenhängender Fehler ist aufgetreten | Überprüfen Sie die Verschlüsselungseinstellung für Ihre Einheitenklasse und Ihr Bandlaufwerk.  |
| 426     | X'1AB'      | Eine CRC-Abweichung ist aufgetreten   | Stellen Sie sicher, dass der Datenträger nicht das Ende des Lebenszyklus erreicht hat, das vom Hersteller des Datenträgers angegeben wurde. Wiederholen Sie die Operation.   |

## Beschreibungen der ASC- und ASCQ-Standardcodes

ASC- und ASCQ-Standardcodes werden beschrieben.

Die ASC- und ASCQ-Codes sind die Byte 12 und 13 für SCSI-2-Einheiten. Auf Windows-Systemen werden diese Codes im Windows-Ereignisprotokoll angezeigt, aber die Informationen zeigen andere Byte.

Die Servernachricht ANR8300E oder ANR8302E gibt die empfohlene Aktion an.

Die folgende Tabelle enthält Standardbeschreibungen für einige ASC- und ASCQ-Codes. Jeder Wert hat das Präfix 0x, das angibt, dass es sich um eine Hexadezimalkonstante handelt. Beachten Sie, dass die Beschreibungen unter Einheiten variieren. Eine genaue Beschreibung der ASC- und ASCQ-Codes für eine bestimmte Einheit enthält die mit der Einheit bereitgestellte Dokumentation.

Tabelle 1. Beschreibungen der ASC- und ASCQ-Standardcodes

| ASC  | ASCQ | Beschreibung                   |
|------|------|--------------------------------|
| 0x00 | 0x00 | Keine weiteren Prüfcodes       |
| 0x00 | 0x01 | Dateimarkierung erkannt        |
| 0x00 | 0x02 | Datenträgerende erkannt        |
| 0x00 | 0x03 | Gruppenmarkierung erkannt      |
| 0x00 | 0x04 | Datenträgeranfang              |
| 0x00 | 0x05 | Datenende                      |
| 0x00 | 0x06 | E/A-Prozess beendet            |
| 0x02 | 0x00 | Kein Suchvorgang abgeschlossen |
| 0x03 | 0x00 | Einheitenschreibfehler         |
| 0x03 | 0x01 | Kein aktueller Schreibvorgang  |
| 0x03 | 0x02 | Zu viele Schreibfehler         |
| 0x04 | 0x00 | Logische Einheit nicht bereit  |
| 0x04 | 0x01 | Wird in Bereitschaft gesetzt   |

| <b>ASC</b> | <b>ASCQ</b> | <b>Beschreibung</b>                                    |
|------------|-------------|--|
| 0x04       | 0x02        | Nicht bereit, Initialisierung des Befehls erforderlich |
| 0x04       | 0x03        | Nicht bereit, manueller Eingriff erforderlich          |
| 0x04       | 0x04        | Nicht bereit, Formatierung läuft                       |
| 0x05       | 0x00        | Keine auszuwählende Antwort                            |
| 0x06       | 0x00        | Keine Referenzposition gefunden                        |
| 0x07       | 0x00        | Mehrere Einheiten ausgewählt                           |
| 0x08       | 0x00        | Übertragungsfehler                                     |
| 0x08       | 0x01        | Zeitlimitüberschreitung bei Übertragung                |
| 0x08       | 0x02        | Übertragungsparitätsfehler                             |
| 0x09       | 0x00        | Fehlerverfolgung                                       |
| 0x0A       | 0x00        | Fehlerprotokollüberlauf                                |
| 0x0C       | 0x00        | Schreibfehler  |
| 0x11       | 0x00        | Nicht behobener Lesefehler                             |
| 0x11       | 0x01        | Wiederholungslimit für Lesen erreicht                  |
| 0x11       | 0x02        | Fehler zum Korrigieren zu lang                         |
| 0x11       | 0x03        | Mehrere Lesefehler                                     |
| 0x11       | 0x08        | Unvollständiges Lesen des Blocks                       |
| 0x11       | 0x09        | Kein Abstand gefunden                                  |
| 0x11       | 0x0A        | Falsch korrigierter Fehler                             |
| 0x14       | 0x00        | Aufgezeichnete Entität nicht gefunden                  |
| 0x14       | 0x01        | Satz nicht gefunden                                    |
| 0x14       | 0x02        | Dateimarkierung/Gruppenmarkierung nicht gefunden       |
| 0x14       | 0x03        | Datenende nicht gefunden                               |
| 0x14       | 0x04        | Blockfolgefehler                                       |
| 0x15       | 0x00        | Fehler bei wahlfreier Positionierung                   |
| 0x15       | 0x01        | Mechanischer Positionierungsfehler                     |
| 0x15       | 0x02        | Lesepositionierungsfehler                              |
| 0x17       | 0x00        | Keine Fehlerkorrektur angewendet                       |
| 0x17       | 0x01        | Mit Wiederholungen wiederhergestellt                   |
| 0x17       | 0x02        | Mit positiver Kopfkorrektur wiederhergestellt          |
| 0x17       | 0x03        | Mit negativer Kopfkorrektur wiederhergestellt          |
| 0x18       | 0x00        | ECC angewendet   |
| 0x1A       | 0x00        | Längenfehler bei Parameterliste                        |
| 0x1B       | 0x00        | Fehler bei synchroner Datenübertragung                 |
| 0x20       | 0x00        | Ungültiger Operationscode                              |
| 0x21       | 0x00        | Block außerhalb des Bereichs                           |
| 0x21       | 0x01        | Ungültige Elementadresse                               |
| 0x24       | 0x00        | Ungültiges Feld in CDB                                 |
| 0x25       | 0x00        | LUN nicht unterstützt                                  |
| 0x26       | 00          | Ungültiges Feld in Parameterliste                      |
| 0x26       | 0x01        | Parameter nicht unterstützt                            |
| 0x26       | 0x02        | Parameterwert ungültig                                 |

| <b>ASC</b> | <b>ASCQ</b> | <b>Beschreibung</b>                         |
|------------|-------------|---|
| 0x26       | 0x03        | Schwellenparameter nicht unterstützt        |
| 0x27       | 0x00        | Schreibgeschützt                            |
| 0x28       | 0x00        | Nicht bereit zu bereit                      |
| 0x28       | 0x01        | Zugriff auf Import-/Exportelement           |
| 0x29       | 0x00        | Einschalten, zurücksetzen, Bus zurücksetzen |
| 0x2A       | 0x00        | Parameter geändert                          |
| 0x2A       | 0x01        | Modusparameter geändert                     |
| 0x2A       | 0x02        | Protokollparameter geändert                 |
| 0x2B       | 0x00        | Kopiervorgang kann nicht ausgeführt werden  |
| 0x2C       | 0x00        | Befehlsfolgefehler                          |
| 0x2D       | 0x00        | Überschreibungsfehler bei Aktualisierung    |
| 0x2F       | 0x00        | Befehl vom Initiator gelöscht               |
| 0x30       | 0x00        | Inkompatible Datenträger                    |
| 0x30       | 0x01        | Unbekanntes Format für Datenträger          |
| 0x30       | 0x02        | Inkompatibles Format für Datenträger        |
| 0x30       | 0x03        | Reinigungskassette installiert              |
| 0x31       | 0x00        | Datenträgerformat beschädigt                |
| 0x33       | 0x00        | Bandlängenfehler                            |
| 0x37       | 0x00        | Gerundeter Parameter                        |
| 0x39       | 0x00        | Sichern von Parametern nicht unterstützt    |
| 0x3A       | 0x00        | Datenträger nicht vorhanden                 |
| 0x3B       | 0x00        | Fehler bei sequentieller Positionierung     |
| 0x3B       | 0x01        | Positionierungsfehler bei BOT               |
| 0x3B       | 0x02        | Positionierungsfehler bei EOT               |
| 0x3B       | 0x08        | Neupositionierungsfehler                    |
| 0x3B       | 0x0D        | Datenträgerzielelement voll                 |
| 0x3B       | 0x0E        | Datenträgerquellenelement leer              |
| 0x3D       | 0x00        | Ungültige Bits in Nachricht                 |
| 0x3E       | 0x00        | LUN nicht selbstkonfiguriert                |
| 0x3F       | 0x00        | Betriebsbedingungen geändert                |
| 0x3F       | 0x01        | Mikrocode geändert                          |
| 0x3F       | 0x02        | Geänderte Betriebsdefinition                |
| 0x3F       | 0x03        | Abfragedaten geändert                       |
| 0x3F       | 0x0E        | Zurückgemeldete LUN-Daten geändert          |
| 0x43       | 0x00        | Nachrichtenfehler                           |
| 0x44       | 0x00        | Fehler bei internem Ziel                    |
| 0x45       | 0x00        | Fehler beim Auswählen/Erneuten Auswählen    |
| 0x46       | 0x00        | Nicht erfolgreicher Warmstart               |
| 0x47       | 0x00        | SCSI-Paritätsfehler                         |
| 0x48       | 0x00        | Initiator hat empfangene Nachricht erkannt  |
| 0x49       | 0x00        | Ungültige Nachricht                         |
| 0x4A       | 0x00        | Befehlsphasenfehler                         |



| ASC  | ASCQ | Beschreibung                                    |
|------|------|---|
| 0x4B | 0x00 | Datenphasenfehler                               |
| 0x4C | 0x00 | Fehlgeschlagene Selbstkonfiguration bei LUN     |
| 0x4E | 0x00 | Überlappte Befehle                              |
| 0x50 | 0x00 | Anfügefehler beim Schreiben                     |
| 0x50 | 0x01 | Anfügepositionsfehler beim Schreiben            |
| 0x50 | 0x02 | Positionsfehler (Ablaufsteuerung)               |
| 0x51 | 0x00 | Fehler beim Löschen                             |
| 0x52 | 0x00 | Kassettenfehler                                 |
| 0x53 | 0x00 | Laden/Entnehmen des Datenträgers fehlgeschlagen |
| 0x53 | 0x01 | Fehler beim Entnehmen des Bandes                |
| 0x53 | 0x02 | Datenträgerentnahme verhindert                  |
| 0x5A | 0x00 | Operatorstatus geändert                         |
| 0x5A | 0x01 | Datenträgerentnahme durch Operator              |
| 0x5A | 0x02 | Operator - kein Schreibzugriff                  |
| 0x5A | 0x03 | Operator - Schreibzugriff                       |
| 0x5B | 0x00 | Protokollausnahme                               |
| 0x5B | 0x01 | Schwellenbedingung erfüllt                      |
| 0x5B | 0x02 | Protokollzähler auf Maximum                     |
| 0x5B | 0x03 | Protokollistencodes erschöpft                   |

- ASC- und ASCQ-Codes im Windows-Ereignisprotokoll  
ASC- und ASCQ-Codes werden im Windows-Ereignisprotokoll angezeigt.

## Einheitenfehlercodes im AIX-Systemfehlerprotokoll

Einige Einheitenfehlercodes werden im AIX-Systemfehlerprotokoll protokolliert.

ADSM\_DD\_LOG1 (0xAC3AB953)  
DEVICE DRIVER SOFTWARE ERROR

Dieser Fehler wird vom IBM Spectrum Protect-Einheitentreiber protokolliert, wenn in der IBM Spectrum Protect-Einheitentreibersoftware ein Fehler vermutet wird. Gibt der IBM Spectrum Protect-Einheitentreiber einen SCSI-E/A-Befehl mit einem ungültigen Operationscode aus, schlägt der Befehl fehl und der Fehler wird mit dieser Kennung protokolliert. Melden Sie diesen Fehler sofort der IBM Spectrum Protect-Unterstützung.

**Detaildaten:** Prüfdaten

Die Prüfdaten enthalten Informationen, die die Fehlerursache bestimmen können. Melden Sie alle Daten in dem Fehlereintrag der IBM Spectrum Protect-Unterstützung.

ADSM\_DD\_LOG2 (0x5680E405)  
HARDWARE/COMMAND-ABORTED ERROR

Dieser Fehler wird vom IBM Spectrum Protect-Einheitentreiber protokolliert, wenn die Einheit einen Hardwarefehler oder Fehler beim Stoppen des Befehls als Antwort auf einen SCSI-E/A-Befehl meldet.

**Detaildaten:** Prüfdaten

Die Prüfdaten enthalten Informationen, mit denen die fehlerhafte Hardwarekomponente und die Fehlerursache bestimmt werden können. Ziehen Sie das SCSI-Spezifikationshandbuch der Einheit zu Rate, um die Prüfdaten für eine bestimmte Einheit zu interpretieren.

ADSM\_DD\_LOG3 (0x461B41DE)  
MEDIA ERROR

Dieser Fehler wird vom IBM Spectrum Protect-Einheitentreiber protokolliert, wenn ein SCSI-E/A-Befehl fehlschlägt, weil Datenträger beschädigt oder inkompatibel sind oder ein Laufwerk gereinigt werden muss.

**Detaildaten:** Prüfdaten

Die Prüfdaten enthalten Informationen, die die Fehlerursache bestimmen können. Ziehen Sie das SCSI-Spezifikationshandbuch der Einheit zu Rate, um die Prüfdaten für eine bestimmte Einheit zu interpretieren.

ADSM\_DD\_LOG4 (0x4225DB66)  
TARGET DEVICE GOT UNIT ATTENTION

Dieser Fehler wird vom IBM Spectrum Protect-Einheitentreiber protokolliert, nachdem bestimmte UNIT ATTENTION-Hinweise von einer Einheit empfangen wurden. UNIT ATTENTION-Hinweise dienen zur Information und geben normalerweise an, dass sich ein bestimmter Zustand der Einheit geändert hat. Dieser Fehler würde beispielsweise protokolliert, wenn die Tür einer Kassettenarchivereinheit geöffnet und dann geschlossen wurde. Durch Protokollieren dieses Ereignisses wird angegeben, dass die Aktivität stattgefunden hat und der Bestand im Kassettenarchiv möglicherweise geändert wurde.

**Detaildaten:** Prüfdaten

Die Prüfdaten enthalten Informationen, die die Ursache für die UNIT ATTENTION beschreiben. Ziehen Sie das SCSI-Spezifikationshandbuch der Einheit zu Rate, um die Prüfdaten für eine bestimmte Einheit zu interpretieren.

ADSM\_DD\_LOG5 (0xDAC55CE5)  
PERMANENT UNKNOWN ERROR

Dieser Fehler wird vom IBM Spectrum Protect-Einheitentreiber protokolliert, nachdem ein unbekannter Fehler von einer Einheit als Antwort auf einen SCSI-E/A-Befehl empfangen wurde. Bleibt der Fehler bestehen, müssen Sie die Mitarbeiter der IBM Spectrum Protect-Unterstützung benachrichtigen.

**Detaildaten:** Prüfdaten

Die Prüfdaten bestehen aus Informationen, die die Fehlerursache bestimmen können. Melden Sie alle Daten in dem Fehlereintrag der IBM Spectrum Protect-Unterstützung.

ADSM\_DD\_LOG6 (0xBC539B26)  
WARNING OR INFORMATIONAL MESSAGE FOR TARGET DEVICE

Dieser Fehler wird vom IBM Spectrum Protect-Einheitentreiber protokolliert, nachdem eine Warnung oder eine Informationsnachricht von einer Einheit als Antwort auf einen SCSI-E/A-Befehl empfangen wurde. Diese Informationsnachrichten müssen nicht notwendigerweise auf ein Problem hinweisen. Wird die Nachricht weiterhin angezeigt, müssen Sie die IBM Spectrum Protect-Unterstützung benachrichtigen.

**Detaildaten:** Prüfdaten

Die Prüfdaten bestehen aus Informationen, die die Ursache für die Nachricht angeben können. Melden Sie alle Daten in dem Eintrag der IBM Spectrum Protect-Unterstützung.

## Rückkehrcodes für IBM Global Security Kit

---

Der Server und Client verwenden das IBM Global Security Kit (GSKit) für die SSL-Verarbeitung (SSL - Secure Sockets Layer) zwischen dem Server und dem Client für Sichern/Archivieren. Einige Nachrichten, die für die SSL-Verarbeitung ausgegeben werden, enthalten GSKit-Rückkehrcodes.

GSKit wird während der IBM Spectrum Protect-Installation automatisch installiert oder aktualisiert und stellt die folgenden Bibliotheken bereit:

- GSKit SSL
- GSKit Key Management API
- IBM Crypto for C (ICC)

Mit dem Dienstprogramm 'tsmdiag' wird die auf Ihrem System installierte GSKit-Version zurückgemeldet. Sie können auch eine der folgenden Methoden verwenden:

- Geben Sie für Windows die folgenden Befehle aus:

```
regedit /e gskitinfo.txt "HKEY_LOCAL_MACHINE\software\ibm\gsk8\"  
notepad gskitinfo.txt
```

Vorsicht:

Sie können das Systemregistry beschädigen, wenn Sie 'regedit' nicht ordnungsgemäß verwenden.

- Geben Sie für den AIX-Server (64-Bit) den folgenden Befehl in der Befehlszeile aus: `gsk8ver_64`

Tabelle 1 enthält die GSKit SSL-Rückkehrcodes.

Der Server verwendet die GSKit Key Management API, um die Schlüsselmanagementdatenbank und die privaten und öffentlichen Schlüssel des Servers automatisch zu erstellen. Einige Nachrichten, die für diese Verarbeitung ausgegeben werden, können GSKit Key Management-Rückkehrcodes einschließen. Tabelle 2 enthält die Key Management-Rückkehrcodes.

Tabelle 1. Allgemeine Rückkehrcodes für IBM Global Security Kit SSL

| Rückkehrcode (hex) | Rückkehrcode (dezimal) | Konstante                          | Erläuterung  |
|--------------------|------------------------|------------------------------------|--|
| 0x00000000         | 0                      | GSK_OK                             | Die Task wurde erfolgreich ausgeführt. Wird von jedem Funktionsaufruf ausgegeben, der erfolgreich ausgeführt wird.   |
| 0x00000001         | 1                      | GSK_INVALID_HANDLE                 | Die Umgebungskennung oder SSL-Kennung ist nicht gültig. Die angegebene Kennung war nicht das Ergebnis eines erfolgreichen Funktionsaufrufs <code>open()</code> . |
| 0x00000002         | 2                      | GSK_API_NOT_AVAILABLE              | Die DLL-Datei wurde entladen und ist nicht verfügbar (tritt nur auf Microsoft Windows-Systemen auf).   |
| 0x00000003         | 3                      | GSK_INTERNAL_ERROR                 | Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.  |
| 0x00000004         | 4                      | GSK_INSUFFICIENT_STORAGE           | Für die Ausführung der Operation ist nicht genügend Speicher verfügbar.  |
| 0x00000005         | 5                      | GSK_INVALID_STATE                  | Die Kennung hat keinen gültigen Status für die Operation, z. B. bei zweimaliger Ausführung einer Operation <code>init()</code> für eine Kennung.                 |
| 0x00000006         | 6                      | GSK_KEY_LABEL_NOT_FOUND            | Der angegebene Schlüsselkennsatz wurde nicht in der Schlüsseldatei gefunden.   |
| 0x00000007         | 7                      | GSK_CERTIFICATE_NOT_AVAILABLE      | Zertifikat nicht vom Partner empfangen.  |
| 0x00000008         | 8                      | GSK_ERROR_CERT_VALIDATION          | Fehler bei der Zertifikatsvalidierung.   |
| 0x00000009         | 9                      | GSK_ERROR_CRYPTO                   | Fehler bei der Verarbeitung der Verschlüsselung.   |
| 0x0000000a         | 10                     | GSK_ERROR_ASN                      | Fehler bei der Validierung von ASN-Feldern im Zertifikat.  |
| 0x0000000b         | 11                     | GSK_ERROR_LDAP                     | Fehler beim Herstellen der Verbindung zur Benutzerregistry.  |
| 0x0000000c         | 12                     | GSK_ERROR_UNKNOWN_ERROR            | Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.  |
| 0x0000000d         | 13                     | GSK_INVALID_PARAMETER              | Ungültiger Parameter.  |
| 0x0000000e         | 14                     | GSK_ERROR_UNEXPECTED_INT_EXCEPTION | Ungültiger Parameter. Melden Sie diesen Fehler dem IBM Software Support.   |
| 0x00000065         | 101                    | GSK_OPEN_CIPHER_ERROR              | Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.  |
| 0x00000066         | 102                    | GSK_KEYFILE_IO_ERROR               | E/A-Fehler beim Lesen der Schlüsseldatei.  |
| 0x00000067         | 103                    | GSK_KEYFILE_INVALID_FORMAT         | Die Schlüsseldatei hat kein gültiges internes Format. Erstellen Sie die Schlüsseldatei erneut.   |
| 0x00000068         | 104                    | GSK_KEYFILE_DUPLICATE_KEY          | Die Schlüsseldatei hat zwei Einträge mit demselben Schlüssel.  |
| 0x00000069         | 105                    | GSK_KEYFILE_DUPLICATE_LABEL        | Die Schlüsseldatei hat zwei Einträge mit demselben Kennsatz.   |

| Rückkehrcode (hex) | Rückkehrcode (dezimal) | Konstante                              | Erläuterung  |
|--------------------|------------------------|--|--|
| 0x0000006a         | 106                    | GSK_BAD_FORMAT_OR_INVALID_PASSWORD     | Das Kennwort für die Schlüsseldatei wird als Integritätsprüfung verwendet. Entweder ist die Schlüsseldatei beschädigt oder die Kennwort-ID ist falsch.   |
| 0x0000006b         | 107                    | GSK_KEYFILE_CERT_EXPIRED               | Der Standardschlüssel in der Schlüsseldatei hat ein abgelaufenes Zertifikat.   |
| 0x0000006c         | 108                    | GSK_ERROR_LOAD_GSKLIB                  | Beim Laden einer der GSK DLL-Dateien ist ein Fehler aufgetreten. Überprüfen Sie, ob GSK korrekt installiert wurde.   |
| 0x0000006d         | 109                    | GSK_PENDING_CLOSE_ERROR                | Gibt an, dass eine Verbindung in einer GSK-Umgebung hergestellt werden soll, nachdem GSK_ENVIRONMENT_CLOSE_OPTIONS auf GSK_DELAYED_ENVIRONMENT_CLOSE gesetzt und die Funktion gsk_environment_close() aufgerufen wurde.              |
| 0x000000c9         | 201                    | GSK_NO_KEYFILE_PASSWORD                | Weder das Kennwort noch der Name der Stashdatei wurde angegeben. Die Schlüsseldatei wurde nicht initialisiert.   |
| 0x000000ca         | 202                    | GSK_KEYRING_OPEN_ERROR                 | Die Schlüsseldatei kann nicht geöffnet werden. Entweder wurde der Pfad nicht korrekt angegeben oder die Dateiberechtigungen erlauben nicht das Öffnen der Datei.   |
| 0x000000cb         | 203                    | GSK_RSA_TEMP_KEY_PAIR                  | Temporäres Schlüsselpaar kann nicht generiert werden. Melden Sie diesen Fehler dem IBM Software Support.   |
| 0x000000cc         | 204                    | GSK_ERROR_LDAP_NO_SUCH_OBJECT          | Das angegebene Benutzernamenobjekt wurde nicht gefunden.   |
| 0x000000cd         | 205                    | GSK_ERROR_LDAP_INVALID_CREDENTIALS     | Ein Kennwort, das für eine LDAP-Abfrage (LDAP = Lightweight Directory Access Protocol) verwendet wird, ist nicht korrekt.  |
| 0x000000ce         | 206                    | GSK_ERROR_BAD_INDEX                    | Ein Index in der Übernahmeliste der LDAP-Server war nicht korrekt.   |
| 0x000000cf         | 207                    | GSK_ERROR_FIPS_NOT_SUPPORTED           | Diese Installation von GSKit unterstützt nicht die FIPS-Betriebsart.   |
| 0x0000012d         | 301                    | GSK_CLOSE_FAILED                       | Gibt an, dass die Anforderung zum Schließen der GSK-Umgebung nicht korrekt ausgeführt wurde. Die Ursache ist wahrscheinlich ein Befehl gsk_secure_socket*(), der nach einem Aufruf gsk_close_environment() ausgeführt werden sollte. |
| 0x00000191         | 401                    | GSK_ERROR_BAD_DATE                     | Das Systemdatum wurde nicht auf einen gültigen Wert gesetzt.   |
| 0x00000192         | 402                    | GSK_ERROR_NO_CIPHERS                   | SSLv2 und SSLv3 sind nicht aktiviert.  |
| 0x00000193         | 403                    | GSK_ERROR_NO_CERTIFICATE               | Das erforderliche Zertifikat wurde nicht vom Partner empfangen.  |
| 0x00000194         | 404                    | GSK_ERROR_BAD_CERTIFICATE              | Das empfangene Zertifikat war nicht korrekt formatiert.  |
| 0x00000195         | 405                    | GSK_ERROR_UNSUPPORTED_CERTIFICATE_TYPE | Der empfangene Zertifikatstyp wurde nicht unterstützt.   |
| 0x00000196         | 406                    | GSK_ERROR_IO                           | Ein E/A-Fehler ist bei einer Datenlese- oder -schreiboperation aufgetreten.  |
| 0x00000197         | 407                    | GSK_ERROR_BAD_KEYFILE_LABEL            | Der angegebene Schlüsseldateikennsatz wurde nicht gefunden.  |

| Rückkehrcode (hex) | Rückkehrcode (dezimal) | Konstante                            | Erläuterung  |
|--------------------|------------------------|--------------------------------------|--|
| 0x00000198         | 408                    | GSK_ERROR_BAD_KEYFILE_PASSWORD       | Das angegebene Kennwort für die Schlüsseldatei ist falsch. Die Schlüsseldatei kann nicht verwendet werden. Die Schlüsseldatei kann auch beschädigt sein. |
| 0x00000199         | 409                    | GSK_ERROR_BAD_KEY_LEN_FOR_EXPORT     | In einer eingeschränkten Verschlüsselungsumgebung wird die Schlüsselgröße nicht unterstützt.   |
| 0x0000019a         | 410                    | GSK_ERROR_BAD_MESSAGE                | Eine falsch formatierte SSL-Nachricht wurde vom Partner empfangen.   |
| 0x0000019b         | 411                    | GSK_ERROR_BAD_MAC                    | Der Nachrichtenauthentifizierungscode wurde nicht erfolgreich überprüft.   |
| 0x0000019c         | 412                    | GSK_ERROR_UNSUPPORTED                | Nicht unterstütztes SSL-Protokoll oder nicht unterstützter Zertifikatstyp.   |
| 0x0000019d         | 413                    | GSK_ERROR_BAD_CERT_SIG               | Das empfangene Zertifikat enthielt eine falsche Signatur.  |
| 0x0000019e         | 414                    | GSK_ERROR_BAD_CERT                   | Falsch formatiertes Zertifikat vom Partner empfangen.  |
| 0x0000019f         | 415                    | GSK_ERROR_BAD_PEER                   | Kein gültiges SSL-Protokoll vom Partner empfangen.   |
| 0x000001a0         | 416                    | GSK_ERROR_PERMISSION_DENIED          | Melden Sie diesen Fehler dem IBM Software Support.   |
| 0x000001a1         | 417                    | GSK_ERROR_SELF_SIGNED                | Das selbst signierte Zertifikat ist nicht gültig.  |
| 0x000001a2         | 418                    | GSK_ERROR_NO_READ_FUNCTION           | <code>read()</code> ist fehlgeschlagen. Melden Sie diesen Fehler dem IBM Software Support.   |
| 0x000001a3         | 419                    | GSK_ERROR_NO_WRITE_FUNCTION          | <code>write()</code> ist fehlgeschlagen. Melden Sie diesen Fehler dem IBM Software Support.  |
| 0x000001a4         | 420                    | GSK_ERROR_SOCKET_CLOSED              | Der Partner hat das Socket geschlossen, bevor das Protokoll beendet war.   |
| 0x000001a5         | 421                    | GSK_ERROR_BAD_V2_CIPHER              | Die angegebene V2-Verschlüsselung ist nicht gültig.  |
| 0x000001a6         | 422                    | GSK_ERROR_BAD_V3_CIPHER              | Die angegebene V3-Verschlüsselung ist nicht gültig.  |
| 0x000001a7         | 423                    | GSK_ERROR_BAD_SEC_TYPE               | Melden Sie diesen Fehler dem IBM Software Support.   |
| 0x000001a8         | 424                    | GSK_ERROR_BAD_SEC_TYPE_COMBINATION   | Melden Sie diesen Fehler dem IBM Software Support.   |
| 0x000001a9         | 425                    | GSK_ERROR_HANDLE_CREATION_FAILED     | Die Kennung kann nicht erstellt werden. Melden Sie diesen Fehler dem IBM Software Support.   |
| 0x000001aa         | 426                    | GSK_ERROR_INITIALIZATION_FAILED      | Initialisierung ist fehlgeschlagen. Melden Sie diesen internen Fehler dem Service.   |
| 0x000001ab         | 427                    | GSK_ERROR_LDAP_NOT_AVAILABLE         | Bei der Überprüfung eines Zertifikats kann nicht auf die angegebene Benutzerregistry zugegriffen werden.   |
| 0x000001ac         | 428                    | GSK_ERROR_NO_PRIVATE_KEY             | Der angegebene Schlüssel enthielt keinen privaten Schlüssel.   |
| 0x000001ad         | 429                    | GSK_ERROR_PKCS11_LIBRARY_NOTLOADED   | Der Versuch, die angegebene gemeinsam genutzte PKCS11-Bibliothek zu laden, ist fehlgeschlagen.   |
| 0x000001ae         | 430                    | GSK_ERROR_PKCS11_TOKEN_LABELMISMATCH | Der PKCS #11-Treiber konnte das vom aufrufenden Programm angegebene Token nicht finden.  |

| Rückkehrcode (hex) | Rückkehrcode (dezimal) | Konstante                           | Erläuterung  |
|--------------------|------------------------|-------------------------------------|--|
| 0x000001af         | 431                    | GSK_ERROR_PKCS11_TOKEN_NOTPRESENT   | Ein PKCS #11-Token ist in dem Bereich nicht vorhanden.   |
| 0x000001b0         | 432                    | GSK_ERROR_PKCS11_TOKEN_BADPASSWORD  | Das Kennwort/die PIN für den Zugriff auf das PKCS #11-Token ist nicht gültig.  |
| 0x000001b1         | 433                    | GSK_ERROR_INVALID_V2_HEADER         | Der empfangene SSL-Header war kein korrekt formatierter SSLv2-Header.  |
| 0x000001b2         | 434                    | GSK_CSP_OPEN_ERROR                  | Der hardwarebasierte Verschlüsselungsserviceanbieter (Cryptographic Service Provider = CSP) kann nicht geöffnet werden. Entweder ist der CSP-Name nicht korrekt angegeben oder ein Versuch, auf den angegebenen CSP-Zertifikatsspeicher zuzugreifen, ist fehlgeschlagen. |
| 0x000001b3         | 435                    | GSK_CONFLICTING_ATTRIBUTE_SETTING   | Konflikt bei der Attributeinstellung zwischen PKCS11, der CMS-Schlüsseldatenbank und der Microsoft Krypto-API.   |
| 0x000001b4         | 436                    | GSK_UNSUPPORTED_PLATFORM            | Die angeforderte Funktion wird auf der Plattform, die von der Anwendung ausgeführt wird, nicht unterstützt. Die Microsoft Krypto-API wird beispielsweise nur auf der Plattform Windows 2000 unterstützt.   |
| 0x000001b6         | 438                    | GSK_ERROR_INCORRECT_SESSION_TYPE    | Ein falscher Wert wird von der Callback-Funktion zum Zurücksetzen des Sitzungstyps zurückgegeben. Nur GSKit <code>gsk_sever_session</code> , <code>gsk_sever_session_with_cl_auth</code> oder <code>gsk_sever_session_with_cl_auth_crit</code> ist zulässig.             |
| 0x000001f5         | 501                    | GSK_INVALID_BUFFER_SIZE             | Die Puffergröße ist negativ oder Null.   |
| 0x000001f6         | 502                    | GSK_WOULD_BLOCK                     | Wird mit nicht geblockter Ein-/Ausgabe verwendet. Siehe den Abschnitt zur nicht geblockten Ein-/Ausgabe.   |
| 0x00000259         | 601                    | GSK_ERROR_NOT_SSLV3                 | SSLv3 ist für <code>reset_cipher()</code> erforderlich, und die Verbindung verwendet SSLv2.  |
| 0x0000025a         | 602                    | GSK_MISC_INVALID_ID                 | Es wurde keine gültige ID für den Funktionsaufruf <code>gsk_secure_soc_misc()</code> angegeben.  |
| 0x000002bd         | 701                    | GSK_ATTRIBUTE_INVALID_ID            | Der Funktionsaufruf hat keine gültige ID. Dieses Problem kann auch durch die Angabe einer Umgebungskennung verursacht werden, wenn stattdessen eine Kennung für eine SSL-Verbindung verwendet werden müsste.   |
| 0x000002be         | 702                    | GSK_ATTRIBUTE_INVALID_LENGTH        | Das Attribut hat eine negative Länge, die nicht gültig ist.  |
| 0x000002bf         | 703                    | GSK_ATTRIBUTE_INVALID_ENUMERATION   | Der Aufzählungswert ist für den angegebenen Aufzählungstyp nicht gültig.   |
| 0x000002c0         | 704                    | GSK_ATTRIBUTE_INVALID_SID_CACHE     | Eine Parameterliste, die zum Ersetzen der SID-Cacheroutinen nicht gültig ist.  |
| 0x000002c1         | 705                    | GSK_ATTRIBUTE_INVALID_NUMERIC_VALUE | Beim Definieren eines numerischen Attributs ist der angegebene Wert für das spezielle Attribut, das definiert wird, nicht gültig.  |
| 0x000002c2         | 706                    | GSK_CONFLICTING_VALIDATION_SETTING  | Für die zusätzliche Zertifikatsvalidierung wurden sich widersprechende Parameter definiert.  |
| 0x000002c3         | 707                    | GSK_AES_UNSUPPORTED                 | Der AES-Verschlüsselungsalgorithmus wird nicht unterstützt.  |

| Rückkehrcode (hex) | Rückkehrcode (dezimal) | Konstante                             | Erläuterung   |
|--------------------|------------------------|---------------------------------------|---|
| 0x000002c4         | 708                    | GSK_PEERID_LENGTH_ERROR               | Die PEERID hat nicht die korrekte Länge.  |
| 0x000002c5         | 709                    | GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF | Der betreffende Chiffrierwert ist nicht zulässig, wenn die FIPS-Betriebsart auf OFF gesetzt ist.  |
| 0x000002c6         | 710                    | GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON  | In der FIPS-Betriebsart sind keine genehmigten FIPS-Chiffrierwerte ausgewählt.  |
| 0x00000641         | 1601                   | GSK_TRACE_STARTED                     | Der Trace wurde erfolgreich gestartet.  |
| 0x00000642         | 1602                   | GSK_TRACE_STOPPED                     | Der Trace wurde erfolgreich gestoppt.   |
| 0x00000643         | 1603                   | GSK_TRACE_NOT_STARTED                 | Es wurde zuvor keine Tracedatei gestartet. Daher kann sie nicht gestoppt werden.  |
| 0x00000644         | 1604                   | GSK_TRACE_ALREADY_STARTED             | Die Tracedatei wurde bereits gestartet. Daher kann sie nicht erneut gestartet werden.   |
| 0x00000645         | 1605                   | GSK_TRACE_OPEN_FAILED                 | Die Tracedatei kann nicht geöffnet werden. Der erste Parameter von <code>gsk_start_trace()</code> muss ein gültiger vollständiger Pfaddateiname sein. |

Tabelle 2. IBM Global Security Kit Key Management-Rückkehrcodes

| Rückkehrcode (hex) | Rückkehrcode (dezimal) | Konstante                     | Erläuterung  |
|--------------------|------------------------|-------------------------------|--|
| 0x00000000         | 0                      | GSK_OK                        | Die Task wurde erfolgreich ausgeführt. Diese Nachricht wird von jedem Funktionsaufruf ausgegeben, der erfolgreich ausgeführt wird.                               |
| 0x00000001         | 1                      | GSK_INVALID_HANDLE            | Die Umgebungskennung oder SSL-Kennung ist nicht gültig. Die angegebene Kennung war nicht das Ergebnis eines erfolgreichen Funktionsaufrufs <code>open()</code> . |
| 0x00000002         | 2                      | GSK_API_NOT_AVAILABLE         | Die DLL-Datei (DLL = Dynamic Link Library) wurde entladen und ist nicht verfügbar (tritt nur auf Microsoft Windows-Systemen auf).                                |
| 0x00000003         | 3                      | GSK_INTERNAL_ERROR            | Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.  |
| 0x00000004         | 4                      | GSK_INSUFFICIENT_STORAGE      | Für die Ausführung der Operation ist nicht genügend Speicher verfügbar.  |
| 0x00000005         | 5                      | GSK_INVALID_STATE             | Die Kennung hat einen falschen Status für die Operation, z. B. bei zweimaliger Ausführung einer Operation <code>init()</code> für eine Kennung.                  |
| 0x00000006         | 6                      | GSK_KEY_LABEL_NOT_FOUND       | Der angegebene Schlüsselkennsatz wurde nicht in der Schlüsseldatei gefunden.   |
| 0x00000007         | 7                      | GSK_CERTIFICATE_NOT_AVAILABLE | Zertifikat nicht vom Partner empfangen.  |
| 0x00000008         | 8                      | GSK_ERROR_CERT_VALIDATION     | Fehler bei der Zertifikatsvalidierung.   |
| 0x00000009         | 9                      | GSK_ERROR_CRYPTO              | Fehler bei der Verarbeitung der Verschlüsselung.   |
| 0x0000000a         | 10                     | GSK_ERROR_ASN                 | Fehler bei der Validierung von ASN-Feldern im Zertifikat.  |
| 0x0000000b         | 11                     | GSK_ERROR_LDAP                | Fehler beim Herstellen der Verbindung zur Benutzerregistry.  |

| <b>Rückkehrcode (hex)</b> | <b>Rückkehrcode (dezimal)</b> | <b>Konstante</b>                   | <b>Erläuterung</b>  |
|---------------------------|-------------------------------|------------------------------------|---|
| 0x0000000c                | 12                            | GSK_ERROR_UNKNOWN_ERROR            | Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.   |
| 0x00000065                | 101                           | GSK_OPEN_CIPHER_ERROR              | Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.   |
| 0x00000066                | 102                           | GSK_KEYFILE_IO_ERROR               | E/A-Fehler beim Lesen der Schlüsseldatei.   |
| 0x00000067                | 103                           | GSK_KEYFILE_INVALID_FORMAT         | Die Schlüsseldatei hat ein internes Format, das nicht gültig ist. Die Schlüsseldatei erneut erstellen.  |
| 0x00000068                | 104                           | GSK_KEYFILE_DUPLICATE_KEY          | Die Schlüsseldatei hat zwei Einträge mit demselben Schlüssel.   |
| 0x00000069                | 105                           | GSK_KEYFILE_DUPLICATE_LABEL        | Die Schlüsseldatei hat zwei Einträge mit demselben Kennsatz.  |
| 0x0000006a                | 106                           | GSK_BAD_FORMAT_OR_INVALID_PASSWORD | Das Kennwort für die Schlüsseldatei wird als Integritätsprüfung verwendet. Entweder ist die Schlüsseldatei beschädigt oder die Kennwort-ID ist falsch.  |
| 0x0000006b                | 107                           | GSK_KEYFILE_CERT_EXPIRED           | Der Standardschlüssel in der Schlüsseldatei hat ein abgelaufenes Zertifikat.  |
| 0x0000006c                | 108                           | GSK_ERROR_LOAD_GSKLIB              | Beim Laden einer der GSK DLL-Dateien ist ein Fehler aufgetreten. Überprüfen Sie, ob GSK korrekt installiert wurde.  |
| 0x0000006d                | 109                           | GSK_PENDING_CLOSE_ERROR            | Diese Nachricht gibt an, dass eine Verbindung in einer GSK-Umgebung hergestellt werden soll, nachdem GSK_ENVIRONMENT_CLOSE_OPTIONS auf GSK_DELAYED_ENVIRONMENT_CLOSE gesetzt und die Funktion gsk_environment_close() aufgerufen wurde. |
| 0x000000c9                | 201                           | GSK_NO_KEYFILE_PASSWORD            | Es wurde weder das Kennwort noch der Stashdateiname angegeben, daher konnte die Schlüsseldatei nicht initialisiert werden.  |
| 0x000000ca                | 202                           | GSK_KEYRING_OPEN_ERROR             | Die Schlüsseldatei kann nicht geöffnet werden. Entweder wurde der Pfad nicht korrekt angegeben oder die Dateiberechtigungen erlauben nicht das Öffnen der Datei.  |
| 0x000000cb                | 203                           | GSK_RSA_TEMP_KEY_PAIR              | Temporäres Schlüsselpaar kann nicht generiert werden. Melden Sie diesen Fehler dem IBM Software Support.  |
| 0x000000cc                | 204                           | GSK_ERROR_LDAP_NO_SUCH_OBJECT      | Das angegebene Benutzernamenobjekt wurde nicht gefunden.  |
| 0x000000cd                | 205                           | GSK_ERROR_LDAP_INVALID_CREDENTIALS | Ein Kennwort, das für eine LDAP-Abfrage verwendet wird, ist nicht korrekt.  |
| 0x000000ce                | 206                           | GSK_ERROR_BAD_INDEX                | Ein Index in der Übernahmeliste der LDAP-Server war nicht korrekt.  |



| <b>Rückkehrcode (hex)</b> | <b>Rückkehrcode (dezimal)</b> | <b>Konstante</b>                       | <b>Erläuterung</b>  |
|---------------------------|-------------------------------|--|---|
| 0x000000cf                | 207                           | GSK_ERROR_FIPS_NOT_SUPPORTED           | Diese Installation von GSKit unterstützt nicht die FIPS-Betriebsart.  |
| 0x0000012d                | 301                           | GSK_CLOSE_FAILED                       | Gibt an, dass die Anforderung zum Schließen der GSK-Umgebung nicht korrekt ausgeführt wurde. Die Ursache ist wahrscheinlich ein Befehl <code>gsk_secure_socket*()</code> , der nach einem Aufruf <code>gsk_close_environment()</code> ausgeführt werden sollte. |
| 0x00000191                | 401                           | GSK_ERROR_BAD_DATE                     | Das Systemdatum wurde auf einen Wert gesetzt, der nicht gültig ist.   |
| 0x00000192                | 402                           | GSK_ERROR_NO_CIPHERS                   | SSLv2 und SSLv3 sind nicht aktiviert.   |
| 0x00000193                | 403                           | GSK_ERROR_NO_CERTIFICATE               | Das erforderliche Zertifikat wurde nicht vom Partner empfangen.   |
| 0x00000194                | 404                           | GSK_ERROR_BAD_CERTIFICATE              | Das empfangene Zertifikat war nicht korrekt formatiert.   |
| 0x00000195                | 405                           | GSK_ERROR_UNSUPPORTED_CERTIFICATE_TYPE | Der empfangene Zertifikatstyp wurde nicht unterstützt.  |
| 0x00000196                | 406                           | GSK_ERROR_IO                           | Ein E/A-Fehler ist bei einer Datenlese- oder -schreiboperation aufgetreten.   |
| 0x00000197                | 407                           | GSK_ERROR_BAD_KEYFILE_LABEL            | Der angegebene Schlüsseldateikennsatz wurde nicht gefunden.   |
| 0x00000198                | 408                           | GSK_ERROR_BAD_KEYFILE_PASSWORD         | Das angegebene Kennwort für die Schlüsseldatei ist falsch. Die Schlüsseldatei kann nicht verwendet werden. Die Schlüsseldatei könnte auch beschädigt sein.  |
| 0x00000199                | 409                           | GSK_ERROR_BAD_KEY_LEN_FOR_EXPORT       | In einer eingeschränkten Verschlüsselungsumgebung wird die Schlüsselgröße nicht unterstützt.  |
| 0x0000019a                | 410                           | GSK_ERROR_BAD_MESSAGE                  | Eine falsch formatierte SSL-Nachricht wurde vom Partner empfangen.  |
| 0x0000019b                | 411                           | GSK_ERROR_BAD_MAC                      | Der Nachrichtenauthentifizierungscode wurde nicht erfolgreich verifiziert.  |
| 0x0000019c                | 412                           | GSK_ERROR_UNSUPPORTED                  | Nicht unterstütztes SSL-Protokoll oder nicht unterstützter Zertifikatstyp.  |
| 0x0000019d                | 413                           | GSK_ERROR_BAD_CERT_SIG                 | Das empfangene Zertifikat enthielt eine falsche Signatur.   |
| 0x0000019e                | 414                           | GSK_ERROR_BAD_CERT                     | Falsch formatiertes Zertifikat vom Partner empfangen.   |
| 0x0000019f                | 415                           | GSK_ERROR_BAD_PEER                     | Ein ungültiges SSL-Protokoll wurde vom Partner empfangen.   |
| 0x000001a0                | 416                           | GSK_ERROR_PERMISSION_DENIED            | Melden Sie diesen Fehler dem IBM Software Support.  |
| 0x000001a1                | 417                           | GSK_ERROR_SELF_SIGNED                  | Das selbst signierte Zertifikat ist nicht gültig.   |

| Rückkehrcode (hex) | Rückkehrcode (dezimal) | Konstante                            | Erläuterung  |
|--------------------|------------------------|--------------------------------------|--|
| 0x000001a2         | 418                    | GSK_ERROR_NO_READ_FUNCTION           | read() ist fehlgeschlagen. Melden Sie diesen Fehler dem IBM Software Support.  |
| 0x000001a3         | 419                    | GSK_ERROR_NO_WRITE_FUNCTION          | write() ist fehlgeschlagen. Melden Sie diesen Fehler dem IBM Software Support.   |
| 0x000001a4         | 420                    | GSK_ERROR_SOCKET_CLOSED              | Der Partner hat das Socket geschlossen, bevor das Protokoll beendet war.   |
| 0x000001a5         | 421                    | GSK_ERROR_BAD_V2_CIPHER              | Die angegebene V2-Verschlüsselung ist nicht gültig.  |
| 0x000001a6         | 422                    | GSK_ERROR_BAD_V3_CIPHER              | Die angegebene V3-Verschlüsselung ist nicht gültig.  |
| 0x000001a7         | 423                    | GSK_ERROR_BAD_SEC_TYPE               | Melden Sie diesen Fehler dem IBM Software Support.   |
| 0x000001a8         | 424                    | GSK_ERROR_BAD_SEC_TYPE_COMBINATION   | Melden Sie diesen Fehler dem IBM Software Support.   |
| 0x000001a9         | 425                    | GSK_ERROR_HANDLE_CREATION_FAILED     | Die Kennung wurde nicht erstellt. Melden Sie diesen Fehler dem IBM Software Support.   |
| 0x000001aa         | 426                    | GSK_ERROR_INITIALIZATION_FAILED      | Initialisierung ist fehlgeschlagen. Melden Sie diesen internen Fehler dem Service.   |
| 0x000001ab         | 427                    | GSK_ERROR_LDAP_NOT_AVAILABLE         | Bei der Überprüfung eines Zertifikats kann nicht auf die angegebene Benutzerregistry zugegriffen werden.   |
| 0x000001ac         | 428                    | GSK_ERROR_NO_PRIVATE_KEY             | Der angegebene Schlüssel enthielt keinen privaten Schlüssel.   |
| 0x000001ad         | 429                    | GSK_ERROR_PKCS11_LIBRARY_NOTLOADED   | Der Versuch, die angegebene gemeinsam genutzte PKCS11-Bibliothek zu laden, ist fehlgeschlagen.   |
| 0x000001ae         | 430                    | GSK_ERROR_PKCS11_TOKEN_LABELMISMATCH | Der PKCS #11-Treiber konnte das vom aufrufenden Programm angegebene Token nicht finden.  |
| 0x000001af         | 431                    | GSK_ERROR_PKCS11_TOKEN_NOTPRESENT    | Ein PKCS #11-Token ist in dem Bereich nicht vorhanden.   |
| 0x000001b0         | 432                    | GSK_ERROR_PKCS11_TOKEN_BADPASSWORD   | Das Kennwort/die PIN für den Zugriff auf das PKCS #11-Token ist falsch.  |
| 0x000001b1         | 433                    | GSK_ERROR_INVALID_V2_HEADER          | Der empfangene SSL-Header war kein korrekt formatierter SSLv2-Header.  |
| 0x000001b2         | 434                    | GSK_CSP_OPEN_ERROR                   | Der hardwarebasierte Verschlüsselungsserviceanbieter (Cryptographic Service Provider = CSP) konnte nicht geöffnet werden. Entweder ist der CSP-Name nicht korrekt angegeben oder ein Versuch, auf den angegebenen CSP-Zertifikatsspeicher zuzugreifen, ist fehlgeschlagen. |

| Rückkehrcode (hex) | Rückkehrcode (dezimal) | Konstante                             | Erläuterung   |
|--------------------|------------------------|---------------------------------------|---|
| 0x000001b3         | 435                    | GSK_CSP_OPEN_ERROR                    | Einige sich widersprechende Attribute für die SSL-Operation wurden definiert.   |
| 0x000001b4         | 436                    | GSK_CSP_OPEN_ERROR                    | Die Microsoft Crypto API wird nur unter Microsoft Windows 2000 mit Service-Pack 2 unterstützt.  |
| 0x000001b5         | 437                    | GSK_CSP_OPEN_ERROR                    | System wird im IPv6-Modus ausgeführt, ohne dass eine PEERID definiert ist.  |
| 0x000001f5         | 501                    | GSK_INVALID_BUFFER_SIZE               | Die Puffergröße ist negativ oder Null.  |
| 0x000001f6         | 502                    | GSK_WOULD_BLOCK                       | Wird mit nicht geblockter Ein-/Ausgabe verwendet. Siehe den Abschnitt zur nicht geblockten Ein-/Ausgabe.  |
| 0x00000259         | 601                    | GSK_ERROR_NOT_SSLV3                   | SSLv3 ist für reset_cipher() erforderlich, und die Verbindung verwendet SSLv2.  |
| 0x0000025a         | 602                    | GSK_MISC_INVALID_ID                   | Eine ungültige ID wurde für den Funktionsaufruf gsk_secure_soc_misc() angegeben.  |
| 0x000002bd         | 701                    | GSK_ATTRIBUTE_INVALID_ID              | Der Funktionsaufruf hat eine ID, die nicht gültig ist. Dieses Problem kann auch durch die Angabe einer Umgebungskennung verursacht werden, wenn stattdessen eine Kennung für eine SSL-Verbindung verwendet werden müsste. |
| 0x000002be         | 702                    | GSK_ATTRIBUTE_INVALID_LENGTH          | Das Attribut hat eine negative Länge, die nicht gültig ist.   |
| 0x000002bf         | 703                    | GSK_ATTRIBUTE_INVALID_ENUMERATION     | Der Aufzählungswert ist für den angegebenen Aufzählungstyp nicht gültig.  |
| 0x000002c0         | 704                    | GSK_ATTRIBUTE_INVALID_SID_CACHE       | Eine Parameterliste, die zum Ersetzen der SID-Cacheroutinen nicht gültig ist.   |
| 0x000002c1         | 705                    | GSK_ATTRIBUTE_INVALID_NUMERIC_VALUE   | Beim Definieren eines numerischen Attributs ist der angegebene Wert für das spezielle Attribut, das definiert wird, nicht gültig.   |
| 0x000002c2         | 706                    | GSK_CONFLICTING_VALIDATION_SETTING    | Für die zusätzliche Zertifikatsvalidierung wurden sich widersprechende Parameter definiert.   |
| 0x000002c3         | 707                    | GSK_AES_UNSUPPORTED                   | Der AES-Verschlüsselungsalgorithmus wird nicht unterstützt.   |
| 0x000002c4         | 708                    | GSK_PEERID_LENGTH_ERROR               | Die PEERID hat nicht die korrekte Länge.  |
| 0x000002c5         | 709                    | GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF | Der betreffende Chiffrierwert ist nicht zulässig, wenn die FIPS-Betriebsart auf OFF gesetzt ist.  |
| 0x000002c6         | 710                    | GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON  | In der FIPS-Betriebsart sind keine genehmigten FIPS-Chiffrierwerte ausgewählt.  |

| Rückkehrcode (hex) | Rückkehrcode (dezimal) | Konstante                 | Erläuterung   |
|--------------------|------------------------|---------------------------|---|
| 0x00000641         | 1601                   | GSK_TRACE_STARTED         | Der Trace wurde erfolgreich gestartet.  |
| 0x00000642         | 1602                   | GSK_TRACE_STOPPED         | Der Trace wurde erfolgreich gestoppt.   |
| 0x00000643         | 1603                   | GSK_TRACE_NOT_STARTED     | Es wurde zuvor keine Tracedatei gestartet. Daher kann sie nicht gestoppt werden.  |
| 0x00000644         | 1604                   | GSK_TRACE_ALREADY_STARTED | Die Tracedatei wurde bereits gestartet. Daher kann sie nicht erneut gestartet werden.   |
| 0x00000645         | 1605                   | GSK_TRACE_OPEN_FAILED     | Die Tracedatei kann nicht geöffnet werden. Der erste Parameter von <code>gsk_start_trace()</code> muss ein gültiger vollständiger Pfaddateiname sein. |

## Glossar

Dieses Glossar stellt Begriffe und Definitionen für IBM Spectrum Protect, IBM Spectrum Protect Snapshot und zugehörige Produkte bereit.

Die folgenden Querverweise werden in diesem Glossar verwendet:

- Mit *Siehe* wird von einem Begriff, der nicht bevorzugt verwendet wird, auf den bevorzugten Begriff oder von einer Abkürzung auf die vollständige Form verwiesen.
- Mit *Siehe auch* wird auf einen zugehörigen oder gegensätzlichen Begriff verwiesen.

Andere Begriffe und Definitionen finden Sie auf der IBM® Terminology-Website.

A B C D E F G H I J K L M N O P Q R S T U V W Z

### A

#### Abruf

Archivierte Informationen aus dem Speicherpool auf die Workstation kopieren, um sie zu verwenden. Die Abrufoperation hat keine Auswirkungen auf die archivierte Version im Speicherpool. Siehe auch Archivierung.

#### Absoluter Modus

Bei der Speicherverwaltung ein Modus der Sicherungskopiengruppe, der angibt, dass eine Datei oder ein Verzeichnis bei der Teilsicherung zu berücksichtigen ist, auch wenn sich die Datei oder das Verzeichnis seit der letzten Sicherung nicht geändert hat. Siehe auch Modus, Geänderter Modus.

#### Abstimmung

Der Prozess, bei dem die Konsistenz zwischen dem ursprünglichen Datenrepository und dem größeren System, auf dem die Daten für die Sicherung gespeichert werden, sichergestellt wird. Beispiele für größere Systeme, auf denen die Daten für die Sicherung gespeichert werden, sind Speicherserver oder andere Speichersysteme. Während des Abstimmungsprozesses werden Daten, die nicht mehr benötigt werden, entfernt.

#### ACK

Siehe Empfangsbestätigung.

#### ACL

Siehe Zugriffssteuerungsliste (ACL).

#### Adaptive Subdateisicherung

Ein Sicherungstyp, bei dem nur geänderte Teile einer Datei an den Server gesendet werden und nicht die gesamte Datei. Mit der adaptiven Subdateisicherung wird der Datenaustausch im Netz reduziert und die Sicherungsgeschwindigkeit wird erhöht.

#### Administrator

Eine Person, die für Verwaltungstasks wie z. B. Zugriffsberechtigungen und Content-Management verantwortlich ist. Administratoren können Benutzern auch Berechtigungsstufen zuordnen.

#### Agentenknoten

Ein Clientknoten, dem Proxyberechtigung erteilt wurde, um Operationen für einen anderen Clientknoten auszuführen, der der Zielknoten ist.

#### Aggregat

Ein Objekt, das in einem oder mehreren Speicherpools gespeichert ist und das aus einer Gruppe von logischen Dateien besteht, die zusammengefasst sind. Siehe auch Logische Datei, Physische Datei.

#### Aktive Maßnahmengruppe

Die aktivierte Maßnahmengruppe. Diese Maßnahmengruppe enthält die Maßnahmenregeln, die alle der Maßnahmendomäne zugeordneten Clientknoten derzeit verwenden. Siehe auch Maßnahmendomäne, Maßnahmengruppe.

#### Aktives Dateisystem

Ein Dateisystem, dem die Speicherverwaltung hinzugefügt wurde. Mit der Speicherverwaltung werden folgende Tasks für ein aktives Dateisystem ausgeführt: automatische Umlagerung, Abstimmung, selektive Umlagerung und Rückruf. Siehe auch Inaktives Dateisystem.

#### Aktive Version

Die neueste Sicherungskopie einer gespeicherten Datei. Die aktive Version einer Datei kann erst dann gelöscht werden, wenn ein Sicherungsprozess erkennt, dass der Benutzer die Datei entweder durch eine neuere Version ersetzt oder vom Dateiserver bzw. von der Workstation gelöscht hat. Siehe auch Sicherungsversion, Inaktive Version.

#### Aktivieren

Den Inhalt einer Maßnahmengruppe überprüfen und die Maßnahmengruppe dann zur aktiven Maßnahmengruppe machen.

#### Aktivitätenprotokoll

Ein Protokoll, in dem die Nachrichten für normale Aktivitäten aufgezeichnet werden, die der Server generiert. Diese Nachrichten enthalten Informationen zu Server- und Clientoperationen, wie die Startzeit der Sitzungen oder E/A-Fehler von Einheiten.

#### Anwendungsclient

Ein Programm, das auf einem System installiert ist, um eine Anwendung zu schützen. Der Server stellt Sicherungsservices für einen Anwendungsclient zur Verfügung.

#### Arbeitsdatenträger

Ein Datenträger mit Kennsatz, der keine Daten oder keine gültigen Daten enthält, der nicht definiert ist und der für die Verwendung zur Verfügung steht. Siehe auch Datenträger.

#### Archivierung

Programme, Daten oder Dateien auf andere Speichermedien kopieren, normalerweise für die Langzeitspeicherung oder zur Absicherung. Siehe auch Abruf.

#### Archivierungskopie

Eine Datei oder Dateigruppe, die im Serverspeicher archiviert wurde.

#### Archivierungskopiengruppe

Ein Maßnahmenobjekt mit Attributen, die die Generierung, den Zielort und das Verfallsdatum von archivierten Dateien steuern. Siehe auch Kopiengruppe.

#### Aufbewahrungsdauer

Die Zeit in Tagen, in denen inaktive gesicherte oder archivierte Dateien im Speicherpool aufbewahrt werden, bevor sie gelöscht werden. Kopiengruppenattribute und Standardaufbewahrungszeiträume für die Domäne definieren die Aufbewahrungszeit.

#### Aufbewahrungszeitraum für Archivierung

Die Anzahl der Tage, die der Speichermanager eine archivierte Datei aufbewahrt, wenn der Server die Datei nicht erneut an eine entsprechende Verwaltungsklasse binden kann. Siehe auch Binden.

#### Aufbewahrungszeitraum für Sicherung

Die Anzahl der Tage, die der Speichermanager eine Sicherungsversion aufbewahrt, nachdem der Server die Datei nicht erneut an eine entsprechende Verwaltungsklasse binden kann.

#### Ausgelagerte VSS-Sicherung

Eine Sicherungsoperation, bei der ein (auf einem anderen System installierter) Microsoft-VSS-Hardwareprovider (VSS - Volume Shadow Copy Service) verwendet wird, um Daten auf den Server zu versetzen. Bei diesem Typ der Sicherungsoperation wird die Arbeitslast der Sicherung vom Produktionssystem auf ein anderes System verlagert.

#### Ausschließen

Der Prozess der Angabe von Dateien in einer Einschluss-/Ausschlussliste. Dieser Prozess verhindert, dass Dateien gesichert oder umgelagert werden, wenn ein Benutzer oder ein Zeitplan eine Teilsicherungsoperation oder selektive Sicherungsoperation startet. Eine Datei kann von der Sicherung und/oder der Speicherverwaltung ausgeschlossen werden.

#### Ausschluss-/Einschlussliste

Siehe Einschluss-/Ausschlussliste.

#### Authentifizierungsregel

Eine Spezifikation, die ein anderer Benutzer verwenden kann, um Dateien aus dem Speicher zurückzuschreiben oder abzurufen.

#### AutoFS

Siehe Auto-Mount-Dateisystem.

#### Automatische Erkennung

Eine Funktion, die die Seriennummer eines Laufwerks oder eines Kassettenarchivs in der Datenbank feststellt, auflistet und aktualisiert, wenn der Pfad vom lokalen Server definiert ist.

#### Automatische Umlagerung

Der Prozess, mit dem Dateien automatisch von einem lokalen Dateisystem in den Speicher versetzt werden. Dieser Prozess basiert auf Optionen und Einstellungen, die ein Root auf einer Workstation auswählt. Siehe auch Bedarfsumlagerung, Schwelkenumlagerung.

#### Auto-Mount-Dateisystem (AutoFS)

Ein Dateisystem, das von einem Automount-Dämon verwaltet wird. Der Automount-Dämon überwacht einen bestimmten Verzeichnispfad und hängt das Dateisystem automatisch an, um auf Daten zuzugreifen.

## B

---

### Bandarchiv

Eine Gruppe von Geräten und Funktionen, die die Bandumgebung einer Installation unterstützen. Das Bandarchiv kann Racks für Bandkassetten, Mechanismen für das automatische Einlegen von Bändern, eine Reihe von Bandlaufwerken und eine Gruppe von zugehörigen Banddatenträgern umfassen, die in diese Laufwerke eingelegt sind.

### Bedarfsumlagerung

Der Prozess, mit dem in einem Dateisystem, für das die hierarchische Speicherverwaltung (Hierarchical Storage Management - HSM) aktiv ist, auf eine Bedingung 'Zu wenig Speicherbereich' reagiert wird. Dateien werden in den Serverspeicher umgelagert, bis die Speicherbereichsbelegung die untere Schwelle erreicht, die für das Dateisystem definiert wurde. Sind die obere Schwelle und die untere Schwelle identisch, wird eine einzige Datei umgelagert. Siehe auch Automatische Umlagerung, Selektive Umlagerung, Schwellenumlagerung.

### Bedienerberechtigungsklasse

Eine Berechtigungsklasse, die einem Administrator die Berechtigung für folgende Tasks erteilt: Server inaktivieren oder stoppen, Server aktivieren, Serverprozesse abbrechen und austauschbare Datenträger verwalten. Siehe auch Berechtigungsklasse.

### Benannte Pipe

Eine Art der Interprozesskommunikation, bei der Nachrichtendatenströme zwischen Peer-Prozessen, wie z. B. einem Client und einem Server, fließen können.

### Berechtigter Benutzer

Ein Benutzer mit Administratorberechtigung für den Client auf einer Workstation. Dieser Benutzer ändert Kennwörter, führt offene Registrierungen durch und löscht Dateibereiche.

### Berechtigung

Das Recht, auf Objekte, Ressourcen oder Funktionen zuzugreifen. Siehe auch Berechtigungsklasse.

### Berechtigungsklasse

Eine Berechtigungsstufe, die einem Administrator erteilt wird. Die Berechtigungsklasse bestimmt, welche Verwaltungstasks vom Administrator ausgeführt werden können. Siehe auch Berechtigung, Knotenberechtigungsklasse, Bedienerberechtigungsklasse, Maßnahmenberechtigungsklasse, Speicherberechtigungsklasse, Systemberechtigungsklasse.

### Berechtigungsregel

Eine Spezifikation, die es einem anderen Benutzer ermöglicht, die Dateien eines Benutzers aus dem Speicher zurückzuschreiben oder abzurufen.

### Beschädigte Datei

Eine physische Datei, in der Lesefehler erkannt wurden.

### Binden

Einer Datei einen Verwaltungsklassennamen zuordnen. Siehe auch Aufbewahrungszeitraum für Archivierung, Verwaltungsklasse, Erneut binden.

### Bucket

Cloudspeichercontainer, der von Amazon Simple Storage Service (Amazon S3) verwendet wird.

## C

---

### Cache

Eine Duplikatkopie einer Datei auf ein Speichermedium mit wahlfreiem Zugriff stellen, wenn der Server eine Datei in einen anderen Speicherpool in der Hierarchie umlagert.

### Cachedatei

Eine Momentaufnahme eines logischen Datenträgers, die vom Logical Volume Snapshot Agent erstellt wurde. Werden Blöcke während der Imagesicherung geändert, werden sie unmittelbar vor der Änderung gesichert und ihre logischen Bereiche werden in den Cachedateien gesichert.

### CAD

Siehe Clientakzeptordämon.

### Client

Ein Softwareprogramm oder ein Computer, das bzw. der Services von einem Server anfordert. Siehe auch Server.

### Clientakzeptor

Ein Service, der Web-Browsern das Java™-Applet für den Web-Client bereitstellt. Auf Windows-Systemen wird der Clientakzeptor so installiert, dass er als Dienst ausgeführt wird. Auf AIX-, UNIX- und Linux-Systemen wird der Clientakzeptor als Dämon ausgeführt.

### Clientakzeptordämon (CAD)

Siehe Clientakzeptor.

### Clientbenutzeroptionsdatei

Eine Datei, die die Gruppe von Verarbeitungsoptionen enthält, die die Clients auf dem System verwenden. Die Gruppe kann Optionen umfassen, die den Server angeben, den der Client kontaktiert, sowie Optionen, die sich auf Sicherungsoperationen, Archivierungsoperationen, Operationen für hierarchische Speicherverwaltung und geplante Operationen auswirken. Diese Datei wird auch als Datei dsm.opt bezeichnet. Für AIX-, UNIX- oder Linux-Systeme siehe auch 'Clientsystemoptionsdatei'. Siehe auch Clientsystemoptionsdatei, Optionsdatei.

### Clientdomäne

Die Gruppe von Laufwerken, Dateisystemen oder Datenträgern, die der Benutzer für das Sichern oder Archivieren von Daten mit dem Client für Sichern/Archivieren auswählt.

**Client für hierarchische Speicherverwaltung (HSM-Client)**

Ein Clientprogramm, das zusammen mit dem Server hierarchische Speicherverwaltung (HSM - Hierarchical Storage Management) für ein System bereitstellt. Siehe auch Hierarchische Speicherverwaltung, Verwaltungsklasse.

**Client für Sichern/Archivieren**

Ein Programm, das auf einer Workstation oder einem Dateiserver ausgeführt wird und Benutzern ein Mittel zum Sichern, Archivieren, Zurückschreiben und Abrufen von Dateien bietet. Siehe auch Verwaltungsclient.

**Clientknoten**

Ein Dateiserver oder eine Workstation, auf dem bzw. der das Clientprogramm für Sichern/Archivieren installiert und beim Server registriert wurde.

**Clientknotensitzung**

Eine Sitzung, in der ein Clientknoten mit einem Server kommuniziert, um Sicherungs-, Zurückschreibungs-, Archivierungs-, Abruf-, Umlagerungs- oder Rückrufanforderungen auszuführen. Siehe auch Sitzung.

**Clientoptionsdatei**

Eine editierbare Datei, in der der Server und die Übertragungsmethode angegeben sind und die die Konfiguration für die Sicherung, Archivierung, hierarchische Speicherverwaltung und Zeitplanung bereitstellt.

**Clientoptionsgruppe**

Eine Gruppe von Optionen, die auf dem Server definiert sind und auf Clientknoten in Verbindung mit der Clientoptionsdatei verwendet werden.

**Client/Server**

Bezieht sich auf das Interaktionsmodell bei der verteilten Datenverarbeitung, bei dem ein Programm auf einem Computer eine Anforderung an ein Programm auf einem anderen Computer sendet und auf eine Antwort wartet. Das anfordernde Programm wird als Client bezeichnet, das antwortende Programm als Server.

**Clientsystemoptionsdatei**

Eine Datei, die auf Clients mit AIX-, UNIX- oder Linux-Systemen verwendet wird. Diese Datei enthält eine Gruppe von Verarbeitungsoptionen, die die Server angeben, die für Services kontaktiert werden sollen. Diese Datei gibt auch die Übertragungsmethoden und Optionen für Sicherung, Archivierung, hierarchische Speicherverwaltung und Zeitplanung an. Siehe auch Clientbenutzeroptionsdatei, Optionsdatei.

**Clientzeitplan**

Ein Datenbanksatz, der die geplante Verarbeitung einer Clientoperation während einer bestimmten Zeitspanne beschreibt. Bei der Clientoperation kann es sich um eine Sicherungs-, Archivierungs-, Zurückschreibungs- oder Abrufoperation, einen Clientbetriebssystembefehl oder ein Makro handeln. Siehe auch Zeitplan für Verwaltungsbefehle, Zentrale Zeitplanung, Zeitplan.

**Cloud-Containerspeicherpool**

Ein Speicherpool, der von einem Server verwendet wird, um Daten im Cloudspeicher zu speichern. Der Cloudspeicher kann sich vor Ort (on premises) oder außerhalb des Unternehmens (off premises) befinden. Siehe auch Containerspeicherpool, Verzeichniscontainerspeicherpool, Speicherpool.

**Container**

Eine Datenspeicherposition, z. B. eine Datei, ein Verzeichnis oder eine Einheit. Siehe auch Containerspeicherpool.

**Containerkopierspeicherpool**

Ein Speicherpool, der von einem Server verwendet wird, um Kopien von Bereichen aus Verzeichniscontainerspeicherpools zu speichern. Die Kopien werden verwendet, um Beschädigungen in einem Verzeichniscontainerspeicherpool zu reparieren. Containerkopierspeicherpools verwenden sequenzielle Datenträger wie z. B. Band. Siehe auch Verzeichniscontainerspeicherpool.

**Containerspeicherpool**

Ein primärer Speicherpool, der von einem Server zum Speichern von Daten verwendet wird. Daten werden in Containern in Dateisystemverzeichnissen oder im Cloudspeicher gespeichert. Falls erforderlich, werden Daten dedupliziert, wenn der Server die Daten in den Speicherpool schreibt. Siehe auch Cloud-Containerspeicherpool, Container, Verzeichniscontainerspeicherpool.

## D

---

**Dämon**

Ein unbeaufsichtigtes Programm, das kontinuierliche oder regelmäßige Funktionen wie Netzsteuerung ausführt.

**Data Storage-Management Application-Programming Interface (DSMAPI)**

Eine Funktions- und Semantikgruppe, die Ereignisse für Dateien überwachen und die Daten in einer Datei verwalten und pflegen kann. In einer HSM-Umgebung verwendet eine DSMAPI Ereignisse, um Datenverwaltungsanwendungen über Operationen mit Dateien zu informieren. Zudem speichert eine DSMAPI beliebige Attributinformationen mit einer Datei; sie unterstützt verwaltete Regionen in einer Datei und verwendet DSMAPI-Zugriffsberechtigungen, um den Zugriff auf ein Dateiobjekt zu steuern.

**Dateialter**

Bei der Festlegung der Umlagerungspriorität die Anzahl Tage seit dem letzten Zugriff auf eine Datei.

**Dateibereich**

Ein logischer Speicherbereich im Serverspeicher, der eine Gruppe von Dateien enthält, die von einem Clientknoten aus einer einzelnen logischen Partition, einem einzelnen Dateisystem oder einem einzelnen virtuellen Mountpunkt gesichert oder archiviert wurden. Clientknoten können ihre Dateibereiche im Serverspeicher zurückschreiben, abzurufen oder löschen. Im Serverspeicher werden Dateien, die zu einem einzigen Dateibereich gehören, nicht notwendigerweise zusammen gespeichert.

**Dateibereichs-ID (FSID)**

- Eine eindeutige numerische Kennung, die der Server einem Dateibereich zuordnet, wenn er in einem Serverspeicher gespeichert wird.
- Dateiindex**  
Die interne Struktur, die einzelne Dateien auf AIX-, UNIX- oder Linux-Systemen beschreibt. Ein Dateiindex enthält den Knoten, den Typ, den Eigner und die Position einer Datei.
- Dateiindexnummer**  
Eine Nummer, die eine bestimmte Dateiindexdatei im Dateisystem angibt.
- Datei mit freien Bereichen**  
Eine Datei, die mit einer Länge erstellt wird, die größer als die darin enthaltenen Daten ist. Somit sind leere Speicherbereiche für die zukünftige Hinzufügung von Daten vorhanden.
- Dateiserver**  
Ein dedizierter Computer mit seinen peripheren Speichereinheiten, die an ein lokales Netz angeschlossen sind. Der Computer speichert Programme und Dateien, die von Benutzern in dem Netz gemeinsam genutzt werden.
- Dateistatus**  
Der Speicherverwaltungsmodus einer Datei, die in einem Dateisystem gespeichert ist, dem die Speicherverwaltung hinzugefügt wurde. Eine Datei kann sich in einem der drei folgenden Status befinden: resident, vorumgelagert oder umgelagert. Siehe auch Umgelagerte Datei, Vorumgelagerte Datei, Residente Datei.
- Dateisystemstatus**  
Der Speicherverwaltungsmodus eines Dateisystems, das sich auf einer Workstation befindet, auf der der HSM-Client (HSM = Hierarchical Storage Management = Hierarchische Speicherverwaltung) installiert ist. Ein Dateisystem kann sich in einem der folgenden Status befinden: nativ, aktiv, inaktiv oder global inaktiv.
- Dateizugriffszeit**  
Auf AIX-, UNIX- oder Linux-Systemen die Zeit, zu der der letzte Zugriff auf die Datei erfolgte.
- Datenbank für vorumgelagerte Dateien**  
Eine Datenbank, die Informationen zu allen in den Serverspeicher vorumgelagerten Dateien enthält.
- Datenbankmomentaufnahme**  
Eine vollständige Sicherung der gesamten Datenbank auf Medien, die an einen anderen Standort gebracht werden können. Wenn eine Momentaufnahme der Datenbank erstellt wird, wird die momentane Datenbanksicherungsserie nicht unterbrochen. Eine Datenbankmomentaufnahme kann keine Datenbanksicherungen enthalten. Siehe auch Datenbanksicherungsserie, Gesamtsicherung.
- Datenbanksicherungsserie**  
Eine Gesamtsicherung der Datenbank, plus bis zu 32 Teilsicherungen, die seit der Gesamtsicherung erstellt wurden. Jede Gesamtsicherung, die ausgeführt wird, startet eine neue Datenbanksicherungsserie. Eine Zahl identifiziert jede Sicherungsserie. Siehe auch Datenbankmomentaufnahme, Gesamtsicherung.
- Datencenter**  
In einer virtualisierten Umgebung ein Container, der Hosts, Cluster, Netze und Datenspeicher enthält.
- Datendeduplizierung**  
Eine Methode zum Reduzieren des Speicherbedarfs, indem redundante Daten entfernt werden. Nur eine Instanz der Daten wird auf Speicherdatenträgern aufbewahrt. Andere Instanzen derselben Daten werden durch einen Zeiger auf die aufbewahrte Instanz ersetzt. Siehe auch Inline-Datendeduplizierung, Nachgeordnete Datendeduplizierung.
- Datenmanagerserver**  
Ein Server, der Metadateninformationen für den Clientdatenträgerbestand sammelt und für den Speicheragenten Transaktionen über das LAN verwaltet. Der Datenmanagerserver informiert den Speicheragenten über die jeweiligen Kassettenarchivattribut und die Kennung des Zieldatenträgers.
- Datenspeicher**  
In einer virtualisierten Umgebung die Position, an der Daten der virtuellen Maschine gespeichert werden.
- Datenträger**  
Ein diskreter Speicherbereich auf Platte, Band oder einem anderen Medium zur Datenaufzeichnung, das eine Kennung und eine Parameterliste unterstützt, z. B. einen Datenträgerkennsatz oder Ein-/Ausgabesteuerung. Siehe auch Arbeitsdatenträger, Serverspeicher, Speicherpool, Speicherpooldatenträger.
- Datenträgerhistorydatei**  
Eine Datei, die Informationen zu Datenträgern enthält, die vom Server für Datenbanksicherungen und für den Export von Administrator-, Knoten-, Maßnahmen- oder Serverdaten verwendet wurde. Die Datei umfasst außerdem Informationen zu Datenträgern in Speicherpools mit sequenziellem Zugriff, die hinzugefügt, erneut verwendet oder gelöscht wurden. Die Informationen sind eine Kopie der Datenträgerinformationen in der Serverdatenbank.
- Datenübertragungsgeschwindigkeit im Netz**  
Eine Geschwindigkeit, die durch Dividieren der Gesamtzahl der übertragenen Byte durch die Datenübertragungszeit berechnet wird. Bei dieser Geschwindigkeit kann es sich beispielsweise um die Zeit handeln, die für die Übertragung von Daten über ein Netz erforderlich ist.
- Deduplizierung**  
Siehe Datendeduplizierung.
- Dialog**  
Eine Verbindung zwischen zwei Programmen über eine Sitzung, über die diese während der Verarbeitung einer Transaktion kommunizieren können.
- Disaster Recovery Manager (DRM)**



Eine Funktion, die Benutzer bei der Vorbereitung und Verwendung einer Plandatei zur Wiederherstellung nach einem Katastrophenfall für den Server unterstützt.

#### Domäne

Eine Gruppierung von Clientknoten mit einer oder mehreren Maßnahmengruppen, die für die Clientknoten Daten oder Speicherressourcen verwalten. Siehe auch Maßnahmendomäne.

#### DRM

Siehe Disaster Recovery Manager.

#### DSMAPI

Siehe Data Storage-Management Application-Programming Interface.

#### Durchnummerierung

Der Prozess, bei dem Dateien verarbeitet werden, die während der Sicherungs- oder Archivierungsverarbeitung geändert wurden. Siehe auch Gemeinsam dynamisch (Durchnummerierung), Gemeinsam statisch (Durchnummerierung), Statisch (Durchnummerierung).

#### Durchsatz

Bei der Speicherverwaltung die Gesamtsumme der Byte im Verarbeitungsprozess (mit Ausnahme des Systemaufwands), die gesichert oder zurückgeschrieben werden, dividiert durch die abgelaufene Zeit.

#### Dynamisch (Durchnummerierung)

Die Kopiennummerierung, bei der eine Datei oder ein Ordner beim ersten Versuch gesichert oder archiviert wird, unabhängig davon, ob sie bzw. er sich bei der Sicherung oder Archivierung ändert. Siehe auch Gemeinsam dynamisch (Durchnummerierung), Gemeinsam statisch (Durchnummerierung), Statisch (Durchnummerierung).

## E

---

#### EA

Siehe Erweitertes Attribut.

#### EB

Siehe Exabyte.

#### EFS

Siehe Verschlüsseltes Dateisystem.

#### EFS (Encrypted File System - Verschlüsseltes Dateisystem)

Ein Dateisystem, das Verschlüsselung auf Dateisystemebene verwendet.

#### Einheitenklasse

Eine benannte Reihe von Merkmalen, die auf eine Gruppe von Speichereinheiten angewendet wird. Jede Einheitenklasse verfügt über einen eindeutigen Namen und stellt den Einheitentyp Platte, Datei, optische Platte oder Band dar.

#### Einheitenkonfigurationsdatei

1. Für einen Server eine Datei, die Informationen zu definierten Einheitenklassen und auf einigen Servern auch zu definierten Kassettenarchiven und Laufwerken enthält. Die Informationen sind eine Kopie der Einheitenkonfigurationsdaten in der Datenbank.
2. Für einen Speicheragenten eine Datei, die den Namen und das Kennwort des Speicheragenten sowie Informationen zu dem Server enthält, der die an ein SAN angeschlossenen Kassettenarchive und Laufwerke verwaltet, die der Speicheragent verwendet.

#### Einheitentyp FILE

Ein Einheitentyp, bei dem Dateien mit sequenziellem Zugriff auf Plattenspeicher als Datenträger verwendet werden.

#### Einheit zum Versetzen von Daten

Eine Einheit, die für den Server Daten versetzt. Ein NAS-Dateiserver (NAS - Network-Attached Storage) ist eine Einheit zum Versetzen von Daten.

#### Einschluss-/Ausschlussdatei

Eine Datei, die Anweisungen enthält, mit denen die zu sichernden Dateien und die zugeordneten Verwaltungsklassen bestimmt werden, die zum Sichern oder Archivieren verwendet werden sollen. Siehe auch Einschluss-/Ausschlussliste.

#### Einschluss-/Ausschlussliste

Eine Liste mit Optionen, die bestimmte Dateien für die Sicherung einschließen oder ausschließen. Eine Exclude-Option gibt Dateien an, die nicht gesichert werden sollen. Eine Include-Option gibt Dateien an, die von den Ausschlussregeln ausgeschlossen sind, oder ordnet einer Datei oder einer Dateigruppe eine Verwaltungsklasse für Sicherungs- oder Archivierungsservices zu. Siehe auch Einschluss-/Ausschlussdatei.

#### Empfänger

Ein Server-Repository, das ein Protokoll der Server- und Clientnachrichten als Ereignisse enthält. Ein Empfänger kann beispielsweise ein Dateiexit, Benutzerexit oder die Serverkonsole und das Aktivitätenprotokoll sein. Siehe auch Ereignis.

#### Empfangsbestätigung (Acknowledgment = ACK)

Das Senden von Empfangsbestätigungszeichen als positive Antwort auf eine Datenübertragung.

#### Ereignis

Ein Vorkommen mit Signifikanz für eine Task oder ein System. Ereignisse können die Beendigung oder das Fehlschlagen einer Operation, eine Benutzeraktion oder die Änderung des Status eines Prozesses einschließen. Siehe auch Unternehmensprotokollierung, Empfänger.

#### Ereignissatz

Ein Datenbanksatz, der den tatsächlichen Status und die Ergebnisse für Ereignisse beschreibt.

#### Ereignisserver

Ein Server, an den andere Server Ereignisse zum Protokollieren senden können. Der Ereignisserver leitet die Ereignisse an alle Empfänger weiter, die für die Ereignisse des sendenden Servers aktiviert sind.

#### Erneut binden

Allen gesicherten Versionen einer Datei einen neuen Verwaltungsklassennamen zuordnen. Beispielsweise wird eine Datei, die über eine aktive Sicherungsversion verfügt, erneut gebunden, wenn eine spätere Version der Datei mit einer anderen Verwaltungsklassenzuordnung gesichert wird. Siehe auch Binden, Verwaltungsklasse.

#### Erweitern

Den Teil des verfügbaren Speicherbereichs vergrößern, der zum Speichern von Datenbank- oder Wiederherstellungsprotokolldaten verwendet wird.

#### Erweitertes Attribut (EA)

Namen oder Wertepaare, die Dateien oder Verzeichnissen zugeordnet sind. Es gibt drei Klassen von erweiterten Attributen: Benutzerattribute, Systemattribute und Vertrauensattribute.

#### Exabyte (EB)

Für den Hauptspeicher, die realen und virtuellen Speicherkapazitäten und die Kanalkapazität 2 hoch 60 oder 1 152 921 504 606 846 976 Byte. Für die Plattenspeicher- und Übertragungskapazität 1 000 000 000 000 000 000 Byte.

#### Externes Kassettenarchiv

Eine Gruppe von Laufwerken, die von einem anderen Datenträgerverwaltungssystem als dem Speicherverwaltungssystem verwaltet wird.

## F

---

#### Fehlerprotokoll

Ein Datensatz oder eine Datei, der bzw. die zum Aufzeichnen von Fehlerinformationen zu einem Produkt oder System verwendet wird.

#### Fern

Bei Produkten für die hierarchische Speicherverwaltung bezieht sich der Begriff auf den Ursprung von umgelagerten Dateien, die versetzt werden. Siehe auch Lokal.

#### Festschreibungspunkt

Ein Zeitpunkt, zu dem Daten als konsistent angesehen werden.

#### File System Migrator (FSM)

Eine Kernelerweiterung, die alle Dateisystemoperationen abfängt und die erforderliche Speicherverwaltungsunterstützung bereitstellt. Ist keine Speicherverwaltungsunterstützung erforderlich, wird die Operation an das Betriebssystem weitergeleitet, das seine normalen Funktionen ausführt. Der File System Migrator wird über das Dateisystem angehängt, wenn dem Dateisystem die Speicherverwaltung hinzugefügt wird.

#### FSID

Siehe Dateibereichs-ID.

#### FSM

Siehe File System Migrator.

## G

---

#### GB

Siehe Gigabyte.

#### Geänderter Modus

Bei der Speicherverwaltung ein Modus der Sicherungskopiengruppe, der angibt, dass eine Datei oder ein Verzeichnis bei der Teilsicherung nur zu berücksichtigen ist, wenn sie bzw. es sich seit der letzten Sicherung geändert hat. Eine Datei oder ein Verzeichnis wird als geändert betrachtet, wenn sich das Datum, die Größe, der Eigner oder die Berechtigung geändert hat. Siehe auch Absoluter Modus, Modus.

#### Gemeinsam dynamisch (Durchnummerierung)

Ein Wert für die Durchnummerierung, der angibt, dass eine Datei nicht gesichert oder archiviert werden darf, wenn sie während der Operation gerade geändert wird. Der Client für Sichern/Archivieren versucht mehrmals, die Sicherungs- oder Archivierungsoperation zu wiederholen. Wenn die Datei bei jedem Versuch gerade geändert wird, sichert oder archiviert der Client für Sichern/Archivieren die Datei beim letzten Versuch. Siehe auch Dynamisch (Durchnummerierung), Durchnummerierung, Gemeinsam statisch (Durchnummerierung), Statisch (Durchnummerierung).

#### Gemeinsam genutztes Kassettenarchiv

Eine Kassettenarchivereinheit, die von mehreren Speicherverwaltungssystemen verwendet wird.

#### Gemeinsam statisch (Durchnummerierung)

Ein Durchnummerierungswert für die Kopiengruppe, der angibt, dass eine Datei während einer Sicherungs- oder Archivierungsoperation nicht geändert werden darf. Der Client versucht mehrmals, die Operation zu wiederholen. Ist die Datei bei jedem Versuch im Gebrauch, wird sie nicht gesichert oder archiviert. Siehe auch Dynamisch (Durchnummerierung), Durchnummerierung, Gemeinsam dynamisch (Durchnummerierung), Statisch (Durchnummerierung).

#### General Parallel File System (GPFS)

Ein leistungsfähiges Dateisystem für gemeinsam genutzte Platten, das den Knoten in einer Clustersystemumgebung Datenzugriff bereitstellen kann. Siehe auch Information Lifecycle Management.

#### Gesamtsicherung

Der Prozess, bei dem die gesamte Serverdatenbank gesichert wird. Eine Gesamtsicherung beginnt eine neue Datenbanksicherungsserie. Siehe auch Datenbanksicherungsserie, Datenbankmomentaufnahme, Teilsicherung.

#### Gesamtübertragungsrate

Eine Leistungsstatistik, die die durchschnittliche Anzahl der Byte angibt, die während der Verarbeitung einer bestimmten Operation pro Sekunde übertragen wurden.

#### Geschätzte Kapazität

Der verfügbare Speicherbereich eines Speicherpools in Megabyte.

#### Geschlossene Registrierung

Ein Registrierungsprozess, bei dem nur ein Administrator Workstations als Clientknoten beim Server registrieren kann. Siehe auch Offene Registrierung.

#### Geschützter Standort

Siehe Primärer Standort.

#### Gigabyte (GB)

Für den Hauptspeicher, den realen und virtuellen Speicher und die Kanalkapazität zwei hoch 30 oder 1.073.741.824 Byte. Für die Plattenspeicher- und Übertragungskapazität 1.000.000.000 Byte.

#### Global eindeutige ID (GUID)

Eine über einen Algorithmus ermittelte Nummer, die eine Entität innerhalb eines Systems eindeutig identifiziert. Siehe auch Universally Unique Identifier.

#### Global inaktiver Status

Der Status aller Dateisysteme, denen die Speicherverwaltung hinzugefügt wurde, wenn die Speicherverwaltung für einen Clientknoten global inaktiviert wird.

#### GPFS

Siehe General Parallel File System.

#### GPFS-Knotengruppe

Eine angehängte, definierte Gruppe von GPFS-Dateisystemen.

#### Grenzwert für Ladeanforderung

Die maximale Anzahl Datenträger, auf die von derselben Einheitenklasse gleichzeitig zugegriffen werden kann. Der Grenzwert für Ladeanforderungen legt die maximale Anzahl von Mountpunkten fest. Siehe auch Mountpunkt.

#### Größe der Stubdatei

Die Größe einer Datei, durch die eine Originaldatei in einem lokalen Dateisystem ersetzt wird, wenn sie in den Serverspeicher umgelagert wird. Die für Stubdateien angegebene Größe legt fest, wie viele Vorspanndaten in der Stubdatei gespeichert werden können. Der Standardwert für die Größe der Stubdatei ist die für ein Dateisystem definierte Blockgröße minus 1 Byte.

#### Gruppensicherung

Die Sicherung einer Gruppe, die eine Liste von Dateien aus einem oder mehreren Dateibereichen enthält.

#### GUID

Siehe Global eindeutige ID.

## H

---

#### Häufigkeit

Ein Kopiengruppenattribut, das das Mindestintervall zwischen Teilsicherungen in Tagen angibt.

#### Hierarchische Speicherverwaltung (HSM - Hierarchical Storage Management)

Eine Funktion, die Daten auf Platte, Band oder beidem automatisch verteilt und verwaltet. Dabei werden die Einheiten dieses Typs und potenzieller anderer Typen als Ebenen in einer Speicherhierarchie betrachtet, die von schnellen, kostenintensiven Einheiten bis hin zu langsameren, kostengünstigeren Einheiten und möglicherweise austauschbaren Einheiten reicht. Diese Funktion soll die Zugriffszeit auf Daten minimieren und die verfügbare Datenträgerkapazität maximieren. Siehe auch Client für hierarchische Speicherverwaltung, Rückruf, Speicherhierarchie.

#### HSM

Siehe Hierarchische Speicherverwaltung.

#### HSM-Client

Siehe Client für hierarchische Speicherverwaltung.

## I

---

#### IBM Spectrum Protect-Befehlsscript

Eine Folge von IBM Spectrum Protect-Verwaltungsbefehlen, die in der Datenbank des IBM Spectrum Protect-Servers gespeichert sind. Das Script kann von jeder Serverschnittstelle aus ausgeführt werden. Das Script kann Ersetzungen für Befehlsparameter und bedingte Logik enthalten. Siehe auch Makrodatei, Script.

#### ILM

Siehe Information Lifecycle Management.

## Image

Ein Dateisystem oder ein unformatierter logischer Datenträger, der als ein einziges Objekt gesichert wird.

## Imagesicherung

Die Sicherung eines gesamten Dateisystems oder eines unformatierten logischen Datenträgers als einzelnes Objekt.

## Inaktives Dateisystem

Ein Dateisystem, für das die Speicherverwaltung inaktiviert wurde. Siehe auch Aktives Dateisystem.

## Inaktive Version

Eine Sicherungsversion einer Datei, bei der es sich entweder nicht um die neueste Sicherungsversion handelt oder bei der es sich um eine Sicherungsversion einer Datei handelt, die nicht mehr im Clientsystem vorhanden ist. Inaktive Sicherungsversionen können entsprechend der Verwaltungsklasse, die der Datei zugeordnet wurde, für die Verfallsverarbeitung ausgewählt werden.

Siehe auch Aktive Version, Sicherungsversion.

## Information Lifecycle Management (ILM, Verwaltung von Daten über ihre gesamte Lebensdauer)

Ein auf Maßnahmen basierendes Dateiverwaltungssystem für Speicherpools und Dateigruppen. Siehe auch General Parallel File System.

## Inline-Datendeduplizierung

Eine Methode zum Reduzieren des Speicherbedarfs, indem redundante Daten entfernt werden. Die Daten werden dedupliziert, während sie in einen Containerspeicherpool geschrieben werden. Siehe auch Datendeduplizierung, Nachgeordnete Datendeduplizierung.

## Inline-Komprimierung

Eine Methode zum Reduzieren des Speicherbereichs. Sich wiederholende Zeichen, Leerzeichen, Zeichenfolgen oder Binärdaten werden entfernt, während Daten in einen Containerspeicherpool geschrieben werden. Siehe auch Komprimierung.

## IP-Adresse

Eine eindeutige Adresse für eine Einheit oder eine logische Einheit in einem Netz, die den IP-Standard (Internet Protocol) verwendet.

## J

---

## Jobdatei

Eine generierte Datei, die Konfigurationsdaten für einen Umlagerungsjob enthält. Die Datei weist das XML-Format auf und sie kann in der grafischen Benutzerschnittstelle des HSM for Windows-Clients (HSM = Hierarchical Storage Management = Hierarchische Speicherverwaltung) erstellt und editiert werden. Siehe auch Umlagerungsjob.

## Journaldämon

Auf AIX-, UNIX- oder Linux-Systemen ein Programm, das die Änderungsaktivität für Dateien verfolgt, die in Dateisystemen gespeichert sind.

## Journalgestützte Sicherung

Eine Methode zum Sichern von Windows-Clients und AIX-Clients, die den Mechanismus einer Datei für Änderungsbenachrichtigung nutzt. Dadurch wird die Leistung bei der Teilsicherung erhöht, da nicht das gesamte Dateisystem durchsucht werden muss.

## JournalService

Unter Microsoft Windows ein Programm, das die Änderungsaktivität für Dateien verfolgt, die in Dateisystemen gespeichert sind.

## K

---

## Kassettenarchiv

1. Ein Repository für beschriebene Speichermedien, die abgehängt werden können, wie Magnetplatten und Magnetbänder.
2. Eine Sammlung aus einem oder mehreren Laufwerken und eventuell ferngesteuerten Einheiten (je nach dem Typ des Kassettenarchivs), die für den Zugriff auf Speicherdatenträger verwendet werden kann.

## Kassettenarchivclient

Ein Server, der Server-zu-Server-Übertragung verwendet, um auf ein Kassettenarchiv zuzugreifen, das von einem anderen Speicherverwaltungsserver verwaltet wird. Siehe auch Kassettenarchivmanager.

## Kassettenarchivmanager

Ein Server, der Einheitenoperationen steuert, wenn mehrere Speicherverwaltungsserver eine Speichereinheit gemeinsam nutzen. Siehe auch Kassettenarchivclient.

## KB

Siehe Kilobyte.

## Kennwortgenerierung

Ein Prozess, der ein neues Kennwort erstellt und in einer verschlüsselten Kennwortdatei speichert, wenn das alte Kennwort abgelaufen ist. Die automatische Generierung eines Kennworts verhindert die Aufforderung zur Kennworteingabe.

## Kilobyte (KB)

Für den Hauptspeicher, den realen und virtuellen Speicher und die Kanalkapazität  $2 \text{ hoch } 10$  oder 1.024 Byte. Für die Plattenspeicher- und Übertragungskapazität 1.000 Byte.

## Knoten

Ein Dateiserver oder eine Workstation, auf dem bzw. der das Clientprogramm für Sichern/Archivieren installiert und beim Server registriert wurde.

#### Knotenberechtigungsklasse

Eine Berechtigungsklasse, die einem Administrator die Berechtigung für den Fernzugriff auf Clients für Sichern/Archivieren für einen bestimmten Clientknoten oder für alle Clients in einer Maßnahmendomäne erteilt. Siehe auch Berechtigungsklasse.

#### Knotenname

Ein eindeutiger Name, mit dem eine Workstation, ein Dateiserver oder ein PC für den Server identifiziert wird.

#### Kollokation

Der Prozess, alle Daten, die zu einem einzelnen Clientdateibereich, einem einzelnen Clientknoten oder einer Gruppe von Clientknoten gehören, auf einer minimalen Anzahl Datenträger mit sequenziellem Zugriff innerhalb eines Speicherpools aufzubewahren. Die Kollokation kann die Anzahl der Datenträger reduzieren, auf die beim Zurückschreiben einer großen Datenmenge zugegriffen werden muss.

#### Kollokationsgruppe

Eine benutzerdefinierte Gruppe von Clientknoten, deren Daten über den Kollokationsprozess auf einer minimalen Anzahl von Datenträgern gespeichert werden.

#### Komprimierung

Eine Funktion, die sich wiederholende Zeichen, Leerzeichen, Zeichenfolgen oder Binärdaten in den Daten, die verarbeitet werden, entfernt und Zeichen durch Steuerzeichen ersetzt. Durch Komprimierung wird der Speicherbereich reduziert, der für Daten erforderlich ist. Siehe auch Inline-Komprimierung.

#### Konfigurationsmanager

Ein Server, der an verwaltete Server Konfigurationsdaten wie Maßnahmen und Zeitpläne entsprechend den Profilen der Server verteilt. Konfigurationsdaten können Maßnahmen und Zeitpläne umfassen. Siehe auch Unternehmenskonfiguration, Verwalteter Server, Profil.

#### Kopie mit grober Übereinstimmung

Eine Sicherungsversion oder Archivierungskopie einer Datei, die möglicherweise nicht genau dem Originalinhalt der Datei entspricht, da die Datei während der Sicherung oder Archivierung geändert wurde.

#### Kopiengruppe

Ein Maßnahmenobjekt, das Attribute enthält, die Folgendes steuern: wie Sicherungsversionen oder Archivierungskopien generiert werden, an welcher Position Sicherungsversionen oder Archivierungskopien sich ursprünglich befinden und wann Sicherungsversionen oder Archivierungskopien verfallen. Eine Kopiengruppe gehört zu einer Verwaltungsklasse. Siehe auch Archivierungskopiengruppe, Sicherungskopiengruppe, Sicherungsversion, Verwaltungsklasse.

#### Kopiensicherung

Eine vollständige Sicherung, bei der die Transaktionsprotokolldateien nicht gelöscht werden, um Auswirkungen auf Sicherungsprozeduren mit Teilsicherungen oder Differenzsicherungen zu vermeiden.

#### Kopienspeicherpool

Eine benannte Gruppe von Datenträgern, die Kopien von Dateien enthalten, die sich in primären Speicherpools befinden. Kopienspeicherpools werden ausschließlich verwendet, um die Daten zu sichern, die in primären Speicherpools gespeichert sind. Ein Kopienspeicherpool kann kein Zielort für eine Sicherungskopiengruppe, eine Archivierungskopiengruppe oder eine Verwaltungsklasse (für speicherverwaltete Dateien) sein. Siehe auch Ziel, Primärer Speicherpool, Serverspeicher, Speicherpool, Speicherpoolatenträger.

## L

#### Ladedauer

Die maximale Anzahl Minuten, die ein Server einen angehängten Datenträger mit sequenziellem Zugriff, der nicht verwendet wird, aufbewahrt, bevor der Datenträger mit sequenziellem Zugriff abgehängt wird.

#### LAN

Siehe Lokales Netz.

#### LAN-unabhängige Datenübertragung

Siehe LAN-unabhängige Datenversetzung.

#### LAN-unabhängige Datenversetzung

Die Versetzung von Clientdaten zwischen einem Clientsystem und einer Speichereinheit in einem Speicherbereichsnetz (Storage Area Network - SAN) unter Umgehung des lokalen Netzes.

#### LOFS

Siehe Loopback Virtual File System.

#### Logical Volume Snapshot Agent (LVSA)

Software, die als Momentaufnahme-Provider fungieren kann, um während einer Online-Imagesicherung eine Momentaufnahme eines logischen Datenträgers zu erstellen.

#### Logische Belegung

Der Speicherbereich, der in einem Speicherpool durch logische Dateien belegt ist. Dieser Speicherbereich umfasst nicht den freien Speicherplatz, der entsteht, wenn logische Dateien aus Aggregatdateien gelöscht werden. Daher kann die logische Belegung geringer als die physische Belegung sein. Siehe auch Physische Belegung.

#### Logische Datei

Eine Datei, die entweder alleine oder als Teil eines Aggregats in einem oder mehreren Serverspeicherpools gespeichert ist. Siehe auch Aggregat, Physische Datei, Physische Belegung.

## Logischer Datenträger

Ein Teil eines physischen Datenträgers, der ein Dateisystem enthält.

## Lokal

1. Bezieht sich auf eine Einheit, eine Datei oder ein System, auf das von einem Benutzersystem aus direkt, ohne DFV-Leitung, zugegriffen wird.
2. Bei Produkten für die hierarchische Speicherverwaltung bezieht sich der Begriff auf das Ziel von umgelagerten Dateien, die versetzt werden. Siehe auch Fern.

## Lokaler Spiegeldatenträger

Daten, die auf Spiegeldatenträgern gespeichert werden, die zu einem Plattenspeichersubsystem gehören.

## Lokales Netz (LAN)

Ein Netz, das mehrere Einheiten in einem begrenzten Gebiet (z. B. in einem einzigen Gebäude oder in mehreren benachbarten Gebäuden) verbindet und das mit einem größeren Netz verbunden werden kann.

## Loopback Virtual File System (LOFS)

Ein Dateisystem, das durch Anhängen eines Verzeichnisses über ein anderes lokales Verzeichnis erstellt wird; auch als "Mount-Over-Mount" bezeichnet. Ein LOFS kann auch mit Hilfe eines automatischen Mountprogramms generiert werden.

## LUN

Siehe Nummer der logischen Einheit.

## LVSA

Siehe Logical Volume Snapshot Agent.

## M

---

## Mailboxzurückschreibung

Eine Funktion, die Microsoft Exchange Server-Daten (aus IBM Data Protection for Microsoft Exchange-Sicherungen) auf der Mailboxebene oder auf der Mailboxelementebene zurückschreibt.

## Makrodatei

Eine Datei, die einen oder mehrere IBM Spectrum Protect-Verwaltungsbefehle enthält und die nur auf einem Verwaltungsclient mit dem Befehl MACRO ausgeführt werden kann. Siehe auch IBM Spectrum Protect-Befehlsscript.

## Maßnahmenberechtigungsklasse

Eine Berechtigungsklasse, die einem Administrator die Berechtigung für folgende Tasks erteilt: Maßnahmenobjekte verwalten, Clientknoten registrieren und Clientoperationen für Clientknoten planen. Die Berechtigung kann auf bestimmte Maßnahmendomänen beschränkt sein. Siehe auch Berechtigungsklasse.

## Maßnahmendomäne

Eine Gruppierung von Maßnahmenbenutzern mit einer oder mit mehreren Maßnahmengruppen, die Daten oder Speicherressourcen für die Benutzer verwalten. Die Benutzer sind Clientknoten, die der Maßnahmendomäne zugeordnet sind. Siehe auch Aktive Maßnahmengruppe, Domäne.

## Maßnahmengruppe

Eine Gruppe von Regeln in einer Maßnahmendomäne. Die Regeln geben an, wie Daten oder Speicherressourcen für Clientknoten in der Maßnahmendomäne automatisch verwaltet werden. Regeln können in Verwaltungsklassen enthalten sein. Siehe auch Aktive Maßnahmengruppe, Verwaltungsklasse.

## Maximale Übertragungseinheit (MTU)

Der größte Block, der auf einem bestimmten physischen Medium in einem einzigen Frame gesendet werden kann. Beispielsweise beträgt die maximale Übertragungseinheit für Ethernet 1500 Byte.

## MB

Siehe Megabyte.

## Media-Server

In einer z/OS-Umgebung ein Programm, das Zugriff auf z/OS-Platten- und -Bandeinheitenspeicher für IBM Spectrum Protect-Server bereitstellt, die auf anderen Betriebssystemen als z/OS ausgeführt werden.

## Megabyte (MB)

Für den Hauptspeicher, den realen und virtuellen Speicher und die Kanalkapazität  $2 \text{ hoch } 20$  oder 1.048.576 Byte. Für die Plattenspeicher- und Übertragungskapazität 1.000.000 Byte.

## Metadaten

Daten, die die Merkmale von Daten beschreiben; beschreibende Daten.

## Modus

Ein Kopiengruppenattribut, das angibt, ob eine Datei gesichert werden soll, die seit der letzten Sicherung nicht mehr geändert wurde. Siehe auch Absoluter Modus, Geänderter Modus.

## Momentaufnahme

Ein Imagesicherungstyp, der aus einer zeitpunktgesteuerten Sicht eines Datenträgers besteht.

## Mountpunkt

Ein logisches Laufwerk, über das auf Datenträger in einer Einheitenklasse für den sequenziellen Zugriff zugegriffen wird. Für Einheitentypen für austauschbare Datenträger wie z. B. ein Band ist der Mountpunkt ein logisches Laufwerk, das einem physischen Laufwerk zugeordnet ist. Für den Einheitentyp FILE ist ein Mountpunkt ein logisches Laufwerk, das einem Ein-/Ausgabedatenstrom zugeordnet ist. Siehe auch Grenzwert für Ladeanforderung.

MTU

Siehe Maximale Übertragungseinheit.

## N

---

Nachgeordnete Datendeduplizierung

Eine Methode zum Reduzieren des Speicherbedarfs, indem redundante Daten entfernt werden. Die Daten werden zuerst in den Speicherpool geschrieben, die doppelten Daten werden identifiziert und dann wird der Speicherbereich im Speicherpool konsolidiert. Siehe auch Datendeduplizierung, Inline-Datendeduplizierung.

Nagle-Algorithmus

Ein Algorithmus, der Engpässe in TCP/IP-Netzen reduziert, indem er kleinere Pakete zusammenfasst und gemeinsam sendet.

NAS-Dateiserver

Siehe Network Attached Storage-Dateiserver.

NAS-Dateiserverknoten

Siehe NAS-Knoten.

NAS-Knoten

Ein Clientknoten, der ein NAS-Dateiserver ist. Die Daten für den NAS-Knoten werden von einem NAS-Dateiserver übertragen, der vom Protokoll NDMP (Network Data Management Protocol) gesteuert wird. Ein NAS-Knoten wird auch als NAS-Dateiserverknoten bezeichnet.

Natives Dateisystem

Ein Dateisystem, das dem Dateiserver lokal und nicht für die Speicherverwaltung hinzugefügt wird. Der HSM-Client (Hierarchical Storage Manager - hierarchische Speicherverwaltung) stellt keine Speicherverwaltungsservices für das Dateisystem bereit.

Natives Format

Ein Datenformat, das vom Server direkt in einen Speicherpool geschrieben wird. Siehe auch Nicht natives Datenformat.

NDMP

Siehe Network Data Management Protocol.

NetBIOS (Network Basic Input/Output System)

Eine Standardschnittstelle für Netze und Personal Computer, die in lokalen Netzen verwendet wird, um Funktionen für Nachrichten, Druckserver und Dateiserver bereitzustellen. Anwendungsprogramme, die NetBIOS verwenden, müssen sich nicht mit den Details von Protokollen für die LAN-Datenübertragungssteuerung (Data Link Control - DLC) beschäftigen.

Network Attached Storage-Dateiserver (NAS-Dateiserver)

Eine dedizierte Speichereinheit mit einem Betriebssystem, das für Dateiserverfunktionen optimiert ist. Ein NAS-Dateiserver kann sowohl die Merkmale eines Knotens als auch die Merkmale einer Einheit zum Versetzen von Daten aufweisen.

Network Basic Input/Output System

Siehe NetBIOS.

Network Data Management Protocol (NDMP)

Ein Protokoll, mit dem eine Netzspeicherverwaltungsanwendung die Sicherung und Wiederherstellung eines NDMP-kompatiblen Dateiservers steuern kann, ohne dass eine spezielle Software auf diesem Dateiserver installiert werden muss.

Nicht natives Datenformat

Ein in den Speicherpool geschriebenes Datenformat, das sich von dem Format unterscheidet, das der Server für Operationen verwendet. Siehe auch Natives Format.

Nummer der logischen Einheit (Logical Unit Number - LUN)

Im SCSI-Standard (Small Computer System Interface) eine eindeutige Kennung, die für die Unterscheidung von Einheiten verwendet wird. Jede dieser Einheiten ist eine logische Einheit (Logical Unit - LU).

## O

---

Offene Registrierung

Ein Registrierungsprozess, bei dem Benutzer ihre Workstations als Clientknoten beim Server registrieren können. Siehe auch Geschlossene Registrierung.

Offlinedatenträgersicherung

Eine Sicherung, bei der der Datenträger gesperrt ist, so dass andere Systemanwendungen während der Sicherungsoperation nicht auf ihn zugreifen können.

Onlinedatenträgersicherung

Eine Sicherung, bei der der Datenträger während der Sicherungsoperation für andere Systemanwendungen verfügbar ist.

Optionsdatei

Eine Datei, die Verarbeitungsoptionen enthält. Siehe auch Clientsystemoptionsdatei, Clientbenutzeroptionsdatei.

## P

---

Paket

Bei der Datenübertragung eine Folge von Binärziffern einschließlich Daten und Steuersignalen, die als Einheit übertragen und weitergeleitet werden.

Partieller Dateirückruf (Rückrufmodus)

Ein Rückrufmodus, bei dem die Funktion für hierarchische Speicherverwaltung (HSM-Funktion) nur denjenigen Teil einer umgelagerten Datei aus dem Speicher liest, den die auf die Datei zugreifende Anwendung anfordert.

#### Pfad

Ein Objekt, das eine Eins-zu-eins-Beziehung zwischen einer Quelle und einem Ziel definiert. Die Quelle greift unter Verwendung des Pfads auf das Ziel zu. Daten können von der Quelle zum Ziel und zurück fließen. Ein Beispiel für eine Quelle ist eine Einheit zum Versetzen von Daten (wie ein NAS-Dateiserver) und ein Beispiel für ein Ziel ist ein Bandlaufwerk.

#### Physische Belegung

Der Speicherbereich, der in einem Speicherpool durch physische Dateien belegt ist. Dieser Speicherbereich umfasst den freien Speicherplatz, der entsteht, wenn logische Dateien aus Aggregaten gelöscht werden. Siehe auch Logische Datei, Logische Belegung, Physische Datei.

#### Physische Datei

Eine Datei, die in einem oder mehreren Speicherpools gespeichert ist und entweder aus einer einzigen logischen Datei oder aus einer Gruppe von logischen Dateien besteht, die in einem Aggregat zusammengefasst sind. Siehe auch Aggregat, Logische Datei, Physische Belegung.

#### Planungsmodus

Der Typ der Planungsoperation für Server und Clientknoten. Zwei Planungsmodi werden unterstützt: Clientsendeaufruf und Serversystemanfrage.

#### Platzhalterzeichen

Ein Sonderzeichen wie ein Stern (\*) oder ein Fragezeichen (?), das verwendet werden kann, um ein oder mehrere Zeichen darzustellen. Das Platzhalterzeichen kann durch ein beliebiges Zeichen oder eine Gruppe von beliebigen Zeichen ersetzt werden.

#### Plug-in

Ein separat installierbares Softwaremodul, das einem vorhandenen Programm, einer Anwendung oder einer Schnittstelle Funktionen hinzufügt.

#### Pool für aktive Daten

Eine benannte Gruppe von Speicherpooldatenträgern, die nur aktive Versionen von Clientsicherungsdaten enthält. Siehe auch Serverspeicher, Speicherpool, Speicherpooldatenträger.

#### Präfix für Banddatenträger

Das übergeordnete Qualifikationsmerkmal des Namens der Datei oder des Datensatzes im Standardbandkennsatz.

#### Primärer Speicherpool

Eine benannte Gruppe von Datenträgern oder Containern, die der Server verwendet, um Sicherungsversionen und Archivierungskopien von Dateien sowie von Clientknoten umgelagerte Dateien zu speichern. Siehe auch Kopienspeicherpool, Serverspeicher, Speicherpool, Speicherpooldatenträger.

#### Primärer Standort

Ein physischer oder virtueller Standort, der aus Hardware-, Netz- und Speicherressourcen besteht. Normalerweise werden Produktionsoperationen am primären Standort ausgeführt. Daten können für die Wiederherstellung nach einem Katastrophenfall und Übernahmeoperationen auf einen sekundären Standort repliziert werden. Siehe auch Sekundärer Standort.

#### Profil

Eine benannte Gruppe aus Konfigurationsdaten, die von einem Konfigurationsmanager verteilt werden kann, wenn ein verwalteter Server eine Subskription vornimmt. Die Konfigurationsdaten können registrierte Administrator-IDs, Maßnahmen, Clientzeitpläne, Clientoptionsgruppen, Verwaltungszeitpläne, Befehlsprozeduren des Speichermanagers, Serverdefinitionen und Servergruppenelemente umfassen. Siehe auch Konfigurationsmanager, Unternehmenskonfiguration, Verwalteter Server.

#### Profilzuordnung

Auf einem Konfigurationsmanager die definierte Beziehung zwischen einem Profil und einem Objekt wie einer Maßnahmendomäne. Profilzuordnungen definieren die Konfigurationsdaten, die einem verwalteten Server zugeteilt werden, wenn er das Profil subskribiert.

#### Prüfen

Die Maßnahmengruppe auf Bedingungen hin prüfen, die unter Umständen Probleme verursachen könnten, wenn die betreffende Maßnahmengruppe zur aktiven Maßnahmengruppe gemacht würde. Bei der Prüfung wird beispielsweise geprüft, ob die Maßnahmengruppe eine Standardverwaltungsklasse enthält.

#### Prüfung

Die Suche nach logischen Inkonsistenzen zwischen Informationen auf dem Server und den tatsächlich auf dem System vorliegenden Gegebenheiten. Der Speichermanager kann Informationen zu Elementen wie Datenträgern, Kassettenarchiven und Lizenzen prüfen. Wenn ein Speichermanager beispielsweise einen Datenträger prüft, stellt der Server Inkonsistenzen zwischen den in der Datenbank gespeicherten Informationen zu gesicherten oder archivierten Dateien und den tatsächlichen Daten fest, die jeder Sicherungsversion oder Archivierungskopie im Serverspeicher zugeordnet sind.



#### Quote

1. Für HSM auf AIX-, UNIX- oder Linux-Systemen der Grenzwert (in Megabyte) für das Datenvolumen, das von einem Dateisystem in den Serverspeicher umgelagert oder vorumgelagert werden kann.
2. Für HSM auf Windows-Systemen ein benutzerdefinierter Grenzwert für den Speicherbereich, der von zurückgerufenen Dateien belegt wird.



## R

---

### Registrieren

Einen Clientknoten oder eine Administrator-ID definieren, der bzw. die auf den Server zugreifen kann.

### Registry

Ein Repository, das Zugriffs- und Konfigurationsdaten für Benutzer, Systeme und Software enthält.

### Residente Datei

Auf einem Windows-System eine vollständige Datei in einem lokalen Dateisystem, bei der es sich auch um eine umgelagerte Datei handeln könnte, da eine umgelagerte Kopie im Serverspeicher vorhanden sein kann. Auf einem UNIX- oder Linux-System eine vollständige Datei in einem lokalen Dateisystem, die nicht umgelagert oder vorumgelagert wurde oder die aus dem Serverspeicher zurückgerufen und geändert wurde.

### Ressourcennutzung in Sitzung

Die Wartezeit, die Prozessorzeit und der Speicherbereich, die während einer Clientsitzung verwendet oder abgerufen werden.

### Root

Ein Systembenutzer, dessen Berechtigungen keinen Einschränkungen unterliegen. Ein Root verfügt über besondere Rechte und Berechtigungen, die für die Ausführung von Verwaltungstasks erforderlich sind.

### Rückruf

Das Zurückkopieren einer umgelagerten Datei aus dem Serverspeicher in das ursprüngliche Dateisystem mit Hilfe des Clients für hierarchische Speicherverwaltung. Siehe auch Selektiver Rückruf.

## S

---

### SAN

Siehe Speicherbereichsnetz.

### Schwellenumlagerung

Der Prozess, bei dem Dateien aus einem lokalen Dateisystem in den Serverspeicher versetzt werden, basierend auf den Werten für die obere und untere Schwelle, die für das Dateisystem definiert wurden. Siehe auch Automatische Umlagerung, Bedarfsumlagerung, Umlagerungsjob, Selektive Umlagerung.

### Script

Eine Serie von Befehlen, die in einer Datei enthalten sind und die eine bestimmte Funktion ausführen, wenn die Datei ausgeführt wird. Scripts werden bei ihrer Ausführung interpretiert. Siehe auch IBM Spectrum Protect-Befehlsscript.

### Secure Sockets Layer (SSL)

Ein Sicherheitsprotokoll, das Daten bei der Übertragung schützt. Mit SSL können Client/Server-Anwendungen miteinander kommunizieren, ohne dass die Daten ausspioniert oder manipuliert und Nachrichten gefälscht werden können.

### Seite

Eine definierte Einheit des Speicherbereichs in einem Speichermedium oder innerhalb eines Datenbankdatenträgers.

### Sekundärer Standort

Ein physischer oder virtueller Standort, der aus den Hardware-, Netz- und Speicherressourcen besteht, die die Wiederherstellungsanforderungen des primären Standorts unterstützen. Wenn ein Fehler an dem primären Standort auftritt, können Operationen am sekundären Standort fortgesetzt werden. Siehe auch Primärer Standort.

### Selektiver Rückruf

Der Prozess, bei dem vom Benutzer ausgewählte Dateien aus dem Serverspeicher in ein lokales Dateisystem kopiert werden. Siehe auch Rückruf, Transparenter Rückruf.

### Selektive Sicherung

Der Prozess der Sicherung bestimmter Dateien oder Verzeichnisse in einer Clientdomäne. Gesichert werden dabei die Dateien, die in der Einschluss-/Ausschlussliste nicht ausgeschlossen sind. Die Dateien müssen den Anforderungen bezüglich der Durchnummerierung in der Sicherungskopiengruppe der Verwaltungsklasse entsprechen, die jeder Datei zugeordnet ist. Siehe auch Teilsicherung.

### Selektive Umlagerung

Der Prozess, bei dem vom Benutzer ausgewählte Dateien aus einem lokalen Dateisystem in den Serverspeicher kopiert und die Dateien in dem lokalen Dateisystem durch Stubdateien ersetzt werden. Siehe auch Bedarfsumlagerung, Schwellenumlagerung.

### Server

Ein Softwareprogramm oder ein Computer, das bzw. der Services für andere Softwareprogramme oder Computer zur Verfügung stellt. Siehe auch Client.

### Serveroptionsdatei

Eine Datei mit Einstellungen, die verschiedene Serveroperationen steuern. Diese Einstellungen betreffen Aspekte wie Datenübertragung, Einheiten und Leistung.

### Serverspeicher

Die primären Speicherpools, Kopierspeicherpools und Speicherpools für aktive Daten, die der Server verwendet, um Benutzerdateien wie Sicherungsversionen, Archivierungskopien und von Clientknoten für hierarchische Speicherverwaltung umgelagerte Dateien (speicherverwaltete Dateien) zu speichern. Siehe auch Pool für aktive Daten, Containerspeicherpool, Kopierspeicherpool, Primärer Speicherpool, Speicherpoolatdatenträger, Datenträger.

### Sicherung logischer Datenträger

Die Sicherung eines Dateisystems oder logischen Datenträgers als einzelnes Objekt.

- Sicherung mit grober Übereinstimmung**  
Eine Sicherungsversion einer Datei, die möglicherweise nicht genau dem Stand der aktuellen Datei entspricht, da die Datei während der Sicherung geändert wurde.
- Sicherungsgruppe**  
Eine übertragbare, konsolidierte Gruppe von aktiven Versionen von Sicherungsdateien, die für einen Client für Sichern/Archivieren generiert werden.
- Sicherungsgruppensammlung**  
Eine Gruppe von Sicherungsgruppen, die zu demselben Zeitpunkt generiert werden und die über dieselben Sicherungsgruppennamen, Datenträgernamen, Beschreibungen und Einheitenklassen verfügen. Der Server identifiziert jede Sicherungsgruppe in der Sammlung über seinen Knotennamen, Sicherungsgruppennamen und Dateityp.
- Sicherungskopiengruppe**  
Ein Maßnahmenobjekt mit Attributen, die die Generierung, den Zielort und den Verfallstermin von Sicherungsversionen von Dateien steuern. Eine Sicherungskopiengruppe gehört zu einer Verwaltungsklasse. Siehe auch Kopiengruppe.
- Sicherungsversion**  
Eine Datei oder ein Verzeichnis, die bzw. das ein Clientknoten im Speicher gesichert hat. Es können mehrere Sicherungsversionen im Speicher vorhanden sein, aber nur eine Sicherungsversion ist die aktive Version. Siehe auch Aktive Version, Kopiengruppe, Inaktive Version.
- Sitzung**  
Eine logische oder virtuelle Verbindung zwischen zwei Stationen, Softwareprogrammen oder Einheiten in einem Netz, über die die beiden Elemente für die Dauer der Sitzung miteinander kommunizieren und Daten austauschen können. Siehe auch Verwaltungssitzung.
- Speicheragent**  
Ein Programm, das die direkte Sicherung von Clientdaten in Speichereinheiten und die direkte Wiederherstellung von Clientdaten aus Speichereinheiten ermöglicht, die mit einem Speicherbereichsnetz (SAN - Storage Area Network) verbunden sind.
- Speicherberechtigungsklasse**  
Eine Berechtigungsklasse, die einem Administrator die Berechtigung erteilt, die Zuordnung und Verwendung der Speicherressourcen für den Server zu steuern. Siehe auch Berechtigungsklasse.
- Speicherbereich**  
Der Teil einer Datei, der während des Datenduplizierungsprozesses erstellt wird. Speicherbereiche werden mit anderen Dateibereichen verglichen, um doppelte Daten zu identifizieren.
- Speicherbereichsnetz (SAN)**  
Ein dediziertes Speichernetz, das an eine bestimmte Umgebung angepasst ist und das Server, Systeme, Speicherprodukte, Netzprodukte, Software und Services kombiniert.
- Speicherhierarchie**  
Eine logische Reihenfolge von primären Speicherpools, die von einem Administrator definiert wurde. Die Reihenfolge basiert normalerweise auf der Geschwindigkeit und der Kapazität der Einheiten, die die Speicherpools verwenden. Die Speicherhierarchie wird durch Angabe des nächsten Speicherpools in einer Speicherpooldefinition definiert. Siehe auch Speicherpool.
- Speichermonitordämon**  
Ein Dämon, der die Speicherbereichsbelegung in allen Dateisystemen überprüft, für die die Speicherverwaltung aktiv ist, und der die Schwellenumlagerung automatisch startet, wenn die Speicherbereichsbelegung in einem Dateisystem die obere Schwelle erreicht oder überschreitet.
- Speicherpool**  
Eine Gruppe von Speicherdatenträgern oder Containern, die der Zielort für das Speichern von Clientdaten sind. Siehe auch Pool für aktive Daten, Cloud-Containerspeicherpool, Kopierspeicherpool, Verzeichniscontainerspeicherpool, Primärer Speicherpool, Speicherhierarchie.
- Speicherpooldatenträger**  
Ein Datenträger, der einem Speicherpool zugeordnet wurde. Siehe auch Pool für aktive Daten, Kopierspeicherpool, Primärer Speicherpool, Serverspeicher, Datenträger.
- Speicherverwaltete Datei**  
Eine Datei, die der HSM-Client (HSM = Hierarchical Storage Management = Hierarchische Speicherverwaltung) von einem Clientknoten umlagert. Der HSM-Client ruft die Datei bei Bedarf in den Clientknoten zurück.
- Speicherverwaltung**  
Siehe Hierarchische Speicherverwaltung.
- Spezielle Datei**  
Auf AIX-, UNIX- oder Linux-Systemen eine Datei, die Einheiten für das System definiert, oder temporäre Dateien, die von Prozessen erstellt werden. Man unterscheidet drei Grundtypen von speziellen Dateien: First In/First Out (FIFO), Block und Zeichen.
- Spiegeldatenträger**  
Die Daten, die aus einer Momentaufnahme eines Datenträgers gespeichert wurden. Die Momentaufnahme kann erstellt werden, während Anwendungen auf dem System weiterhin Daten auf die Datenträger schreiben.
- Spiegelkopie**  
Eine Momentaufnahme eines Datenträgers. Die Momentaufnahme kann erstellt werden, während Anwendungen auf dem System weiterhin Daten auf die Datenträger schreiben.
- Spiegeln**

Der Prozess, bei dem dieselben Daten gleichzeitig auf mehrere Platten geschrieben werden. Die Spiegelung von Daten bietet Schutz vor Datenverlust in der Datenbank oder im Wiederherstellungsprotokoll.

#### SSL

Siehe Secure Sockets Layer.

#### Stabilisierter Dateibereich

Ein Dateibereich, der auf dem Server, jedoch nicht auf dem Client vorhanden ist.

#### Standardverwaltungsklasse

Eine Verwaltungsklasse, die einer Maßnahmengruppe zugeordnet ist. Diese Klasse wird zum Verwalten von gesicherten oder archivierten Dateien verwendet, wenn eine Datei nicht explizit über die Einschluss-/Ausschlussliste einer bestimmten Verwaltungsklasse zugeordnet ist.

#### Startfenster

Eine Zeitspanne, während der ein Zeitplan eingeleitet werden muss.

#### Statisch (Durchnummerierung)

Ein Durchnummerierungswert für die Kopiengruppe, der angibt, dass eine Datei während einer Sicherungs- oder Archivierungsoperation nicht geändert werden darf. Ist die Datei beim ersten Versuch im Gebrauch, kann der Client für Sichern/Archivieren die Datei nicht sichern oder archivieren. Siehe auch Dynamisch (Durchnummerierung), Durchnummerierung, Gemeinsam dynamisch (Durchnummerierung), Gemeinsam statisch (Durchnummerierung).

#### Stub

Eine Verknüpfung im Windows-Dateisystem, die vom HSM-Client (HSM = Hierarchical Storage Management = Hierarchische Speicherverwaltung) für eine umgelagerte Datei generiert wird. Diese Verknüpfung ermöglicht den transparenten Benutzerzugriff. Ein Stub ist die Darstellung einer umgelagerten Datei als Datei mit freien Bereichen, der ein Analysepunkt zugeordnet ist.

#### Stubdatei

Eine Datei, die die Originaldatei in einem lokalen Dateisystem ersetzt, wenn die Datei in den Speicher umgelagert wird. Eine Stubdatei enthält die Informationen, die erforderlich sind, um eine umgelagerte Datei aus dem Serverspeicher zurückzurufen. Sie enthält darüber hinaus weitere Informationen, die möglicherweise verwendet werden können, anstatt die umgelagerte Datei zurückzurufen. Siehe auch Umgelagerte Datei, Residente Datei.

#### Stubdatei ohne Verbindung

Eine Datei, für die keine umgelagerte Datei auf dem Server gefunden wird, von dem der Clientknoten Speicherverwaltungsservices anfordert. Eine Stubdatei kann beispielsweise zu einer Stubdatei ohne Verbindung werden, wenn die Optionsdatei des Clientsystems so geändert wird, dass ein anderer Server kontaktiert wird als der Server, auf den die Datei umgelagert wurde.

#### Subskription

In einer Speicherumgebung der Prozess der Identifizierung der Subskribenten, an die die Profile verteilt werden. Siehe auch Unternehmenskonfiguration, Verwalteter Server.

#### Systemberechtigungsklasse

Eine Berechtigungsklasse, die einem Administrator die Berechtigung für das Ausgeben aller Serverbefehle erteilt. Siehe auch Berechtigungsklasse.

## T

---

#### TCA

Siehe Trusted Communications Agent.

#### TCP/IP

Siehe Transmission Control Protocol/Internet Protocol.

#### Teilsicherung

Der Prozess, bei dem Dateien oder Verzeichnisse gesichert oder Seiten in die Datenbank kopiert werden, die seit der letzten Gesamt- oder Teilsicherung hinzugefügt oder geändert wurden. Siehe auch Selektive Sicherung.

#### Tombstoneobjekt

Eine kleine Untergruppe von Attributen eines gelöschten Objekts. Das Tombstoneobjekt wird für einen angegebenen Zeitraum aufbewahrt und am Ende des angegebenen Zeitraums permanent gelöscht.

#### Transmission Control Protocol/Internet Protocol (TCP/IP)

Eine standardisierte, nicht proprietäre Gruppe von Übertragungsprotokollen, die zuverlässige End-to-End-Verbindungen zwischen Anwendungen über miteinander verbundene Netze verschiedenen Typs zur Verfügung stellt. Siehe auch Übertragungsmethode.

#### Transparenter Rückruf

Der Prozess, mit dem eine umgelagerte Datei automatisch auf eine Workstation oder einen Dateiserver zurückgerufen wird, wenn auf die Datei zugegriffen wird. Siehe auch Selektiver Rückruf.

#### Trusted Communications Agent (TCA)

Ein Programm, das das Anmeldekennwortprotokoll bearbeitet, wenn Clients die Kennwortgenerierung verwenden.

## U

---

#### Übertragungsmethode

Die Methode, mit der ein Client und Server Daten austauschen. Siehe auch Transmission Control Protocol/Internet Protocol.

#### Übertragungsprotokoll

Eine Gruppe definierter Schnittstellen, über die Computer miteinander kommunizieren können.

## UCS-2

Ein Schema für Codeumsetzung in 2 Byte (16 Bit), das auf der ISO/IEC-Spezifikation 10646-1 basiert. UCS-2 definiert drei Implementierungsebenen: Ebene 1 - Kombination codierter Elemente ist nicht zulässig; Ebene 2 - Kombination codierter Elemente ist nur für die Sprachen Thailändisch, Indoisch, Hebräisch und Arabisch zulässig; Ebene 3 - Jede Kombination codierter Elemente ist zulässig.

## Umgelagerte Datei

Eine Datei, die aus einem lokalen Dateisystem in den Speicher kopiert wurde. Für HSM-Clients auf UNIX- oder Linux-Systemen wird die Datei durch eine Stubdatei im lokalen Dateisystem ersetzt. Unter Windows ist die Erstellung einer Stubdatei optional. Siehe auch Dateistatus, Vorumgelagerte Datei, Residente Datei, Stubdatei.

## Umlagern

Daten an eine andere Position oder eine Anwendung auf ein anderes Computersystem versetzen.

## Umlagerung

Der Prozess, bei dem Daten von einem Computersystem auf ein anderes Computersystem versetzt werden oder eine Anwendung auf ein anderes Computersystem versetzt wird.

## Umlagerungsjob

Eine Spezifikation der umzulagernden Dateien und der Aktionen, die nach der Umlagerung mit den Originaldateien auszuführen sind. Siehe auch Jobdatei, Schwellenumlagerung.

## Umlagerungsschwelle

Ein hoher und ein niedriger Wert für die Kapazität von Speicherpools oder Dateisystemen, ausgedrückt in Prozentsätzen. Diese Werte legen fest, wann die Umlagerung gestartet und gestoppt wird.

## UNC

Siehe Universal Naming Convention.

## Unformatierter logischer Datenträger

Ein Bereich eines physischen Datenträgers, der aus nicht zugeordneten Blöcken besteht und nicht über eine JFS-Definition (Journaled File System) verfügt. Nur Ein-/Ausgabefunktionen der unteren Ebene haben Lese-/Schreibzugriff auf einen logischen Datenträger.

## Unicode

Ein Standard für die Zeichencodierung, der den Austausch, die Verarbeitung und die Anzeige von Texten in allen Sprachen der Welt sowie von vielen klassischen und historischen Texten ermöglicht.

## Unicode-aktivierter Dateibereich

Ein Dateibereich mit einem Namen, der dem Unicode-Standard entspricht und mit jeder Ländereinstellung auf mehrsprachigen Workstations kompatibel ist.

## Universally Unique Identifier (UUID)

Die aus 128 Bit bestehende numerische Kennung, mit der sichergestellt wird, dass zwei Komponenten nicht über dieselbe Kennung verfügen. Siehe auch Global eindeutige ID.

## Universal Naming Convention (UNC)

Die Kombination aus Servername und Netzname. Diese Namen geben zusammen die Ressource in der Domäne an.

## Unternehmenskonfiguration

Eine Methode der Servereinrichtung, mit der Administratoren die Konfiguration eines der Server mit Hilfe der Server-zu-Server-Übertragung an die anderen Server verteilen kann. Siehe auch Konfigurationsmanager, Verwalteter Server, Profil, Subskription.

## Unternehmensprotokollierung

Der Prozess des Sendens von Ereignissen von einem Server an einen angegebenen Ereignisserver. Der Ereignisserver leitet die Ereignisse an angegebene Empfänger, z. B. an einen Benutzerexit, weiter. Siehe auch Ereignis.

## Ursprüngliches Dateisystem

Das Dateisystem, aus dem eine Datei umgelagert wurde. Wird eine Datei zurückgerufen, wird sie an das ursprüngliche Dateisystem zurückgegeben.

## UTF-8

Unicode Transformation Format, ein 8-Bit-Codierungsformat, das sich für die Verwendung mit vorhandenen ASCII-basierten Systemen eignet. Der CCSID-Wert für Daten im UTF-8-Format lautet 1208.

## UUID

Siehe Universally Unique Identifier.

## V

---

## Verfall

Der Prozess, durch den Dateien, Datensätze oder Objekte für die Löschung gekennzeichnet werden, da ihr Verfallsdatum oder ihr Aufbewahrungszeitraum überschritten wurde.

## Verfallende Datei

Eine umgelagerte oder vorumgelagerte Datei, die für den Verfall und die Entfernung aus dem Speicher markiert wurde. Wird eine Stubdatei oder eine Originalkopie einer vorumgelagerten Datei aus einem lokalen Dateisystem gelöscht oder wird die Originalkopie einer vorumgelagerten Datei aktualisiert, wird die entsprechende umgelagerte oder vorumgelagerte Datei bei Ausführung der nächsten Abstimmung als verfallen markiert.

## Version

Eine Sicherungskopie einer Datei, die im Serverspeicher gespeichert ist. Die letzte Sicherungskopie einer Datei ist die aktive Version. Frühere Kopien derselben Datei sind inaktive Versionen. Die Anzahl der vom Server aufbewahrten Versionen wird durch

die Kopiengruppenattribute in der Verwaltungsklasse bestimmt.

#### Verwalteter Server

Ein Server, der über eine Subskription für ein oder mehrere Profile Konfigurationsdaten von einem Konfigurationsmanager empfängt. Konfigurationsdaten können Definitionen von Objekten wie Maßnahmen und Zeitpläne umfassen. Siehe auch Konfigurationsmanager, Unternehmenskonfiguration, Profil, Subskription.

#### Verwaltetes Objekt

Eine Definition in der Datenbank eines verwalteten Servers, die dem verwalteten Server von einem Konfigurationsmanager zugeteilt wurde. Wenn ein verwalteter Server ein Profil subskribiert, werden alle diesem Profil zugeordneten Objekte zu verwalteten Objekten in der Datenbank des verwalteten Servers.

#### Verwaltungsberechtigungsklasse

Siehe Berechtigungsklasse.

#### Verwaltungsclient

Ein Programm, das auf einem Dateiserver, einer Workstation oder einem Großrechner ausgeführt wird und von Administratoren für die Steuerung und Überwachung des Servers verwendet wird. Siehe auch Client für Sichern/Archivieren.

#### Verwaltungsklasse

Ein Maßnahmenobjekt, das Benutzer an jede Datei binden können, um anzugeben, wie der Server die Datei verwaltet. Die Verwaltungsklasse kann eine Sicherungskopiergruppe, eine Archivierungskopiergruppe und Speicherverwaltungsattribute enthalten. Siehe auch Binden, Kopiergruppe, Client für hierarchische Speicherverwaltung, Maßnahmengruppe, Erneut binden.

#### Verwaltungssitzung

Ein Zeitraum, während dessen eine Administrator-ID mit einem Server kommuniziert, um Verwaltungstasks auszuführen. Siehe auch Clientknotensitzung, Sitzung.

#### Verwendung von Platzhalterzeichen

Siehe Platzhalterzeichen.

#### Verzeichniscontainerspeicherpool

Ein Speicherpool, der von einem Server verwendet wird, um Daten in Containern in Speicherpoolverzeichnissen zu speichern. Daten, die in einem Verzeichniscontainerspeicherpool gespeichert werden, können entweder die Inline-Dateneduplizierung oder die clientseitige Dateneduplizierung verwenden. Siehe auch Cloud-Containerspeicherpool, Containerspeicherpool, Containerkopierspeicherpool, Speicherpool.

#### Virtueller Dateibereich

Eine Darstellung eines Verzeichnisses in einem NAS-Dateisystem (NAS = Network-Attached Storage) als Pfad zu diesem Verzeichnis.

#### Virtueller Datenträger

Eine Archivierungsdatei auf einem Zielserver, die einen Datenträger mit sequenziellem Zugriff für einen Quellenserver repräsentiert.

#### Virtueller Mountpunkt

Eine Verzeichnisverzweigung eines Dateisystems, das als virtuelles Dateisystem definiert ist. Das virtuelle Dateisystem wird in seinem eigenen Dateibereich auf dem Server gesichert. Der Server verarbeitet den virtuellen Mountpunkt als separates Dateisystem, das Clientbetriebssystem jedoch nicht.

#### Volume Shadow Copy Service (VSS)

Eine Gruppe von Microsoft-Anwendungsprogrammierschnittstellen (APIs - Application-Programming Interfaces), mit denen Spiegelkopiersicherungen von Datenträgern, exakte Kopien von Dateien einschließlich aller offenen Dateien usw. erstellt werden.

#### Vorspanndaten

Datenbytes ab dem Anfang einer umgelagerten Datei, die in der Stubdatei für diese Datei im lokalen Dateisystem gespeichert werden. Der Umfang der Vorspanndaten, die in einer Stubdatei gespeichert werden, ist von der angegebenen Stubgröße abhängig.

#### Vorumgelagerte Datei

Eine Datei, die in den Serverspeicher kopiert, jedoch in dem lokalen Dateisystem nicht durch eine Stubdatei ersetzt wurde. Im lokalen Dateisystem und im Serverspeicher sind identische Kopien der Datei vorhanden. Vorumgelagerte Dateien sind in UNIX- und Linux-Dateisystemen vorhanden, denen die Speicherverwaltung hinzugefügt wurde. Siehe auch Dateistatus, Umgelagerte Datei, Residente Datei.

#### Vorumlagerung

Der Prozess, bei dem Dateien, die für die Umlagerung auswählbar sind, in den Serverspeicher kopiert werden, wobei jedoch die ursprünglichen Dateien in dem lokalen Dateisystem intakt bleiben.

#### Vorumlagerungsprozentsatz

Eine Speicherverwaltungseinstellung, die festlegt, ob die nächsten auswählbaren Kandidaten in einem Dateisystem nach der Schwellen- oder Bedarfsumlagerung vorumgelagert werden.

#### VSS

Siehe Volume Shadow Copy Service.

#### VSS-Schnellzurückschreibung

Eine Operation, bei der Daten aus einer lokalen Momentaufnahme zurückgeschrieben werden. Die Momentaufnahme ist die VSS-Sicherung, die sich auf einem lokalen Spiegeldatenträger befindet. Die Zurückschreibungsoperation ruft die Daten mithilfe einer Kopiermethode auf Dateiebene ab.

#### VSS-Sicherung

Eine Sicherungsoperation, bei der die Microsoft-VSS-Technologie (Volume Shadow Copy Service) verwendet wird. Bei der Sicherungsoperation wird eine Onlinemomentaufnahme (eine konsistente zeitpunktgesteuerte Kopie) erstellt. Diese Kopie kann auf lokalen Spiegeldatenträgern oder im Serverspeicher gespeichert werden.

#### VSS-Sofortzurückschreibung

Eine Operation, bei der Daten aus einer lokalen Momentaufnahme zurückgeschrieben werden. Die Momentaufnahme ist die VSS-Sicherung, die sich auf einem lokalen Spiegeldatenträger befindet. Die Zurückschreibungsoperation ruft die Daten mithilfe einer hardwareunterstützten Zurückschreibungsmethode ab (z. B. eine FlashCopy-Operation).

#### VSS-Zurückschreibung

Eine Funktion, die einen Microsoft-VSS-Softwareprovider (VSS - Volume Shadow Copy Service) verwendet, um Momentaufnahmen zurückzuschreiben, die sich im Serverspeicher befinden. Die Momentaufnahmen wurden durch eine VSS-Sicherung erstellt und werden an ihre ursprüngliche Position zurückgeschrieben.

## W

---

#### Weltweiter Name (WWN)

Eine nicht signierte 64-Bit-Namenskennung, die eindeutig ist.

#### Wiederherstellung

Der Prozess der Konsolidierung der verbleibenden Daten von vielen Datenträgern mit sequenziellem Zugriff auf einer geringeren Anzahl neuer Datenträger mit sequenziellem Zugriff.

#### Wiederherstellungsplan

Eine Datei, die vom Disaster Recovery Manager (DRM) erstellt wird. Sie enthält Informationen zur Wiederherstellung von Computersystemen für den Katastrophenfall sowie Scripts, mit denen einige Wiederherstellungstasks ausgeführt werden können. Die Datei umfasst Informationen zu der vom Server verwendeten Software und Hardware sowie zu dem Standort der Wiederherstellungsdatenträger.

#### Wiederherstellungsprotokoll

Ein Protokoll mit Aktualisierungen, die in Kürze in die Datenbank geschrieben werden. Das Protokoll kann verwendet werden, um Daten nach System- und Datenträgerfehlern wiederherzustellen. Das Wiederherstellungsprotokoll besteht aus dem aktiven Protokoll (einschließlich der Protokollspiegelung) und den Archivprotokollen.

#### Wiederherstellungsschwelle

Der Prozentsatz des Speicherbereichs, über den ein Datenträger mit sequenziellem Zugriff verfügen muss, damit der Server den Datenträger wiederherstellen kann. Speicherbereich kann wiederhergestellt werden, wenn Dateien verfallen oder gelöscht werden.

#### Wiederherstellungsstandort

Siehe Sekundärer Standort.

#### Workloadpartition (WPAR)

Eine Partition innerhalb einer einzelnen Betriebssysteminstanz.

#### Workstation

Eine Datenstation oder ein Personal Computer, an der bzw. dem ein Benutzer Anwendungen ausführen kann und die bzw. der normalerweise mit einem Großrechner oder einem Netz verbunden ist.

#### WPAR

Siehe Workloadpartition.

#### WWN

Siehe Weltweiter Name.

## Z

---

#### Zeilengruppe

Eine Gruppe von Zeilen in einer Datei, die eine gemeinsame Funktion ausführen oder einen Teil des Systems definieren. Zeilengruppen werden normalerweise durch Leerzeilen oder Doppelpunkte getrennt und jede Zeilengruppe hat einen Namen.

#### Zeitlimitüberschreitung

Ein Zeitintervall, das einem Ereignis zugeordnet ist. Tritt das Ereignis innerhalb dieses Zeitintervalls nicht auf oder wird das Ereignis innerhalb dieses Zeitintervalls nicht beendet, wird die Operation unterbrochen.

#### Zeitplan

Ein Datenbanksatz, der Clientoperationen oder Verwaltungsbefehle beschreibt, die verarbeitet werden sollen. Siehe auch Zeitplan für Verwaltungsbefehle, Clientzeitplan.

#### Zeitplan für Verwaltungsbefehle

Ein Datenbanksatz, der die geplante Verarbeitung eines Verwaltungsbefehls während einer bestimmten Zeitspanne beschreibt. Siehe auch Zentrale Zeitplanung, Clientzeitplan, Zeitplan.

#### Zeitplanung über Clientsendeaufruf

Eine Betriebsart, bei der der Client den Server nach Arbeit abfragt. Siehe auch Zeitplanung über Serversystemanfrage.

#### Zeitplanung über Serversystemanfrage

Ein Client/Server-Kommunikationsverfahren, bei dem der Server den Clientknoten kontaktiert, wenn Tasks ausgeführt werden müssen. Siehe auch Zeitplanung über Clientsendeaufruf.

#### Zeitspanne für Mount Wait

Die maximale Anzahl Minuten, die der Server darauf wartet, dass eine Anforderung zum Anhängen eines Datenträgers mit sequenziellem Zugriff ausgeführt wird, bevor die Anforderung abgebrochen wird.

#### Zentrale Zeitplanung

Eine Funktion, die es einem Administrator erlaubt, Clientoperationen und Verwaltungsbefehle zu planen. Die Operationen können so geplant werden, dass sie in regelmäßigen Abständen oder an einem bestimmten Datum ausgeführt werden. Siehe auch Zeitplan für Verwaltungsbefehle, Clientzeitplan.

**Ziel**

Kopiengruppen- oder Verwaltungsklassenattribut, das den primären Speicherpool angibt, in dem eine Clientdatei gesichert, archiviert oder umgelagert wird. Siehe auch Kopierspeicherpool.

**Zielknoten**

Ein Clientknoten, für den anderen Clientknoten (die Agentenknoten genannt werden) Proxyberechtigung erteilt wurde. Mit der Proxyberechtigung können Agentenknoten Operationen wie Sicherung und Zurückschreibung für den Zielknoten ausführen, der Eigner der Daten ist.

**Zufallsverarbeitung**

Der Prozess, bei dem Zeitplanstartzeiten für unterschiedliche Clients innerhalb eines angegebenen Prozentsatzes des Startfensters des Zeitplans verteilt werden.

**Zugriffsmodus**

Ein Attribut eines Speicherpools oder eines Speicherdatenträgers, das angibt, ob der Server in den Speicherpool oder Speicherdatenträger schreiben oder aus diesen lesen kann.

**Zugriffssteuerungsliste (ACL)**

In der Computersicherheit eine Liste, die einem Objekt zugeordnet ist und die alle Subjekte, die auf das Objekt zugreifen können, und deren Zugriffsberechtigungen identifiziert.

**Zuordnung**

Die definierte Beziehung zwischen einem Clientknoten und einem Clientzeitplan. Eine Zuordnung kennzeichnet den Namen eines Zeitplans, den Namen der Maßnahmendomäne, zu der der Zeitplan gehört, sowie den Namen eines Clientknotens, der geplante Operationen ausführt.

**Zurückschreiben**

Informationen vom Sicherungsstandort in den aktiven Speicherstandort kopieren, damit sie verwendet werden können. Ein Beispiel ist das Kopieren von Informationen aus dem Serverspeicher auf eine Client-Workstation.

**Zurückschreibung einer einzelnen Mailbox**

Siehe Mailboxzurückschreibung.